

# HOW CAN TECHNOLOGIES HELP SECURE OUR BORDERS?

---

---

## HEARING BEFORE THE COMMITTEE ON SCIENCE HOUSE OF REPRESENTATIVES ONE HUNDRED NINTH CONGRESS

SECOND SESSION

SEPTEMBER 13, 2006

**Serial No. 109-60**

Printed for the use of the Committee on Science



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

U.S. GOVERNMENT PRINTING OFFICE

28-628PS

WASHINGTON : 2006

---

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

COMMITTEE ON SCIENCE

HON. SHERWOOD L. BOEHLERT, New York, *Chairman*

RALPH M. HALL, Texas	BART GORDON, Tennessee
LAMAR S. SMITH, Texas	JERRY F. COSTELLO, Illinois
CURT WELDON, Pennsylvania	EDDIE BERNICE JOHNSON, Texas
DANA ROHRABACHER, California	LYNN C. WOOLSEY, California
KEN CALVERT, California	DARLENE HOOLEY, Oregon
ROSCOE G. BARTLETT, Maryland	MARK UDALL, Colorado
VERNON J. EHLERS, Michigan	DAVID WU, Oregon
GIL GUTKNECHT, Minnesota	MICHAEL M. HONDA, California
FRANK D. LUCAS, Oklahoma	BRAD MILLER, North Carolina
JUDY BIGGERT, Illinois	LINCOLN DAVIS, Tennessee
WAYNE T. GILCHREST, Maryland	DANIEL LIPINSKI, Illinois
W. TODD AKIN, Missouri	SHEILA JACKSON LEE, Texas
TIMOTHY V. JOHNSON, Illinois	BRAD SHERMAN, California
J. RANDY FORBES, Virginia	BRIAN BAIRD, Washington
JO BONNER, Alabama	JIM MATHESON, Utah
TOM FEENEY, Florida	JIM COSTA, California
RANDY NEUGEBAUER, Texas	AL GREEN, Texas
BOB INGLIS, South Carolina	CHARLIE MELANCON, Louisiana
DAVE G. REICHERT, Washington	DENNIS MOORE, Kansas
MICHAEL E. SODREL, Indiana	DORIS MATSUI, California
JOHN J.H. "JOE" SCHWARZ, Michigan	
MICHAEL T. MCCAUL, Texas	
MARIO DIAZ-BALART, Florida	

# CONTENTS

September 13, 2006

Witness List .....	Page 2
Hearing Charter .....	3

## Opening Statements

Statement by Representative Sherwood L. Boehlert, Chairman, Committee on Science, U.S. House of Representatives .....	15
Written Statement .....	15
Statement by Representative Bart Gordon, Minority Ranking Member, Committee on Science, U.S. House of Representatives .....	16
Written Statement .....	17
Prepared Statement by Representative Jerry F. Costello, Member, Committee on Science, U.S. House of Representatives .....	17
Prepared Statement by Representative Darlene Hooley, Member, Committee on Science, U.S. House of Representatives .....	18
Prepared Statement by Representative Lincoln Davis, Member, Committee on Science, U.S. House of Representatives .....	18

## Witnesses:

Admiral Jay M. Cohen, Under Secretary for Science and Technology, U.S. Department of Homeland Security; Accompanied by Mr. Gregory L. Giddens, Director, Secure Border Initiative Program Executive Office, U.S. Department of Homeland Security	
Oral Statement .....	19
Written Statement .....	22
Biography (Admiral Jay M. Cohen) .....	26
Biography (Gregory L. Giddens) .....	27
Mr. Gordon Daniel Tyler, Jr., Johns Hopkins University, Applied Physics Laboratory, National Security Technology Division	
Oral Statement .....	28
Written Statement .....	30
Biography .....	45
Financial Disclosure .....	48
Dr. Peter R. Worch, Independent Consultant, Member of the U.S. Air Force Science Advisory Board	
Oral Statement .....	49
Written Statement .....	51
Biography .....	60
Financial Disclosure .....	63
Dr. Gervasio Prado, President, Sentech, Inc.	
Oral Statement .....	63
Written Statement .....	65
Biography .....	66
Financial Disclosure .....	67
Dr. Gregory J. Pottie, Associate Dean for Research and Physical Resources, Henry Samueli School of Engineering and Applied Science, University of California, Los Angeles	
Oral Statement .....	67
Written Statement .....	70
Biography .....	80

IV

	Page
Dr. Gregory J. Pottie, Associate Dean for Research and Physical Resources, Henry Samueli School of Engineering and Applied Science, University of California, Los Angeles—Continued	
Financial Disclosure .....	81
Discussion .....	82

**Appendix: Answers to Post-Hearing Questions**

Admiral Jay M. Cohen, Under Secretary for Science and Technology, U.S. Department of Homeland Security; Accompanied by Mr. Gregory L. Giddens, Director, Secure Border Initiative Program Executive Office, U.S. Department of Homeland Security .....	110
Dr. Peter R. Worch, Independent Consultant, Member of the U.S. Air Force Science Advisory Board .....	115

## **HOW CAN TECHNOLOGIES HELP SECURE OUR BORDERS?**

---

**WEDNESDAY, SEPTEMBER 13, 2006**

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON SCIENCE,  
*Washington, DC.*

The Committee met, pursuant to call, at 2:19 p.m., in Room 2318 of the Rayburn House Office Building, Hon. Sherwood L. Boehlert [Chairman of the Committee] presiding.

**COMMITTEE ON SCIENCE  
U.S. HOUSE OF REPRESENTATIVES**

***How Can Technologies Help Secure Our Borders?***

Wednesday, September 13, 2006  
2:00 p.m. – 4:00 p.m.  
2318 Rayburn House Office Building

**Witness List**

**Admiral Jay M. Cohen**  
Under Secretary for Science and Technology  
U.S. Department of Homeland Security

**Mr. Gregory Giddens**  
Director, Secure Border Initiative Program Executive Office  
U.S. Department of Homeland Security

**Mr. G. Daniel Tyler**  
Johns Hopkins University  
Applied Physics Laboratory  
National Security Technology Division

**Dr. Peter R. Worch**  
Independent Consultant  
Member of the U.S. Air Force Science Advisory Board

**Dr. Gervasio Prado**  
President  
SenTech Inc.

**Dr. Gregory Pottie**  
Associate Dean for Research and Physical Resources  
Henry Samueli School of Engineering and Applied Science  
University of California Los Angeles

Section 210 of the Congressional Accountability Act of 1995 applies the rights and protections covered under the Americans with Disabilities Act of 1990 to the United States Congress. Accordingly, the Committee on Science strives to accommodate/meet the needs of those requiring special assistance. If you need special accommodation, please contact the Committee on Science in advance of the scheduled event (3 days requested) at (202) 225-6371 or FAX (202) 225-0891.

Should you need Committee materials in alternative formats, please contact the Committee as noted above

HEARING CHARTER

**COMMITTEE ON SCIENCE  
U.S. HOUSE OF REPRESENTATIVES****How Can Technologies  
Help Secure Our Borders?**WEDNESDAY, SEPTEMBER 13, 2006  
2:00 P.M.—4:00 P.M.  
2318 RAYBURN HOUSE OFFICE BUILDING**1. Purpose**

On September 13, 2006, the House Science Committee will hold a hearing to examine how technology could be used to monitor the borders of the United States to deter illegal entry into the country and aid in apprehension of those crossing between legal points of entry.

**2. Witnesses**

**Mr. Jay M. Cohen** (RAdm., USN ret.) is the Under Secretary of Science and Technology at the U.S. Department of Homeland Security (DHS).

**Mr. Gregory Giddens** is the Director of the Secure Border Initiative Program Executive Office at DHS.

**Dr. Gregory J. Pottie** is the Associate Dean for Research and Physical Resources and a member of the Center for Embedded Network Sensors (funded in part by the National Science Foundation), Henry Samueli School of Engineering and Applied Science, UCLA.

**Dr. Gervasio Prado** is the President of Sentech, Inc. He is an expert in seismic and acoustic ground sensors.

**Mr. G. Daniel Tyler** heads the National Security Technology Division at the Johns Hopkins University Applied Physics Laboratory.

**Dr. Peter R. Worch** is an independent consultant, member of Air Force Science Advisory Board, and former Vice Commander of the Air Force's Rome Air Development Center (now Rome Laboratory).

**3. Overarching Questions**

- What technologies are currently being used at the borders? What are the strengths and weaknesses of these technologies? What technologies are currently available or in development that could improve security at the borders?
- How should the effectiveness of technologies be evaluated? How can the proper balance between deployment of technology and deployment of personnel be determined?
- What research is or should be underway to develop the next generation of border security technologies? How is DHS determining specific technology requirements, and how are these communicated to researchers and technology manufacturers?

**4. Brief Overview**

- The United States shares a border with Mexico that is over 2,000 miles long, and a border with Canada that is over 5,200 miles long. Both borders include remote stretches of land where unauthorized aliens can and do enter the United States.
- An array of technologies that are either currently available commercially, adaptable from military applications, or in development, could be deployed along the borders to enhance surveillance of human or vehicular traffic. Some experts suggest that an integrated system of advanced surveillance technologies, deployed along the borders with the necessary communications and information technology infrastructure, could provide more effective security in remote areas than would be provided by physical barriers.

- Impediments to deployment of border surveillance technologies include the cost of the technologies and their operation; the sensitivity of high-tech surveillance equipment to extreme temperatures and harsh environments; and the need to efficiently monitor, analyze, and respond to the potentially vast quantities of information generated by such equipment.
- On November 2, 2005, DHS announced the Secure Border Initiative (SBI), a multi-year plan to secure the Nation's borders through improvements in technology and increases in personnel. The fiscal year 2007 (FY07) budget request for SBI is \$639 million. Questions remain about how DHS will manage the technology selection and deployment process, as well as whether the DHS Science and Technology (S&T) Directorate is carrying out the appropriate programs to support the SBI and develop the next generation of border security technologies.
- Congress has become increasingly concerned that the S&T Directorate is not providing adequately technical support to the operational units of DHS or effectively engaging the scientific community and private sector in targeted research and development programs. As a result, both the House and Senate appropriators have proposed significant reductions in the S&T Directorate's funding for FY07.

## 5. Background

Most traffic across the borders of the United States occurs at formal, monitored points of entry. Between the official entry points, however, there are vast stretches of undeveloped and unpopulated land where drug trafficking occurs and unauthorized aliens can and do enter the United States; these remote stretches of land along the borders also provide an opportunity for terrorists to enter the country undetected. Advanced sensing and information technology can assist in improving border surveillance and may constitute an effective alternative or supplement to physical barriers.

On November 2, 2005, DHS announced the Secure Border Initiative (SBI), a multi-year plan to secure the Nation's borders and reduce illegal immigration by installing state-of-the-art surveillance technologies along the border as well as by increasing the personnel dedicated to border security and alien detention and processing. A component of this plan is SBInet, a system to integrate the relevant technologies and personnel at the border. DHS plans to award a single large contract for this technology integration project by September 30, 2006. The FY07 budget request for SBInet was \$100 million, and current estimates suggest that the SBInet program will eventually cost approximately \$2.5 billion over five years. While the House and Senate FY07 appropriations bills allot DHS \$115 and \$132 million, respectively, to start on the SBInet, both bills require DHS to provide a strategic plan to Congress before most of the funding may be spent. Recent articles in *The Washington Post* and *The New York Times* describe concerns about whether the department is prepared to adequately manage the SBInet development and acquisition process and to effectively deploy and use the resulting technologies (see Appendices A and B).

### *Technologies for Border Security*

The two main classes of surveillance technologies are ground sensors and aerial vehicles. Ground sensors are devices that can detect movement or traffic in areas near or at the borders. These may be buried underground or elevated on fixed poles. Examples of such sensors include magnetic sensors (which detect passing metal objects), seismic sensors (which detect land movement resulting from the passage of groups of people or vehicles), infrared sensors (which detect changes in heat patterns), and visual sensors (i.e., regular or night vision cameras). Radar systems mounted on towers may also be utilized to detect movement. The strengths of these sensors is that their ranges vary from tens of yards to upwards of several miles, they are "always on" without getting tired or hungry, and by designing their deployment strategically, the different types of data they supply can be integrated to provide information on the path or behavior of whatever traffic has been observed and reduce the likelihood of false alarms. Their potential weaknesses relate to the cost of the sensors and their operation, and the difficulty of operating technologies in remote terrain, such as the need to develop long-lasting power sources to support sensors and communication systems, and electronic hardware that does not break down in extreme heat or cold. Acquisition costs for ground sensors are thousands of dollars per sensor, and installing ground-based radar systems can cost hundreds of thousands of dollars.



Aerial vehicles equipped with a variety of sensors can be used to provide broad area surveillance over hundreds of miles. Examples include manned or unmanned aircraft and lighter than air platforms, including aerostats (which are tethered blimps) or airships (which hover at high altitudes). All of these platforms can carry sensor systems including visual cameras, radar systems, and electro-optical and infrared devices that use physical characteristics such as heat and movement to detect objects hidden from or too distant for visual inspection. The attraction of these aerial vehicles is that they can detect moving objects on the ground as well as capture images of recently traveled paths and thus can facilitate tracking suspicious motion in remote regions until Border Patrol agents can arrive to investigate. In addition, unmanned aerial vehicles can spend a significantly longer period of time in the air than manned aircraft since they are independent of an on-board human operator. However, there are limitations to the use of unmanned aerial vehicles in civilian airspace, and it is likely to be at least three to eight years before the Federal Aviation Administration approves of the use of unmanned aerial vehicles in commercial airspace. For the FAA to approve the use of unmanned aerial vehicles in commercial airspace, the unmanned vehicles will have to demonstrate the same capability as a human pilot to detect and avoid other aircraft. Unmanned aerial vehicles cost millions of dollars. For example, the replacement cost of the Customs and Border Protection Predator B unmanned aerial vehicle that crashed in April 2006 is \$6.8 million.

A variety of ground sensors and aerial vehicles are available today from commercial sources and are in use at the borders and by the military. These systems can be used to start the SBInet program, but improved technologies and new technologies are likely to be needed for a fully effective system. Relevant research and development is ongoing at academic centers, military laboratories, and the private sector, and these programs should lead to technologies with more accurate detection, improved resolution, and reduced procurement and maintenance costs. One question is how DHS S&T can best support, guide and accelerate such research and development work.

#### *Past Use of Technologies for Border Security*

The security of the U.S. border is the responsibility of Customs and Border Protection, a unit of DHS that includes the Border Patrol and an air patrol unit. For many years, various forms of technology have been used at the border to support Border Patrol activities. For example, the Border Patrol has, since the early 1970s, placed sensors in remote areas to detect traffic by using ground sensors that detect movement and heat as well as video cameras and night vision cameras for surveillance. However, the DHS Office of the Inspector General (OIG) conducted a review<sup>1</sup> of remote surveillance technology acquisition programs managed by the Border Patrol, evaluating primarily the Integrated Surveillance Intelligence System established in 1998, and determined that the technology acquired could not be credited for increases in apprehensions, and it consumed significant staff time to monitor videos and investigate sensor alarms. The report, published in December 2005, also concluded:

- There was no integration of the technology components (i.e., if a camera was installed in the vicinity of a sensor, it had to be manually redirected so that a visual check could be done when motion was detected);
- The sensor systems were unable to differentiate false alarms due to weather changes or animal movement from incidents worth investigating;
- Efficient management of alarms and information was lacking (i.e., messages containing no information beyond that an alarm was triggered were sent to a remote office requiring agents to be dispatched to investigate the area); and
- Many sensors were not designed to withstand the stresses of the variations in terrain and weather conditions along the borders.

In February, 2006, DHS testified before Congress on the agency's response to the OIG report.<sup>2</sup> DHS agreed with the concerns outlined in the report and noted that the Integrated Surveillance Intelligence System program had already been terminated (in 2004). DHS faulted the former Immigration and Naturalization Service and the General Services Administration for the poor management and oversight, lack of acquisition planning, and inadequate vendor competition noted by the OIG

<sup>1</sup> Report OIG-0615, "A Review of Remote Surveillance Technology Along the U.S. Land Borders," Department of Homeland Security, Office of the Inspector General, December 2005.

<sup>2</sup> Testimony of Greg Giddens, Director, Secure Border Initiative Program Executive Office, DHS before the House Committee on Homeland Security, Subcommittee on Management, Integration, and Oversight, February 16, 2006.

and stated that Customs and Border Protection had already taken steps to create a program management office with expertise in systems acquisition, contract management and oversight, and engineering to ensure that the administration of the SBI program would make more appropriate and effective decisions about technology acquisition, deployment, and use.

In addition to the Border Patrol's use of sensors on the ground, the air unit of Customs and Border Protection also conducts surveillance and interdiction of illegal activity using helicopters and small planes. These activities were supplemented by surveillance by unmanned aircraft with the assistance of the Department of Defense from June 2004 through January 2005. DHS then acquired a Predator B unmanned aircraft and deployed it along the southern border in September 2005. This aircraft crashed in April 2006, and the preliminary National Transportation Safety Board review implicates a procedural error made by the land-based pilot. DHS had already contracted to purchase a second Predator B prior to the crash of the first one and both the House and Senate Appropriations bills for FY07 include funding for acquisition of unmanned aerial vehicles.

In addition to ground sensors and aerial surveillance, the Border Patrol has also used fencing in certain locations as part of border traffic control efforts. In 1993, the Border Patrol completed a 14-mile fence along the San Diego sector border, and a more robust secondary fence replacement has been built along nine of the 14 miles since then. The effectiveness of the San Diego sector fence has been debated; proponents cite the drastic reduction in apprehensions in the years following its construction as evidence of its success, while opponents attribute the reduction to growth in Border Patrol personnel and increased local deployment of ground sensors. Outside factors such as economics and the job market may have also played a role. In addition, counting the number of apprehensions locally does not provide information about the displacement of illegal traffic to areas without a fence.<sup>3</sup> Proponents continue to advocate for the construction of physical barriers. In the current Congress, the House and Senate immigration bills<sup>4</sup> both authorize the Secretary of Homeland Security to build a fence over hundreds of miles along the southwest border. An amendment to fund the construction of 370 miles of fencing along the southern border at a cost of \$1.8 billion originally proposed to the Senate's FY07 Department of Homeland Security appropriations bill was defeated, however it was later adopted in the Senate FY07 Department of Defense appropriations bill.

#### *Future Use of Technologies for Border Security*

In determining what sensors to use, one critical issue is the capability of the sensors to function with minimal interruption in a variation of environments, including desert, forests, mountains, and waterways, with significant temperature and weather fluctuations. In remote areas, providing power to support both the sensors and the communications systems that transmit the sensor data is also a technical challenge.

A second critical issue is that the installation of large numbers of sensors, cameras, and other surveillance systems in the ground, on elevated platforms and on aerial vehicles will generate tremendous amounts of data. Computer systems can be used to manage the data, but it will be important to figure out where to deploy the sensors and how to link them together into a network so that information from different sensors can be compiled to provide a more complete picture of activities along the border. For example, installing infrared cameras and motion sensors in related positions can help Border Patrol distinguish between false alarms (say a passing coyote) and events worthy of further investigation and significantly reduce the dependence on personnel to look into alarms triggered by each sensor separately. Networked systems of sensors may also be used to collect data over a period of time and distance to allow agents or even computers to track a series of movements observed through several sensors being activated along the path of a group of people or a vehicle. Such data would assist in predicting where a Border Patrol agent could intercept the group most effectively. More advanced computer systems and networks could even take all of the information from the sensors and combine it with information about personnel and other infrastructure assets to provide a broad picture of activity along the border, which can be seen both by agents on patrol and central offices as needed in order to effectively manage responses and adjust agent deployments.

<sup>3</sup> Blas Nunez-Neto and Stephen Vina, "Border Security: Fences Along the U.S. International Border," CRS Report RS22026, January 11, 2006.

<sup>4</sup> The immigration bills are H.R. 4437, *The Border Protection, Anti-terrorism, and Illegal Immigration Control Act of 2005*, which passed the House on December 16, 2005, and S. 2611, *The Comprehensive Immigration Reform Act of 2006*, which passed the Senate on May 25, 2006.

A third critical issue is how border security personnel will be deployed to make effective use of the sensor technologies and how to ensure that sensor information is displayed in a clear and usable fashion.

Computer models of the border security system developed with the support of DHS can help officials make decisions about what sensors to purchase and how to arrange them. Modeling is a mechanism to test system design to predict the effectiveness of different configurations of technology, forecast the personnel necessary to respond to incidents, and better understand the trade-offs between various options.

Research and development at universities, federal laboratories, and in the private sector is underway to produce the next generation of sensors and computer software that will improve sensor data analysis and interpretation. Nanotechnology is increasingly facilitating the miniaturization of sensors, allowing the creation of devices that can perform multiple sensor functions (i.e., combining movement and light detection). Sensors may be designed that can detect mobile communication devices such as radios and cell phones which are likely to be carried by smugglers. New computer analysis software programs are creating “smart” systems, such as sensors that can make adjustments based on data from nearby sensors, altering their sensitivity or orientation to focus on local activity and assist with differentiating background noise from real events, or computer programs that can “learn” from past experiences to properly predict which activities require investigation by personnel. One of the great challenges is development of “automated scene understanding” programs, computer systems that can automatically analyze images and recognize certain types of activities, such as characteristic physical behavior of migrants crossing through remote areas. Such automated interpretation of the feeds from cameras could greatly reduce the time spent by people interpreting images and deciding if they merit investigation.

#### *The Role of the DHS Science and Technology Directorate*

The DHS Science and Technology Directorate (S&T) conducts research, development, testing, and evaluation of technologies to support the components of DHS, such as Customs and Border Protection. The funding levels within DHS S&T for border security activities are provided in Table 1.

Table 1: Funding for Border Security Activities within DHS S&T

Year	Funding Level (\$ in millions)
FY04	19.5 <sup>5</sup>
FY05	14.5
FY06	14.7
FY07 (requested)	23.3 <sup>6</sup>

<sup>5</sup> FY04 appropriations included a one-time provision of \$4.0 million to support analysis of unmanned aerial vehicle capabilities in support of the Border Patrol’s potential acquisition.

<sup>6</sup> The FY07 DHS appropriations bills do not allot specific funding levels for border security activities in DHS S&T.

DHS S&T has supported DHS border security operations beginning in FY04, when it participated in the analysis and selection of an unmanned aerial vehicle for acquisition by the Border Patrol. In FY05, S&T evaluated various commercially available sensors to determine how well they could distinguish between animal and human traffic and how well their power sources worked. S&T also supported the development of BorderNet, a pilot program to provide Border Patrol agents with mobile computers to compare names and fingerprints of apprehended individuals with a database while still in the field and to allow them to communicate with other agents and potential backup teams.

Currently, DHS S&T is contributing to the DHS-wide Secure Border Initiative by developing software that simulates the relationships and interdependencies among all personnel and assets at the border as well as immigration and customs enforcement infrastructure. This software is designed to allow the people making decisions about procurement and deployment of technologies to understand the trade-offs and possible unintended consequences of various changes in the broader border and immigration system, such as increased apprehensions requiring more detainment facilities and leading to backlogs in immigration court proceedings. In addition, DHS

S&T is developing software that provides situational awareness to assist Border Patrol supervisors in tracking the location of agents and sensor activity on computer generated map displays to allow for efficient coordination of all possible resources in response to incidents or alarms.

Since DHS was created in 2003, the S&T Directorate has struggled with issues related to program execution, the setting of priorities, and the building of relationships with the potential users of technologies within DHS. Congress and outside observers have expressed concerns that the S&T Directorate does not provide sufficient help in evaluating technologies for DHS acquisition programs, is not moving quickly enough to assess and adopt potential new technologies proposed by the private sector, and does not have a clear way to determine priorities for long-term research investments.

Congressional concerns about ill-defined priorities, poor financial management systems, and staff turnover have affected DHS S&T's appropriations. In FY07, the House and Senate-passed appropriations levels are \$956 million and \$818 million, respectively; each is significantly below the request level (\$1,002 million) and the FY06 appropriated funding for the current S&T programs (\$1,153 million). Jay M. Cohen was sworn in as Under Secretary for Science and Technology on August 10, 2007. He filled a position which had been vacant since March 2006.

#### **6. Questions for the Witnesses**

Mr. Cohen and Mr. Giddens were asked to address the following questions in their testimony:

- What technologies are currently being used at the borders? What are the strengths and weaknesses of these technologies? What technologies are currently available or in development that could improve security at the borders?
- How is DHS making decisions about technology acquisition? How does DHS evaluate the effectiveness of technologies? How is the proper balance between deployment of technology and deployment of personnel determined?
- What research is underway to develop the next generation of border security technologies? How is DHS determining specific technology requirements and how are these communicated to researchers and technology manufacturers?

Dr. Pottie, Dr. Prado, Mr. Tyler, and Dr. Worch were asked to address the following questions in their testimony:

- What technologies are currently being used at the borders? What are the strengths and weaknesses of these technologies? What technologies are currently available or in development that could improve security at the borders?
- How should the effectiveness of technologies be evaluated? How can the proper balance between deployment of technology and deployment of personnel be determined?
- What research is or should be underway to develop the next generation of border security technologies? How is DHS communicating specific technology requirements to researchers and technology manufacturers?

**Appendix A:****Technology Has Uneven Record on Securing Border***Washington Post*, May 21, 2006, Page A01

BY SPENCER S. HSU AND JOHN POMFRET,

*Washington Post* Staff Writers

Applying lessons the U.S. military has learned in Afghanistan and Iraq, the Bush administration is embarking on a multi-billion-dollar bid to help secure the U.S.-Mexican border with surveillance technology—a strategy that veterans of conflicts abroad say will be more difficult than it appears.

One component of the Strategic Border Initiative provides the technological underpinning for the bold prediction by Homeland Security Secretary Michael Chertoff that the United States will gain control of the Mexican border and the Canadian border in as little as three years.

The plan envisions satellites, manned and unmanned aircraft, ground sensors and cameras tied to a computerized dispatch system that would alert Border Patrol units. “We are launching the most technologically advanced border security initiative in American history,” President Bush said in his address to the Nation Monday.

Skeptics contend that the Department of Homeland Security’s record of applying technology is abysmal. Industry analysts say that an initial \$2 billion private-sector estimate is low. And by allowing the winning bidder to determine the technology and personnel needed to detect, catch, process and remove illegal immigrants, experts say, the plan ensures a big payday for contractors, whatever the outcome.

“If the military could seal a 6,000-mile border for \$2 billion, Iraq’s borders would have been sealed two years ago,” said Andrew F. Krepinevich Jr., Executive Director of the Center for Strategic and Budgetary Assessments, a defense think tank.

SBI-net, part of the border initiative, will dictate the government’s long-term presence. Bush’s push for a guest-worker program is grounded in the premise that conventional “enforcement alone will not do the job.”

By reducing demand for immigrant labor, beefing up the Border Patrol and deploying next-generation technology to catch illegal border crossers, the administration plan “assumes operational control within . . . three to five years,” Chertoff told Congress last month.

To supporters such as Sen. Judd Gregg (R-N.H.), Chairman of the Senate subcommittee that funds homeland security, the Pentagon already possesses the necessary technology.

“It’s complex, but it doesn’t have to be invented. It hardly even has to be modified,” Gregg said. “It’s really just a question of will—and dollars.”

On the ground, early results of the government’s multi-billion-dollar wager to plug the porous border already are on display.

In far southwestern Arizona, U.S. Customs agents, the Border Patrol and the National Guard patrol 120 miles of forbidding desert from a communications room filled with computer workstations and lined with 25 flat-screen televisions on the wall.

The Border Patrol installed 25 fixed cameras over favored smuggling routes in the sector in recent years. More than 100 sensors lie buried in the ground. Seismic sensors alert at the movement of large numbers of people. Infrared sensors pick up heat signatures of people and objects, and magnetic sensors detect vehicles.

Agents also point to what they call the “skybox”—a 25-square-foot room 30 feet above the border on a hydraulic jack, with top-of-the-line night-vision equipment. Agents say it’s claustrophobic but has one redeeming virtue—air conditioning.

Overhead, the border agencies use blimps, unmanned aircraft, Black Hawk and Chinook helicopters and fixed-wing aircraft.

“We are starting to see substantial improvements,” said Chris Van Wagenen, a senior patrol agent assigned to Yuma, Ariz. “Now we’ve got sensors, cameras. We’ve doubled our manpower in a year, but we still need more.”

Bush has budgeted \$100 million this year for SBI-net. But Chertoff’s department declined to estimate how much the three-to-six-year contract ultimately will cost. Industry analysts expect at least \$2 billion in spending—and possibly much more over a longer period, based on the history of overruns in major Homeland Security technology programs.

By turning to contractors such as Boeing, Ericsson, Lockheed Martin, Northrop Grumman and Raytheon to design the workings of the system, SBI-net also marks a government reliance on private-sector partners to carry out missions without a

clear idea of what the network will look like, according to experts and immigration officials.

“SBI-net represents a potential bonanza” for tens if not hundreds of companies, said John Slye, senior analyst of federal opportunities for Input, a Reston-based federal contracting consulting firm. The project is the most anticipated single civilian information technology contract since the Sept. 11, 2001, terrorist attacks, he said.

Skeptics in Congress cite a decade of frustration at the border.

Because of poor management, two failed border technology programs have cost taxpayers \$429 million since 1998, the Homeland Security inspector general reported in December. Nearly half of 489 remote video surveillance sites planned for the border in the past eight years were never installed. Sixty percent of sensor alerts are never investigated, 90 percent of the rest are false alarms and only one percent overall result in arrests.

A 10-year, \$10 billion system to automate border entry and exit data, US-VISIT, has yet to test security and privacy controls in its seventh year, congressional auditors reported.

Sen. Joseph I. Lieberman (Conn.), top Democrat on the homeland security committee, called the plan to solicit bids by May 30, pick a single winner and start to deploy by September “unrealistic” and filled with “too many questions.”

“How is ‘SBI’ not just another three-letter acronym for failure?” Harold Rogers (R-Ky.), Chairman of the House Appropriations Subcommittee, asked at a hearing last month.

Chertoff deputy Michael P. Jackson said government is not the best judge of innovation in rapidly evolving technology and will benefit from the nimbleness of the private sector while conducting disciplined oversight.

“We are not buying a pig in a poke. . . . We don’t have to buy everything they sell,” said Jackson, former head of a division at Lockheed Martin.

In Arizona, agents say cameras are mainly limited to populated areas because other parts of the border, where most illegal crossings occur, do not have electricity, and solar-powered cameras don’t work. Sand, insects and moisture play havoc with the sensors, causing them to shut down or fire repeatedly. Agents and support staff are too busy to respond to each alarm.

On April 25, the Border Patrol’s first and only Predator 2 unmanned aerial vehicle crashed outside Tubac, Ariz., just seven months after the \$6.5 million craft began its flights.

To military experts, the goal of erecting a “virtual fence” recalls attempts four decades ago to shut down the 1,700-square-mile area of the Ho Chi Minh Trail used to infiltrate South Vietnam, and more recently, to halt incursions along 1,200 miles of Iraq’s border with Iran, Saudi Arabia and Syria.

“It’s always harder than you think,” said Robert Martinage, Krepinevich’s senior defense analyst. “The record is mixed.”

Technology has, of course, advanced rapidly over the decades. The Southwest’s climate and foliage pose fewer challenges, and U.S. law enforcement has advantages of mobility, security and infrastructure on its side, said retired Air Force Maj. Gen. Glen D. Shaffer, a former director for intelligence for the Joint Chiefs of Staff.

Shaffer, now President and Chief Operating Officer of dNovus RDI, a Texas firm that may bid on SBI-net, said the project is reasonable but not foolproof. “Where the military historically has fallen short is putting all investments in sensors and not enough in the people that exploit the sensors. I would hope that DHS can get this right.”

But smugglers of drugs and immigrants also are highly adaptable and willing to escalate the border “arms race,” said Deborah W. Meyers, senior policy analyst at the Migration Policy Institute, a think tank.

“Coyotes” are regularly caught with night-vision goggles, military-issue binoculars, hand-held global positioning systems, and a treasure trove of cell phones and police scanners that allow them to listen to border agents.

Border Patrol agents said that smugglers dispatch scouts every five minutes to check enforcement through the border crossing at San Luis, due south of Yuma on the Mexican border.

“They even know the names of our drug dogs, and which are better at which drugs,” one agent said. “It’s unbelievable how much we are being watched.”

Officials say they don’t need to seal the borders. They just need to catch enough illegal border crossers to deter others from attempting the trip.

Robert C. Bonner, head of Customs and Border Protection from 2003 to 2005, said that at current staffing, the Border Patrol can handle only 10 percent of the illegal immigrant problem.

“But if you can reduce the flow even by half,” he said, “with moderate increases for Border Patrol and technology, we actually can control our border in a way we haven’t been able to in 20 or 30 years.”

**Appendix B:**

**Seeking to Control Borders,  
Bush Turns to Big Military Contractors**

*The New York Times*, May 18, 2006, Page A1  
BY ERIC LIPTON

The quick fix may involve sending in the National Guard. But to really patch up the broken border, President Bush is preparing to turn to a familiar administration partner: the Nation's giant military contractors.

Lockheed Martin, Raytheon and Northrop Grumman, three of the largest, are among the companies that said they would submit bids within two weeks for a multi-billion-dollar federal contract to build what the Administration calls a "virtual fence" along the Nation's land borders.

Using some of the same high-priced, high-tech tools these companies have already put to work in Iraq and Afghanistan—like unmanned aerial vehicles, ground surveillance satellites and motion-detection video equipment—the military contractors are zeroing in on the rivers, deserts, mountains and settled areas that separate Mexico and Canada from the United States.

It is a humbling acknowledgment that despite more than a decade of initiatives with macho-sounding names, like Operation Hold the Line in El Paso or Operation Gate Keeper in San Diego, the Federal Government has repeatedly failed on its own to gain control of the land borders.

Through its Secure Border Initiative, the Bush administration intends to not simply buy an amalgam of high-tech equipment to help it patrol the borders—a tactic it has also already tried, at a cost of hundreds of millions of dollars, with extremely limited success. It is also asking the contractors to devise and build a whole new border strategy that ties together the personnel, technology and physical barriers.

"This is an unusual invitation," the deputy secretary of homeland security, Michael Jackson, told contractors this year at an industry briefing, just before the bidding period for this new contract started. "We're asking you to come back and tell us how to do our business."

The effort comes as the Senate voted Wednesday to add hundreds of miles of fencing along the border with Mexico. The measure would also prohibit illegal immigrants convicted of a felony or three misdemeanors from any chance at citizenship.

The high-tech plan being bid now has many skeptics, who say they have heard a similar refrain from the government before.

"We've been presented with expensive proposals for elaborate border technology that eventually have proven to be ineffective and wasteful," Representative Harold Rogers, Republican of Kentucky, said at a hearing on the Secure Border Initiative program last month. "How is the S.B.I. not just another three-letter acronym for failure?"

President Bush, among others, said he was convinced that the government could get it right this time.

"We are launching the most technologically advanced border security initiative in American history," Mr. Bush said in his speech from the Oval Office on Monday.

Under the initiative, the Department of Homeland Security and its Customs and Border Protection division will still be charged with patrolling the 6,000 miles of land borders.

The equipment these Border Patrol agents use, how and when they are dispatched to spots along the border, where the agents assemble the captured immigrants, how they process them and transport them—all these steps will now be scripted by the winning contractor, who could earn an estimated \$2 billion over the next three to six years on the Secure Border job.

More Border Patrol agents are part of the answer. The Bush administration has committed to increasing the force from 11,500 to about 18,500 by the time the president leaves office in 2008. But simply spreading this army of agents out evenly along the border or extending fences in and around urban areas is not sufficient, officials said.

"Boots on the ground is not really enough," Homeland Security Secretary Michael Chertoff said Tuesday at a news conference that followed Mr. Bush's announcement to send as many as 6,000 National Guard troops to the border.

The tools of modern warfare must be brought to bear. That means devices like the Tethered Aerostat Radar, a helium-filled airship made for the Air Force by Lockheed Martin that is twice the size of the Goodyear Blimp. Attached to the



ground by a cable, the airship can hover overhead and automatically monitor any movement night or day. (One downside: it cannot operate in high winds.)

Northrop Grumman is considering offering its Global Hawk, an unmanned aerial vehicle with a wingspan nearly as wide as a Boeing 737, that can snoop on movement along the border from heights of up to 65,000 feet, said Bruce Walker, a company executive.

Closer to Earth, Northrop might deploy a fleet of much smaller, unmanned planes that could be launched from a truck, flying perhaps just above a group of already detected immigrants so it would be harder for them to scatter into the brush and disappear.

Raytheon has a package of sensor and video equipment used to protect troops in Iraq that monitors an area and uses software to identify suspicious objects automatically, analyzing and highlighting them even before anyone is sent to respond.

These same companies have delivered these technologies to the Pentagon, sometimes with uneven results.

Each of these giant contractors—Lockheed Martin alone employs 135,000 people and had \$37.2 billion in sales last year, including an estimated \$6 billion to the Federal Government—is teaming up with dozens of smaller companies that will provide everything from the automated cameras to backup energy supplies that will keep this equipment running in the desert.

The companies have studied every mile of border, drafting detection and apprehension strategies that vary depending on the terrain. In a city, for example, an immigrant can disappear into a crowd in seconds, while agents might have hours to apprehend a group walking through the desert, as long as they can track their movement.

If the system works, Border Patrol agents will know before they encounter a group of intruders approximately how many people have crossed, how fast they are moving and even if they might be armed.

Without such information, said Kevin Stevens, a Border Patrol official, “we send more people than we need to deal with a situation that wasn’t a significant threat,” or, in a worst case, “we send fewer people than we need to deal with a significant threat, and we find ourselves outnumbered and outgunned.”

The government’s track record in the last decade in trying to buy cutting-edge technology to monitor the border—devices like video cameras, sensors and other tools that came at a cost of at least \$425 million—is dismal.

Because of poor contract oversight, nearly half of video cameras ordered in the late 1990’s did not work or were not installed. The ground sensors installed along the border frequently sounded alarms. But in 92 percent of the cases, they were sending out agents to respond to what turned out to be a passing wild animal, a train or other nuisances, according to a report late last year by the homeland security inspector general.

A more recent test with an unmanned aerial vehicle bought by the department got off to a similarly troubling start. The \$6.8 million device, which has been used in the last year to patrol a 300-mile stretch of the Arizona border at night, crashed last month.

With Secure Border, at least five so-called system integrators—Lockheed, Raytheon and Northrop, as well as Boeing and Ericsson—are expected to submit bids.

The winner, which is due to be selected before October, will not be given a specific dollar commitment. Instead, each package of equipment and management solutions the contractor offers will be evaluated and bought individually.

“We’re not just going to say, ‘Oh, this looks like some neat stuff, let’s buy it and then put it on the border,’” Mr. Chertoff said at a news conference on Tuesday.

Skepticism persists. A total of \$101 million is already available for the program. But on Wednesday, when the House Appropriations Committee moved to approve the Homeland Security Department’s proposed \$32.1 billion budget for 2007, it proposed withholding \$25 million of \$115 million allocated next year for the Secure Border contracting effort until the Administration better defined its plans.

“Unless the department can show us exactly what we’re buying, we won’t fund it,” Representative Rogers said. “We will not fund programs with false expectations.”

**CORRECTION:** A front-page article on Thursday about a federal plan to use contractors to help secure the borders of the United States misstated the amount that Lockheed Martin made in Federal Government sales in 2005. Of \$37.2 billion in sales, more than \$31 billion, not \$6 billion, was in sales to the government.

## New Technology on the Border

The Department of Homeland Security will soon accept bids for a border control system that will use existing and new technologies in a single integrated information system. These five companies are expected to submit bids. Also shown are some existing technologies that could be involved.

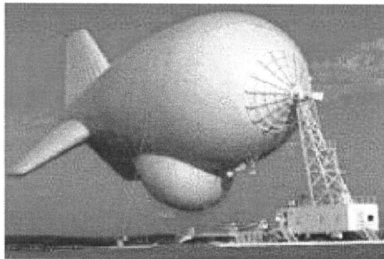
	EMPLOYEES	2005 REVENUE (BILLIONS)
<b>Boeing</b>	153,000	\$54.8
<b>Lockheed Martin</b>	135,000	37.2
<b>Northrop Grumman</b>	125,000	36.7
<b>Raytheon</b>	80,000	21.9
<b>Ericsson</b>	56,000	20.3*

Source: the companies



Northrop Grumman

▲ Northrop Grumman's Global Hawk is an unmanned surveillance plane.



Lockheed Martin

◀ Lockheed Martin's Tethered Aerostat Radar System hangs radar from an anchored balloon.

\*Converted from Swedish Krona

The New York Times

Chairman BOEHLERT. Sorry for the delay, but a vote is in progress on the Floor. I don't think we will be interrupted for several hours now, so we are all set.

I want to welcome everyone to this afternoon's hearing. I especially want to welcome Admiral Cohen, who has been confirmed as Under Secretary right just before the August recess, and who is making his first appearance before our Committee. Admiral, to know us is to love us. We have very high hopes for Admiral Cohen, and we appreciate his efforts to make sure he could attend today's hearing.

I want to remind Admiral Cohen, as we always reminded your predecessor, that this is the Committee that created the Science and Technology Directorate, and we are eager to see it succeed. As we said at the time we were establishing the Department of Homeland Security, "Like the Cold War, the war against terrorism will be won as much in the laboratory as on the battlefield." We cannot afford to let the Directorate flounder.

One of the Directorate's most important areas of responsibility is the subject of today's hearing: border security. There are many aspects of border security, a hot topic right now, but one essential aspect is certainly how to successfully deploy technology to help prevent or thwart illegal border crossings.

My sense is that we haven't done a very good job of that so far. We haven't methodically thought through what technology to develop, how to deploy it, and how to integrate it with the people who will actually be apprehending those trying to cross the border illegally. We haven't come up with a clear, adequately funded plan to conduct the research needed to improve existing technologies and create new ones. And in Congress, we haven't thought comprehensively about border security, instead focusing on massive public works projects, like border fences.

Hopefully, the Secure Border Initiative the Department of Homeland Security is in the process of implementing will start us down a more thoughtful and successful path. This committee certainly will be watching that with great anticipation. And we will especially want to be sure that there is adequate research to ensure that technology can continue to improve.

We have before us today, my colleagues, some of the leading experts in the field, who will give us their views on what the Department, and particularly the Science and Technology Directorate, should be doing to ensure that border security improves. And that, in everyone's mind, is an imperative. Our motto here should be "better living through technology." That doesn't mean technology to the exclusion of people. It means technology that is designed with the users in mind and that is integrated with the Border Patrol.

I am very eager to hear their testimony.

Mr. Gordon.

[The prepared statement of Chairman Boehlert follows:]

PREPARED STATEMENT OF CHAIRMAN SHERWOOD L. BOEHLERT

I want to welcome everyone this afternoon's hearing. I especially want to welcome Admiral Cohen, who was confirmed as Under Secretary right before the August recess and who is making his first appearance before our committee. We have very high hopes for Admiral Cohen, and we appreciate his efforts to make sure he could attend today's hearing.

I want to remind Admiral Cohen, as we always reminded his predecessor, that this is the Committee that created the Science and Technology Directorate, and we are eager to see it succeed. As we said at the time we were establishing the Department of Homeland Security, "Like the cold war, the war against terrorism will be won as much in the laboratory as on the battlefield." We cannot afford to let the Directorate flounder.

One of the Directorate's most important areas of responsibility is the subject of today's hearing, border security. There are many aspects of border security—a hot topic right now—but one essential aspect is certainly how to successfully deploy technology to help prevent or thwart illegal border crossings.

My sense is that we haven't done a very good job of that so far. We haven't methodically thought through what technology to deploy, how to deploy it, and how to integrate it with the people who will actually be apprehending those trying to cross the border illegally. We haven't come up with a clear, adequately funded plan to conduct the research needed to improve existing technologies and create new ones. And in Congress, we haven't thought comprehensively about border security, instead focusing on massive public works projects, like border fences.

Hopefully, the Secure Border Initiative the Department of Homeland Security is in the process of implementing will start us down a more thoughtful and successful path. This committee will certainly be watching that with great anticipation. And we will especially want to be sure that there is adequate research to ensure that technology can continue to improve.

We have before us today some of the leading experts in the field, who will give us their views on what the Department, and particularly the Science and Technology Directorate, should be doing to ensure that border security improves. Our motto here should be "better living through technology." That doesn't mean technology to the exclusion of people. It means technology that is designed with the users in mind and that is integrated with the Border Patrol.

I am very eager to hear their testimony.

Mr. Gordon.

Mr. GORDON. Thank you, Mr. Chairman.

Securing the Nation's borders is one of the main responsibilities of the Department of Homeland Security. Border control is prominent in the current debate on illegal immigration and certainly is a necessary component of the larger issue of defending the country against terrorist attacks.

Technology has an important role to play in border security simply because of the size and nature of the problem. There are thousands of miles of border, much of it remote and rugged, and a limited number of enforcement officers. Technology can provide tools needed to multiply the effectiveness of the Border Patrol officers in the detecting and apprehending illegal intruders at the border.

The question is what detection, surveillance, communication, and computer-aided analysis and control techniques—technologies are appropriate and cost-effective, and how can they be integrated into an effective system for border security.

The Department of Homeland Security's Science and Technology Directorate has developed a resource portfolio that is focused on improving border security. I am particularly interested in hearing how the S&T Directorate will be providing its expertise and advice to assist the Border Patrol in its procurement of the new, integrated border control system called for under the Border Security Initiative.

The Secure Border Initiative is an ambitious undertaking that follows past unsuccessful efforts to integrate and automate sensors and surveillance technologies in a user-friendly system. To succeed this time will require close supervision by DHS. I hope to hear that this S&T Directorate will be closely involved with the establishment of a new border control system and with its evolution as new technology becomes available.

Again, thanks, Mr. Chairman. I want to thank you for holding this hearing, and I look forward to this very distinguished panel discussion.

[The prepared statement of Mr. Gordon follows:]

PREPARED STATEMENT OF REPRESENTATIVE BART GORDON

Securing the Nation's borders is one of the main responsibilities of the Department of Homeland Security.

Border control is prominent in the current debate on illegal immigration and certainly is a necessary component of the larger issue of defending the country against terrorist attacks.

Technology has an important role to play in border security simply because of the size and nature of the problem. There are thousands of miles of border, much of it remote and rugged, and a limited number of enforcement officers.

Technology can provide the tools needed to multiply the effectiveness of the Border Patrol officers in detecting and apprehending illegal intruders at the border.

The question is what detection, surveillance, communication, and computer-aided analysis and control technologies are appropriate and cost-effective, and how can they be integrated into an effective system for border security?

The Department of Homeland Security's Science and Technology Directorate has developed a research portfolio that is focused on improving border security.

I am particularly interested in hearing how the S&T Directorate will be providing its expertise and advice to assist the Border Patrol in its procurement of the new integrated border control system called for under the Secure Border Initiative.

The Secure Border Initiative is an ambitious undertaking that follows past, unsuccessful efforts to integrate and automate sensors and surveillance technologies in a user-friendly system.

To succeed this time will require close supervision by DHS. I hope to hear that the S&T Directorate will be closely involved with the establishment of the new border control system and with its evolution, as new technology becomes available.

Mr. Chairman, I want to thank you for calling this hearing, and I look forward to our discussion with the panel.

Chairman BOEHLERT. Thank you very much.

All of our colleagues have the opportunity to insert opening remarks in the record at this juncture, but let us go right to the panel, as is our modus operandi here, because we want to listen and learn from the distinguished panelists before us.

[The prepared statement of Mr. Costello follows:]

PREPARED STATEMENT OF REPRESENTATIVE JERRY F. COSTELLO

Good morning. I want to thank the witnesses for appearing before our committee to examine the current and potential uses of technology for improving border security and the research needs in this area.

I believe border security and strengthening enforcement at our borders is the first step needed to reform our immigration policies. With my support, Congress has taken action to improve border facility infrastructure and to increase the number of Border Patrol agents and immigration inspectors. In addition to an increased physical presence, officials also need the technological capabilities, such as cameras, sensors, and surveillance equipment, to successfully detect and intercede illegal border activity.

Within the Department of Homeland Security, the Office of Border Patrol (OBP) and the Science and Technology (S&T) Directorate work together to secure the land border of the United States. Specifically, the S&T Directorate assists the OBP in its efforts to implement the Secure Border Initiative, the networked system for detection and response to border incursions. To date, much of the work at S&T has been focused on the actual border, both at ports of entry and between ports of entry. The current technologies being used to secure the border include cameras and Unattended Ground Sensors (UGS) to detect and identify illegal border intrusions. I look forward to hearing from witnesses at the Department of Homeland Security as to why the current technological system is limited in its ability to detect activity and effectively operate.

The number of people entering the country illegally at our borders presents risks to national security. I share the views of the witnesses that there is a not a "one size fits all solution" for border security. I believe we must provide adequate re-

source levels to support all aspects of border security in order to meet the challenges of securing our borders.

I look forward to hearing from our witnesses.

[The prepared statement of Ms. Hooley follows:]

PREPARED STATEMENT OF REPRESENTATIVE DARLENE HOOLEY

I first want to thank the Chairman for holding a hearing today on this very important topic. The issue of illegal immigration is one that evokes passionate responses from most Americans. It is a complicated problem with many proposed solutions. However, while people may disagree on other aspects of the immigration debate, everyone agrees that we must have a secure border.

Securing our border is going to take a multi-pronged approach. We will need to look at the problem comprehensively and address each component: increase the number of Border Patrol officers, place troops on the U.S. border, expand the use of technology to monitor our borders, track those who come into our country on temporary visas, and construct a fence to prevent illegal immigrants from crossing the border.

The focus of today's hearing is on one of these components, expanding the use of technology to monitor our borders and making this technology easier to use for our Border Patrol officers, and I believe that this discussion is not coming a day too early.

We need to be focusing on improving the various forms of border monitoring: cameras, motion detectors, ground sensors, unmanned aerial surveillance, so that they can be used effectively by the Border Patrol to construct a virtual fence across the border.

Much talk has been made of building a fence along the entire border, a length of approximately 2,000 miles. However, limitations in funding and materials, as well as challenges posed by rugged terrain, may make this an impossible task. However, if we can build up our technology to the point that it allows for the continual monitoring of the entire border, we will be able to achieve a balance between the physical presence of a fence and the flexibility that technology allows.

It is one thing for the technology to be developed and deployed. If the people on the ground can't integrate it into their training, it will be wasted. That is why I am heartened to hear many of the witnesses today make the statement that the focus needs to be on what technology works in the field, what technology will make the agents' lives easier, and not on what seems like a good idea in the lab. We will not achieve border security in a lab.

Again, I thank the Chairman for holding this hearing and I thank all of today's witnesses for appearing and giving us much needed insight and expertise.

I yield back the balance of my time.

[The prepared statement of Mr. Davis follows:]

PREPARED STATEMENT OF REPRESENTATIVE LINCOLN DAVIS

Good morning. Thank you, Mr. Chairman and Ranking Member, for the opportunity to discuss border security and the technology that can help secure American borders. Thank you, Witnesses, for your presence today.

Over the past several months a debate about immigration and border security has finally received the attention it deserves. As I have been saying for years now, the influx of illegal immigrants into the United States is a problem that I wish Congress and the Administration would take more seriously. The ease with which people can cross the border should concern every American. I look forward to hearing from the panel today and to learn what technologies exist that can be used to make America safer.

In the wake of 9/11, we must look at every possible solution and I believe an automated system at the border would be a positive step in securing our border. But I also believe that to make sure the taxpayers receive a reliable system that really works, the Department of Homeland Security (DHS) must proceed carefully with this project. DHS needs to be sure that the development process stays on time and, once complete, produces a program that actually works. I would encourage DHS to report back to Congress and update us on the progress of the project.

It is my hope that today's hearing will provide the committee with the information we need to properly solve this important issue.

Thank you, Mr. Chairman.

Chairman BOEHLERT. Admiral Jay M. Cohen, Under Secretary for Science and Technology, U.S. Department of Homeland Security in your maiden appearance before this committee. Admiral, welcome. Mr. Gregory Giddens, Director, Secure Border Initiative Program Executive Office, U.S. Department of Homeland Security. Dr. Greg Pottie, Associate Dean for Research and Physical Resources, School of Engineering and Applied Science, University of California at Los Angeles. Dr. Gervasio Prado, President, SenTech, Incorporated. Mr. G. Dan Tyler, Johns Hopkins University, Applied Physics Laboratory, National Security Technology Division. And Dr. Peter Worch, Independent Consultant, Member of the U.S. Air Force Science Advisory Board.

Thank you all, gentlemen. We really appreciate you being here and serving as resources for this committee.

Now we are going to listen, hopefully learn, and then we will get right to the questions.

Admiral, you are up first.

**STATEMENT OF ADMIRAL JAY M. COHEN, UNDER SECRETARY FOR SCIENCE AND TECHNOLOGY, U.S. DEPARTMENT OF HOMELAND SECURITY; ACCOMPANIED BY MR. GREGORY L. GIDDENS, DIRECTOR, SECURE BORDER INITIATIVE PROGRAM EXECUTIVE OFFICE, U.S. DEPARTMENT OF HOMELAND SECURITY**

Admiral COHEN. Chairman Boehlert, Congressman Gordon, and all of the distinguished Members of this committee, I will tell you, it is a personal honor for me to be here, and I normally don't correct the Chairman, but I did have the honor of testifying before this committee in my prior life as Chief of Naval Research alongside Bob Ballard and other wonderful—

Chairman BOEHLERT. That was a prior life.

Admiral COHEN. It was a prior life.

Chairman BOEHLERT. And I won't talk about it if you won't.

Admiral COHEN. And it is looking pretty good.

But I always like to start out by reminding everybody, and certainly not the Members or the witnesses, but everyone else who is here why we are here. And we just had the commemoration of the fifth anniversary, a very sad event, tragic events of September 11 of 2001. But we would not have a Department of Homeland Security, in my opinion, if it had not been for that heinous attack. And Chairman, you have addressed the enabling legislation for the Department of Homeland Security and the 19 pages that created the S&T Directorate. I think that that was a very brave and inspired move on the part of the Congress and the Administration, and I salute you for that.

I have had the opportunity over the last three weeks to meet with both majority and minority staffs in a very non-partisan, bipartisan way, of six of my seven oversight committees and briefed the new organization, which Secretary Chertoff very kindly approved last Wednesday, and I briefed to the Homeland Security Committee last Thursday, and is now in effect. And that organizational construct, and the processes associated with it, will affect how Greg Giddens and I operate as we go forward. From my prior

life and from Greg's prior life in deepwater, we have already a professional and a personal relationship.

Mr. Chairman, on a personal note, I would like to thank you for your service. I know that—I understand—I don't think I am making that announcement. I understand it is public that you will be leaving, but your leadership and your vision has been incredibly important to the science and technology of this country. We are in crisis. The young kids are turning away in middle school from science and math, and I take that aspect of the enabling legislation my leadership role in encouraging the future generations to pursue the hard topics so that we continue to enjoy the wealth and the freedom that science and technology and innovation has brought us very, very seriously. And in fact, I enjoy that part of my portfolio.

I had prepared remarks, which I would request be made a part of the record.

Chairman BOEHLERT. Without objection, so ordered, as will the complete statements of all our witnesses.

Admiral COHEN. And in light of the distinguished witnesses who are here, the number of witnesses, and the number of Members who I know have questions, and the importance of this topic, I am going to depart even from my short oral statement that I had prepared to share with you the answer, the short answer, to what role does S&T play in enabling the Secure Border Initiative.

Five years ago when Secretary Gordon England had just got to the job as Secretary of the Navy from his General Dynamics, F-16, very technological background, he called me in and he said, "Admiral, before we sit down, tell me what I will get from my basic research investment today in 20 years." I wanted to make a good impression. I didn't want to say, "I don't know." And so I said to the Secretary, "Mr. Secretary, I cannot answer your question unless you let me control one variable." And he said, "Well, Admiral, what is that?" And I said, "Well, Mr. Secretary, I can tell you, beyond a shadow of a doubt, that if we invest nothing today, in 20 years, you will have nothing." At that point, he went from "Admiral" to "Jay." He said, "Sit down. You are right. Let us do business." And we had a wonderful five-year run together.

So the converse of that is I could go through a litany of individual technologies, individual capabilities, but you are very familiar with that. The facts of life are it is S&T, in a spiral development with risk taking, that will initially, and you are going to hear some of the promise and some of the deficiencies, I am sure, from the other witnesses, in making our borders secure. One size doesn't fit all. We have different terrain. We have coverage where we need to see through trees. We have Rocky Mountains. We have desert. We have water. In my organizational construct, we have established a Borders and Maritime Department, which is enduring what I found was a department that was organized for projects, not for enduring disciplines where projects might come and go.

And so in the new organizational construct that the Secretary has approved, to date, there has been a very close alignment. We have got Merv Leavitt here, who worked with Greg's predecessor, of offering, and we have given detailed briefs to Members and to Hill staff and to industry. It has been part of the SBI/BAA, and I have been involved with them the short time I have been on board.



But the facts of life are that, in my opinion, what you will see in terms of the industry who has come forward to give us the initial answers and the initial construct to make our borders secure should be considered either phase one or phase two. That is to kick-start it and that is medium- to low-risk technology solutions, some of which involve manpower, others of which leverage off the incredible investment that we have made in the Department of Defense over many years developing common operational pictures, air, land, and sea sensors, and the weapons and integration, both manned and unmanned.

But in my role as Under Secretary for S&T, you all and the Congress, over many years, have wisely given S&T the authority to take risk. I am the risk component of acquisition. I put millions of dollars at risk in order to prevent putting billions of dollars in acquisition at risk. And we don't have the time today, and it is not the purpose of this hearing, but again, both the majority and minority staff has been fully briefed on this. I am pleased to brief you at any time. But you will see my portfolio now has acquisition enablers. These are the low- to medium-risk technologies across all the venues that Greg must fulfill. This is when you go to Best Buy you have a five mega pixel camera and they are offering an eight mega pixel camera and it is cheaper. That is spiral development. That is low risk. That is insertion of technologies. And by the way, ladies and gentlemen, it has metrics and S&T of cost, schedule, and capability.

But there are other avenues where we take higher risk, and you gave me HSARPA, and you told me to prototype and deploy and test. That is medium- to high-risk. With that comes the probability of failure. But failure is not a negative in science and technology. We learn from those failures. We get it back into the scientific method, and we then come through with the success. Those are two- to five-year prototypical demonstrations. Candidly, they embarrass the status quo. They are meant to embarrass the status quo. And if they work, when they work, we then insert them laterally for leap-ahead capabilities in the SBI or other initiatives.

And then finally, I have basic research. Basic research makes leadership very uncomfortable. It doesn't make this committee uncomfortable, because they understand the value of change in paradigms. They understand that only the Federal Government can make the sustained investment year to year in our laboratories and in our universities to cultivate the discoveries like the small investment in more precise measurement of time in the mid 1970s that gave us global positioning in the 1990s and changed the world, or the transistor that has given us the wireless world today, or  $E=MC^2$  that has given us nuclear power. But the model that exists today, and that has worked for many, many years, is 1,000 flowers are planted in basic research, 100 projects are taken and matured in applied research, two to three prototypes then are developed in advanced technology, and we get the George Foreman grill. The George Foreman grill is the profit-maker. Now every boss I have worked for, on the output side, this is true in industry and in the military and in government, would like the following model: one flower will result in one project, will give us one prototype, and

then give us the George Foreman grill. Oh, that it could be that way.

So the model you will see with me has balanced risk, different times to delivery, but in all cases, it is slave to the customer.

And on specific questions of different technologies, I know Members will ask, and I will be glad to answer that.

And with that, this is a joint statement for Greg and I. I am honored to be here and look forward to your questions, sir.

[The prepared statement of Admiral Cohen and Mr. Giddens follows:]

PREPARED STATEMENT OF JAY M. COHEN AND GREGORY L. GIDDENS

### **Introduction**

Good morning. Chairman Boehlert, Congressman Gordon, and distinguished Members of the Committee, it is a pleasure to be with you today to discuss the progress the Department of Homeland Security is making in the Nation's efforts to secure America's borders. Today, in accordance with the Committee's letter of invitation to testify, we will focus our testimony on how technology can help secure our borders, especially the ways in which science and technology support the Department of Homeland Security's Secure Border Initiative.

Under the Secure Border Initiative, the Science and Technology (S&T) Directorate supports the homeland security missions of U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), United States Coast Guard (USCG), Intelligence and Analysis (I&A), US-VISIT, the Domestic Nuclear Detection Office (DNDO), and others by conducting, stimulating, and enabling research, development, test, evaluation, and timely transition of homeland security capabilities to end-users in the field.

### **Problem Statement**

The challenge of securing the Nation's borders is enormous. Border security is a continuum that begins far beyond the borders of the United States and continues to the interior of our country. It involves the movement of both people and goods and is not successful unless it protects the country from harm and allows lawful trade and immigration. Border security requires a critical blend of tangible resources such as equipment and personnel, along with intangible items such as useful intelligence and strong partnerships with foreign governments. Securing the United States borders is a Presidential priority. In his May 15, 2006, Address to the Nation, President Bush said, "First, the United States must secure its borders. This is a basic responsibility of a sovereign nation. It is also an urgent requirement of our national security. Our objective is straightforward: The border should be open to trade and lawful immigration—and shut to illegal immigrants, as well as criminals, drug dealers, and terrorists. . . . We are launching the most technologically advanced border security initiative in American history. We will construct high-tech fences in urban corridors, and build new patrol roads and barriers in rural areas. We will employ motion sensors, infrared cameras, and unmanned aerial vehicles to prevent illegal crossings. America has the best technology in the world, and we will ensure that the Border Patrol has the technology they need to do their job and secure our border."

To date, much of the work of S&T has been focused on the actual border, both at ports of entry and between ports of entry. The current technologies being used between ports of entry to secure the border include cameras and Unattended Ground Sensors (UGS) to detect and identify illegal border intrusions. Cameras—both daylight and thermal infrared that are installed on poles and other structures along high-volume illegal alien traffic areas of the border—constitute the Remote Video Surveillance (RVS) system. UGS are also used along high-volume illegal alien traffic areas of the border.

The current systems provide a remote detection and identification capability, but with limitations. For example, (1) sensors are not able to differentiate between illegal activity and legitimate events; (2) RVS cameras cannot automatically detect any activity or movement and are limited by weather; (3) sensors are limited by battery power and RVS cameras have infrastructure requirements; and (4) system effectiveness is dependent upon the availability and capability of skilled operations and maintenance personnel.

### Secure Border Initiative

The Secure Border Initiative (SBI) is the Department's approach to lead, integrate, and unify our efforts against cross border and international activities that threaten border security. SBI's approach is that the border is not merely a physical frontier and effectively securing it requires attention to processes that begin far outside the U.S. borders, occur at the border and continue to all regions of the United States. SBI brings a systems approach to meeting this challenge; its mission is to integrate and unify the systems, programs and policies needed to secure the border and enforce our customs and immigration laws. It is a national effort to transform the border security continuum with the objective to disrupt, dismantle and deter all cross-border crime and balance legitimate travel and trade into and out of the United States.

The Science & Technology Directorate is supporting SBI by providing the systems engineering tools, processes, and manpower to ensure that SBI implementation is effective and affordable. In addition to providing systems integration, analysis and engineering support, S&T is developing an integrated systems model. Using modeling & simulation, SBI decision-makers will have the tools to make informed choices for investment strategies and program and policy formulation. The decision makers will understand: 1) where to invest scarce resources (e.g., how many agents and detention beds, how much technology and fencing), 2) the trade-offs associated with their decisions, and 3) where the gaps and risks are. The first phase of this model focuses on the immigration system.

Technology is required that will provide better detection of illegal activity and situational awareness to give us the ability to make near-real-time strategic and tactical decisions regarding our response. These technological capabilities will include new sensors and platforms using manned, unmanned, ground, air, maritime or perhaps even space assets, as well as command and control, decision support aids, robust communications capability, surveillance equipment, and data transfer.

DHS has a requirement for a Common Operating Picture (COP) at the tactical, operational and strategic levels that can seamlessly interface with systems used by other federal, State and local law enforcement partners. Better situational awareness and command and control at the border will facilitate the apprehension and location of individuals and groups who have violated or intend to violate the border. Leveraging emerging technologies and the development of standards, protocols and symbology enables the creation of common user views and information exchange. These common views and information then may be shared with all who operate at the border, independent of the method an agency chooses to implement its specific COP.

S&T is also developing and transitioning technologies critical to SBInet (a component program of SBI) per the request of CBP, which is the executive agent for this program. Specific needs to be addressed to enhance the ability to detect and interdict illegal border activity are:

- Improved technology for detection, classification and interdiction of illegal activity and enhancing the ability to make rapid strategic and tactical response decisions.
- A COP of the border environment for tactical and operational planning with other federal, State and local law enforcement partners.
- Access by DHS personnel, both at and between ports of entry, to the same information at the same time to ensure tight coordination and effective response to all threats.
- Rapid response capabilities to effectively respond to cross-border violations, including technologies that improve situational awareness, command & control, and communications, and provide decision aids for commanders.
- Identification of individuals with hostile intentions toward the United States and its citizenry and secure and accurate communication of that information to those who can expeditiously assess the risk of each person, leading to timely interdiction.
- Technologies that aid in the deterrence and channeling of illegal cross-border activity.
- Technologies that survive rugged handling and extreme environmental and operational conditions with improved reliability and maintainability.
- Technologies that improve voice and data connectivity in remote field areas.

While SBI initially focuses on land border security, it will also address security of the U.S. maritime borders. Specific needs to be addressed to enhance maritime border security are:

- Improved detection, surveillance and reconnaissance capabilities in ports and off shore, using improved platforms, communication networks, and sensors; as well as vessel tracking and anomaly detection.

The goal is to provide agents and officers with a total scene awareness capability that provides a geo-spatially referenced detection, classification and tracking capability along with collaboration and decision-making tools to improve efficiency. Only highly reliable technologies, coupled with a validated and improved concept of operations, will meet the goal. Greater confidence in successful interdiction through advanced technology will lead to force efficiencies and an enhanced ability to prioritize the deployment of intelligence, surveillance, and reconnaissance assets. The effectiveness of any one technology must be balanced against the considerations of its impact on ancillary systems including people, processes, and other deployed technologies.

While SBI is a multi-year development, it looks to S&T to provide technology insertion on a 12–18 month cycle. This insertion into SBI will be in the form of system hardware specifications, software code, supporting documentation, and lessons learned from technology developments and operational tests.

### **Risk**

As stated above, the President has declared that securing our borders is an urgent priority for the national security. Not resolving existing capability gaps directly impacts the Department's overall mission to prevent and deter terrorist attacks. One of the Department's highest priorities is the prevention of the entry of terrorists and their instruments of terror into the United States. S&T addresses this priority by providing technology and processes for detecting, apprehending and prosecuting this illegal activity.

S&T conducts continuing technical evaluation of current and future risks to the borders as a foundation of risk-based decision-making by both the S&T Directorate and the Department of Homeland Security. Additionally, S&T analyzes and distills scientific and operational information to better inform strategic and operational choices made by decision-makers. S&T also conducts technology evaluation and assessment by identifying, developing, testing, and facilitating the transition of advanced homeland security technical capabilities to DHS's operational components and State, local and tribal entities.

S&T also reduces risk by prototyping concepts and technologies and demonstrating their capabilities in an operational environment. We are currently piloting two important capabilities that we call BorderNet and COP/Data Fusion System at the Douglas Border Patrol Station in the Tucson Sector. These systems are force multipliers that decrease officer workload and response time and increase detection and apprehension of illegal border crossers. The results from our prototyping and pilots provide valuable lessons learned for SBI and future systems development. This approach ensures that the most advanced technological solutions are provided to those who protect our borders and that new capabilities are deployed to the field in the shortest possible time and at an affordable cost.

### **S&T Border Security Programs**

The Department of Homeland Security has already put several new technologies in place to aid in securing our borders. Besides BorderNet and the COP/Data Fusion System, we have provided a long range acoustic device (LRAD), which gives Border Patrol agents the ability to communicate with persons at a long distance and we partnered with CBP in deploying Unmanned Aerial Vehicles along the Southern border. We continue to develop and demonstrate new and enhanced capabilities to ensure enhanced security.

The Border Watch Program is a technology-based initiative to develop and transition capabilities that improve the security of our nation's borders. Its goal is to develop and integrate information management and sensor technologies necessary to prevent the entry of terrorists and their instruments of terror, criminals, and illegal aliens through our nation's borders. Border Watch technologies will be integrated into SBI as capabilities mature. Border Watch consists of the following program components:

- Border Detection Grid,
- Border Network (BorderNet),
- Border Protection Pattern Discovery and Prediction, and
- Common Operating Picture (COP).

The Border Detection Grid components will identify available sensors and sensor monitoring capabilities, as well as technology gaps, in order to achieve persistent

electronic surveillance of the U.S./Mexico and U.S./Canada borders. The detection target includes people or groups of people on foot, in vehicles (cars, trucks, and snowmobiles), and in tunnels, vessels, and low-flying aircraft. Sensor and sensor platform technology gaps will be addressed through studies, system design and development, test and evaluation, and/or pilot programs. The program will investigate the potential use of radar, Electro-Optic/Infrared (EO/IR) cameras, unattended ground sensors (UGS), fiber optic tripwires, and other emergent sensors. Sensor platforms will include fixed and mobile towers, vehicles, and manned and unmanned airborne vehicles. Variations in environmental conditions (terrain, weather, marine versus land) and communication availability are expected to drive the solution set for different geographical areas. Department of Defense sensors and sensor systems will be surveyed and adopted, as appropriate.

The Border Network (BorderNet) is a proof-of-concept, prototype development. Capabilities will be developed in spirals with each spiral providing greater capability and user base. BorderNet provides Border Patrol agents with the capability to conduct biometric and biographic queries to identify detainees, in the field and at the time of apprehension. Fusion of multiple data sources provides the agent with actionable intelligence in the form of indications, warning and incident responses recommendations. BorderNet also generates a tactical situation awareness display at the agent and station level, and includes sensor alerts and blue force tracking (BFT) or friendly force ID. Target tracks generated by the COP/Data Fusion System, developed under the Arizona Border Control Initiative, provide overlays on the BorderNet situation awareness display. Field agent connectivity to the various information sources occurs via wireless communications using handheld digital devices and vehicle mounted mobile data computers. Initially, BorderNet accesses biographical data from the Enforcement Case Management System (ENFORCE), the Automated Biometric Identification System (IDENT), and the National Criminal Information Center (NCIC) based on personal data collected from a detainee. NCIC will be accessed through the Arizona Criminal Justice Information Center. Vehicle registration and status information will be obtained through the Arizona Department of Public Safety. Subsequent spirals will connect to the Homeland Security Information Network (HSIN) and the Homeland Security Data Network (HSDN), as well as other local, State and national data sources. Additional features in future spirals may include language translation, knowledge discovery, improved Blue Force Tracking, detainee field enrollment, video transmission, detainee tracking, federated query, and northern border applications.

Border Protection Pattern Discovery and Prediction technologies will provide a new capability to Customs and Border Protection to rapidly fuse disparate information sources to discover geo-spatial, behavioral, and temporal patterns and indicators that provide field agents local scene awareness and actionable intelligence. A prototype will be developed in concert with CBP customers, which will develop patterns and indicators that address topics such as:

- 1) crossing routes and staging areas for cross border smuggling,
- 2) crossing patterns by group—to discover patterns that will help identify the number of organized groups involved and their respective “signatures,”
- 3) crossing patterns by tactic—to discover patterns that will help identify distinctive “signatures” for specific tactics, such as drug smuggling, human smuggling, etc.,
- 4) identifying the links and patterns between illegal border crossing and criminal activity within the U.S., and
- 5) tunnel activity—to discover the likely next tunneling start and end points.

The Common Operating Picture (COP) component will provide the capability to fuse and display at a tactical level the information from select assets within DHS, including but not limited to, Border Patrol Stations, Ports of Entry (POE) and the U.S. Coast Guard. It will be a layered architecture, scalable from the agent/officer in the field to the DHS Operations Center. It will use multi-level security and authentication measures to protect sensitive information and will provide collaborative tools as decision aids. It will use an approved set of standards, including interfaces, services, protocols, and supporting structures. The COP will provide a command and control capability and a tool for inter-agency collaboration. Initially, it will be a sector capability focusing on the southwest border. Subsequent versions will expand to include additional DHS components.

#### **Unmanned Aerial Vehicles (UAVs)**

The Department of Homeland Security has made a great deal of progress in the area of UAVs over the past three years. At the request of Congress, S&T led an

extensive study effort, involving all DHS operational Components, Department of Defense (DOD), Department of Transportation (DOT), Federal Aviation Administration (FAA), and National Aeronautics and Space Administration (NASA) that provided a comprehensive evaluation on the uses of UAVs to support DHS missions. The report was delivered to Congress on time on March 31, 2004, as directed.

Beginning in the summer of 2004, S&T funded two major UAV evaluations as part of DHS' Arizona Border Control Initiative (ABCI). The first period of operational evaluation ran from June through September and utilized the Hermes 450 UAV. The second period of operational evaluation employed the Army's Hunter UAV with operations beginning in November 2004 and continuing through January 2005. The data from these evaluations and other analyses, including an extensive Analysis of Alternatives developed by S&T, led to the establishment of a DHS UAV initial operational capability along the Southern Border.

S&T worked very closely with CBP to acquire DHS's first UAVs to support the initial operational along the Southern Border. The initial DHS/CBP UAV capability, consisting of one UAV system (one aircraft and ground control equipment), became operational in 2005. CBP is the lead for operations and acquisition with S&T providing program and systems integration support. The priority for DHS/CBP UAVs will be to support CBP operations along the border but they will also be used by S&T for evaluation and development of new UAV payloads and systems that will continuously improve DHS UAV mission effectiveness.

Current FAA restrictions on the use of UAVs within United States air space limit their utilization. S&T is working with DOD and FAA to remove current flight restrictions on Border Patrol Southwest border operations through the development of Sense-and-Avoid capability to allow freer use of CBP UAVs in the national air space.

### **Conclusion**

The Department of Homeland Security believes strongly that, only by developing the border security technologies that will be needed five and ten years from now, can we fully ensure that the Nation will be secure for decades to come.

Mr. Chairman, Congressman Gordon, and Members of the Committee, this concludes our prepared statement. With the Committee's permission, we request our formal statement be submitted for the record.

We thank you for the opportunity to appear before this committee and we will be happy to answer any questions you may have.

### **BIOGRAPHY FOR JAY M. COHEN**

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

His early Navy assignments included service on conventional and nuclear submarines. From 1985 to 1988 Cohen commanded USS HYMAN G. RICKOVER (SSN 709) after putting this new ship into commission.

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

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

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

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

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

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

an unprecedented five and a half year assignment as Chief of Naval Research, Rear Admiral Cohen retired on February 1, 2006.

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

#### BIOGRAPHY FOR GREGORY L. GIDDENS

Mr. Gregory L. Giddens, a member of the Senior Executive Service, is the Director for the Secure Border Initiative, Department of Homeland Security. The Secure Border Initiative (SBI) is a broad multi-year initiative that looks at all aspects of border control and immigration enforcement using systems thinking to enhance deterrence, detection, apprehension, detention and removal of illegal aliens, and compliance with immigration laws.

Mr. Giddens entered civil service after completing his undergraduate degree in Electrical Engineering at Georgia Institute of Technology. He earned an MBA from Georgia College and completed Air War College and is a graduate of the advanced Program Manager's course at Defense Systems Management College. Mr. Giddens has also received an MS in National Resource Strategy from the Industrial College of the Armed Forces and has completed the Defense Acquisition University's Senior Acquisition Course.

He began his civil service career at Warner Robins Air Logistics Center where he worked in both depot production and logistics management. He was transferred to Wright-Patterson AFB to work in the Training System Product Group as a program manager for C-17 aircrew and maintenance training. He subsequently served as the Deputy Director and Director for all of the Product Group's Air Mobility Command training programs.

Mr. Giddens was then reassigned to the Air Force's Program Executive Office for Battle Management at the Pentagon where he was an Assistant for Acquisition. He was detailed to the Office of the Assistant Secretary of the Army (Research, Development, and Acquisition) to be the director of the Department of Defense (DOD) Acquisition Workforce Personnel Demonstration Project and jointly reported to the Deputy Under Secretary of Defense for Acquisition Reform. Mr. Giddens attended the Industrial College of the Armed Forces (ICAF) before being assigned to Hanscom AFB as the Program Manager for the Air Force Weather Weapon System. He was then assigned as the Deputy System Program Director for the Airborne Warning and Control Systems (AWACS) at Hanscom AFB. In 2000, Mr. Giddens was selected as the Deputy Assistant Commandant for Acquisition at USCG Headquarters and later that year was selected to be the Deputy Program Executive Officer for the Integrated Deepwater System, United States Coast Guard. In October 2005, Mr. Giddens was selected to lead the Secure Border Initiative (SBI) Program Office for the Department of Homeland Security.

He was a member of Air Force Materiel Command's Top Rung senior executive development program and was an initial selectee into DOD's Defense Leadership and Management Program. Mr. Giddens was selected as a member of the Senior Executive Service in 2000. He was a 2004 recipient of the Presidential Rank Award Distinguished for exceptional long-term accomplishments. He holds certifications in Program Management and Logistics Management.

Chairman BOEHLERT. Thank you very much, Admiral.

I like your style. I couldn't agree more. You are not preaching, but you are talking to the choir, so to speak, here. And one of the reasons why, in a bipartisan basis, this committee is optimistic is that there is a little thing called the American Competitiveness Initiative that is finally getting some attention around this town. The need to invest more in basic research, the need to do a better job of preparing our youngsters in the science and math disciplines, and we take great pride from this committee, being one of the driving forces for that.

So thank you very much.

And Mr. Giddens, thank you.

Mr. Tyler, you are up next.

**STATEMENT OF MR. GORDON DANIEL TYLER, JR., JOHNS HOPKINS UNIVERSITY, APPLIED PHYSICS LABORATORY, NATIONAL SECURITY TECHNOLOGY DIVISION**

Mr. TYLER. Chairman Boehlert, Congressman Gordon, Members of the House Committee on Science, I am Daniel Tyler, head of the National Security Technology Department at Johns Hopkins Applied Physics Lab.

Thank you for this opportunity to share my insights with the Committee on the applicability of a system engineering approach to the daunting challenge of securing our nation's border.

With your permission, I would like to submit my written testimony for the record.

This nation has a rich history of developing massive, complex systems. In the 1950s, three major weapons systems, the strategic triad, were developed and integrated for the global command control and communications network to realize an immense strategic deterrent system of systems, and it has worked for a decade. In the 1960s, as we all know, we went to the Moon with a very impressive application of systems engineering. And not so well known, in the 1970s and 1980s, AT&T seamlessly re-engineered the Nation's entire telecommunications infrastructure, changing the entire system from analog to digital at a cost of \$50 billion without their customers even knowing that it was going on.

We have a lot of experience that is on a scale with the border security challenge, which has addressed very similar issues in the past: major technical issues, a need for research to provide solutions, balancing technology against human resources, developing a concept of operation, policies issues, and involvement of numerous agencies. We have learned a lot about what works and what doesn't work.

The systems engineering methodology has specifically assimilated this past experience into a disciplined approach for solving the problem of massive and complex system development.

How is system engineering defined? It is by a set of phases with associated activities that you have to perform. If the activities aren't there, you are not doing system engineering. Specifically, first phase: concept development. This is where needs, feasibility, requirements, risks are identified and concept definition with detailed planning.

The second phase: engineering development. Here, high-risk mitigation prototyping is done, and very importantly, limited systems are developed and tested to ensure operational suitability. And that is done before the third phase where you go to production, deployment, operations, and effectiveness assessment.

Systems engineering brings rigor and discipline to each of these elements of systems development. The system engineering methodology has been institutionalized in standards and policy by virtually all acknowledged professional technical societies, government agencies for the development of massive complex systems, like the DOD 5000 series.

A reasonable question for this committee to ask is: "In an era of tight budgets and urgent national security imperatives, is system engineering really necessary?" Discipline, rigor, due diligence sounds slow and expensive. Well, picture trying to develop a com-



plex system that is massive in scale, has many interrelated tasks and specific requirements, employs different disciplines, multiple organizations, demanding schedules and budgets, and picture all of that in the absence of a well-defined process.

Without a defined disciplined process, there is no knowledge of progress and no technical control over development until the system is deployed, and then it is too late.

There is a profound difference between activity and progress. It is easy to perform activity. You need a disciplined methodology, like system engineering, to make and measure progress.

We are all familiar with the current border security problem: 10,000 miles of borders, 1.5 million illegal aliens yearly, and according to the GAO, the DHS IG, and other testimony, we have spent about \$5 billion and more than doubled the number of Border Patrol agents over the last decade and haven't realized significant progress.

Secretary Chertoff and other senior government officials have committed to rapid progress on operational control of the borders and, in some reports, is said within two years.

The issue is then how to fix the current situation, understand and solve the technical problems, and make progress expeditiously. In particular, what could we do in a timeframe like two years?

My thesis is, obviously, we need to start by employing a disciplined system engineering methodology. Given that one has done that, this methodology, however, is not prescriptive in implementation. From past experience, we know how important it is that an implementation strategy first ensure adherence to rigid system engineering principles and second, ensure successful execution of each phase. Recognize that the government is ultimately accountable for results and needs to ensure that there is governmental technical competence to understand issues and make decisions. If the government, itself, doesn't have the needed breadth and depth of technical expertise, then it needs to engage third-party organizations to support them.

Organizational roles, in general, are critical: who sets requirements, how the broad technical community is engaged, the existence of independent assessments for every element of the process, the role of the prime contractor. These are critical in determining the success.

So what can be done in two years? Well, we have learned lessons from previous efforts that have attempted to develop complex systems on an urgent basis, to get out of the starting gate rapidly.

First, the existence of major hardware and infrastructure is critical for getting started. We have got ISIS, we have got sensors, and we have got a substantial infrastructure to build on.

Second, open architecture is necessary to allow many organizations to plug-and-play and to enable spiral development upgrade, like the Admiral alluded to. This is included in the SBI solicitation.

Third, major contracts need to be in place, because if they are not, you know this could easily cost you a year or more. And the DHS is about to award the prime contract for SBI.

Fourth, very critical, resolving critical technical issues requires the key technology already be in the pipeline, and that is that it be available now. For this, the SBI strategy needs to encourage

outreach to the broad technical community. There is a lot of technology out there, and I think you are going to hear about some of it in a minute.

I believe that system engineering, properly implemented, will provide, within two years, a very good probability of fielding an operational system on some sections of the U.S. border, which could then demonstrate significant progress in resolving the technical issues. Decisions could then be made for full-scale production and deployment.

This ends my remarks concerning the applicability of system engineering to the daunting challenge of securing our nation's borders.

Again, thank you for this opportunity to address you today.

[The prepared statement of Mr. Tyler follows:]

PREPARED STATEMENT OF GORDON DANIEL TYLER, JR.

## **Applying Systems Engineering Methodology to Help Secure America's Borders**

### **EXECUTIVE SUMMARY**

Significant investments in securing our nation's borders over the last decade have not produced capabilities that met operational expectations. The issue for developing systems and operations that address this massive, technically complex, and time critical challenge is identifying an approach to systems development that has a high likelihood of success. Notably, the collective experience of a rich history of producing complex engineered systems has been assimilated into a methodology with a proven track record of achievements—systems engineering.

The systems engineering methodology provides a disciplined approach to requirements, concepts, planning, prototyping, testing, and other elements of system development and operational deployment. Systems engineering mitigates risk, controls cost, and ensures performance when prompt responses to exigent challenges are needed. In particular, the systems engineering methodology can provide the oversight tool that helps Congress and the Department of Homeland Security (DHS) monitor the progress of the Secure Border Initiative (SBI) with metrics and guide its ultimate success. In times of tight budgets and the need for urgency, as in today's volatile national security environment, it is tempting to abandon the rigor and discipline of systems engineering in favor of ways of doing business that appear less expensive and more rapid. Repeatedly, these other formulas have fallen short of the mark, producing activity without real progress, while systems engineering has a history of delivering performance, on budget and schedule. The systems engineering methodology has been institutionalized in standards and policy by virtually all acknowledged professional technical societies and Government agencies for the development of massive, complex systems.

While adopting the systems engineering methodology is essential for engineering large-scale, highly complex systems, special attention must be paid to employing an implementation strategy that ensures adherence to the principles of systems engineering, and successful execution of its various phases. The Government is ultimately accountable for results, and must ensure adequate Government technical competence is brought to bear for understanding issues and making decisions. When needed, especially with complex problems, the Government may engage 3rd party organizations to support them in this capacity.

The systems engineering discipline is not prescriptive regarding implementation strategies, and there are assorted successful examples. The Navy's management of the Polaris Program, initiated in 1956, included a technical staff of 450 in the Program Office fully dedicated to the development and production of the Polaris system. The Navy's sonar development program started in 1996, relies heavily on the broad technical community, operating in peer working groups, for concept identification, feasibility assessment, prototyping, and especially for validation and testing at every phase of the systems engineering methodology. For each system development activity, specific consideration should be given to the appropriate roles for Government agencies and Government laboratories, prime contractors, associate contractors,

Federally Funded Research and Development Centers (FFRDCs), University Affiliated Research Centers (UARCs), academia, nonprofits, and small or minority owned businesses. In architecting an implementation strategy, especially in defining the roles of prime contractors, note that history has shown that the strength of this nation for addressing massive, complex challenges is the wealth of available domain expertise, and the power of competitive forces.

The systems engineering methodology is flexible. It can be tailored to emphasize risk mitigation, incremental improvement, capability-based acquisition, as well as milestone- or cost-driven development. Given the urgency of the current national security environment, a particularly relevant issue is how to make real and rapid progress: How much can we improve operational effectiveness and how long will it take? The Secure Border Initiative program component (SBInet) has existing advantages for getting underway quickly: i.e., current Integrated Surveillance Intelligence System (ISIS) sensors, video surveillance, and infrastructure; an imminent Indefinite Delivery, Indefinite Quantity (IDIQ) prime contract; very promising technology in the pipeline; and data that can be used to address technical issues and support technology development. The program now needs to adopt a disciplined systems engineering methodology, and demonstrate a successful, limited-deployment operational system, conceivably within two years, before going into full production and deployment.

#### MAIN TESTIMONY

Chairman Boehlert, Congressman Gordon, and Members of the House Committee on Science. I am G. Daniel Tyler, Head of the National Security Technology Department at The Johns Hopkins University Applied Physics Laboratory (JHU/APL). Thank you for the opportunity to address you today on *“How Can Technologies Help Secure Our Borders?”* The Applied Physics Laboratory has been a long-term, trusted strategic partner with the Federal Government, in particular the Department of Defense (DOD) and the Navy, for providing critical contributions to our nation’s most pressing national security challenges. I am pleased to be able to share our insights with the Committee as to the applicability of a disciplined systems engineering approach to the elusive challenge of securing our nation’s borders.

#### PREFACE

What is systems engineering? Other areas of engineering (e.g., electrical, mechanical, chemical, etc.) are considered “disciplines” in that they are fields of study, and spheres of domain expertise. More prescriptive are “processes” that define the steps or tasks to be executed conducting to an end. Systems engineering is a discipline, less regimented than a well-defined process, best described as a methodology. In particular, systems engineering is defined by a set of phases with associated activities that must be performed. If these activities are absent, then the systems engineering methodology is not being followed.

The traditional systems engineering methodology for designing, developing, and deploying major systems is usually described in three phases:

1. **Concept Development**—needs, feasibility, requirements, concept definition, and detailed planning
2. **Engineering Development**—prototyping and testing for operational use
3. **Post-Development**—production, deployment, operations, effectiveness assessment

In times of tight budgets and urgency driven by a volatile national security environment, it is tempting to look for ways of acquiring needed capabilities that appear to be less expensive and more rapid. A reasonable question is: Are the rigor and discipline of the systems engineering process really necessary for developing appreciably complex systems? The foreman on a job site constructing a new home may be able to manage the entire construction process, plan, and schedule in his head, and single-handedly coordinate contractors. In contrast, consider the program manager responsible for the construction of an aircraft carrier, clearly dealing with more complexity than a single human brain can accommodate at once. Major system development efforts are usually complex, need to support specified user requirements, are composed of many interrelated tasks, involve several different disciplines, are performed by multiple organizations, have a specific schedule and budget, and may require years to complete. The human brain can conceptualize and manage small development activities, but larger efforts demand a disciplined process. The issue is identifying a process that, in some sense, optimizes the probability of success for developing a complex system, while mitigating risk and controlling cost and schedule.

### SYSTEMS ENGINEERING AND SBI/SBINET

The Secure Border Initiative (SBI) and SBInet are large, complex system solutions to an immediate critical challenge facing our nation. Properly applying the systems engineering methodology to the challenge of securing our borders makes sense because:

- A disciplined systems engineering approach can develop and deliver massive, complex systems with a proven high rate of success.
- Previous approaches to securing our country's borders have not met operational expectations, according to the GAO and other testimony.
- The systems engineering methodology provides the right tools for oversight and success: i.e., requirements, metrics, planning, prototyping, testing, and deployment for operational use.
- Both the public and private technical and acquisition communities have embraced systems engineering and shown its effectiveness for controlling performance, schedules, and cost.
- Organizationally, implementing a systems engineering process properly requires appropriate roles for the Government and Government laboratories, prime contractors, associate contractors, independent laboratories, and academia.

There is a profound difference between mere activity and progress. There are easy ways to simply take action, but systems engineering is the way to ensure progress. Applying a disciplined, deliberate systems engineering methodology to the border security challenge provides a proven development process for controlling performance, budgets, and schedules. Moreover, the systems engineering methodology provides an oversight tool to help Congress and the Department of Homeland Security (DHS) monitor the progress of SBInet with metrics and therefore guide its ultimate success.

### DELIVERING MASSIVE, COMPLEX SYSTEMS WITH PROVEN SUCCESS

The Nation has a rich history of relevant experience in successfully developing massive, engineered systems:

- Investing \$50B in converting the Nation's telecommunications infrastructure from analog to digital;
- Going to the Moon in less than a decade;
- Integrating three major and diverse weapons systems from two services with global command, control, and communications, and providing interfaces with the Intelligence Community and the White House to realize a Strategic Deterrence system of systems.

We even have experience, similar to the border security challenge, in more than one mission area, for providing surveillance over large geographic areas and supplying cuing for follow-on forces. Between 1950 and 1985, for example, in support of the Anti-Submarine Warfare mission, the Navy's surveillance community successfully produced a system that provided surveillance and cuing for 12,000,000 square nautical miles of ocean, including 20 worldwide Naval Facilities for shore-based processing and analysis and thousands of Navy and civilian support personnel.<sup>1</sup>

Previous efforts have tackled the same types of issues facing the border security challenge. Historically, in the development of large and complex systems it has been the norm that at the outset, designers could readily identify many technical issues to address; however, there have also been "unknown unknowns" that surfaced only during the phases of development and testing. Critical system elements may have been nonexistent and required rapid directed research to produce seemingly miraculous results. Prior system development efforts necessarily had to deal with the problem of balancing technology against human resources. Concepts of Operations (CONOPS) had to be developed. Often, the total solution for a successful mission required addressing a myriad of issues under the jurisdiction of multiple agencies. However, lessons have been learned in the design, development, and deployment of these major systems that clarified what processes, management structures, and assignment of organizational roles and responsibilities were most effective for realizing acceptable system performance, controlling cost, and attaining operational capability as rapidly as possible. The modern discipline of systems engineering has assimilated this collective experience into a proven process.

<sup>1</sup>Edward C. Whitman, "The Secret Weapon of Undersea Surveillance," *Undersea Warfare*, Winter 2005, Vol. 7, No. 2.

An example that Congress is familiar with is the Navy's Fleet Ballistic Missile (FBM) Program. This program has been so widely recognized and studied as a DOD acquisition success story, that in 1990, the General Accounting Office (GAO) produced a report<sup>2</sup> for Congress to clarify what made this program so successful. The Navy initiated the program in December, 1956, when it began development of a submarine-launched ballistic missile (Polaris) under a new organization, the Special Projects Office [now called Strategic Systems Programs (SSP)]. SSP was given complete authority to design, develop, produce, and support the FBM system.

“Three major components—a solid propellant fuel, a small high yield nuclear warhead, and an accurate guidance/fire control/navigation system—needed major technical breakthroughs at the time that the Polaris project was authorized. A nuclear attack submarine also had to be modified to carry and launch the missiles while submerged.”

The first Plans and Programs Director of SSP made the analogy that,

“. . . building and fielding Polaris was similar to building the entire automobile industry. That is, not only did the first automobile have to be developed but also the internal combustion engine, tires, the oil industry, gas stations, and driver training before the automobile's feasibility was known.”<sup>3</sup>

Amazingly, the technical problems were solved, and “the Polaris program went from concept development to deployment in three years—three years ahead of the original schedule.” Between 1956 and 1990, about \$74B was appropriated for FBM program acquisition. Three classes of FBM submarines have been deployed (59 hulls), and six generations of missiles (more than 3,000 missiles). A key finding of the GAO study is the commitment over the entire life cycle of the system, for the following:

“(1) concept exploration/definition, (2) concept demonstration/validation, (3) full-scale development and low rate initial production, (4) full-rate production and initial deployment, and (5) operations support”

(coincidentally, all of the components of the systems engineering paradigm).

Importantly, SSP's implementation of systems engineering relies strongly on independent test and evaluation in all phases of the process.

The message from the FBM program and history is clear. We have engineered many large, complex, technology-based systems, comparable in scale to the challenge of securing our borders. We have learned a lot from employing different development processes and from our successes and failures. We have developed a sense for what works and what does not work. Although there is no guaranteed “cook-book” approach to developing massively complex systems, there is a high correlation of success with employing a disciplined systems engineering development process.

#### **THE CURRENT INABILITY TO MEET OPERATIONAL EXPECTATIONS**

Some of the challenges in securing our nation's borders are obvious: 10,000 miles<sup>4</sup> of diverse land borders and coastline and 1.5 million illegal aliens yearly<sup>5</sup> present formidable impediments to gaining control of our borders. Solutions whose core attribute consists of employing large quantities of sophisticated technology and significant human resources (e.g., Border Patrol agents), may have an intuitive appeal, but this is in the absence of a deeper understanding of more subtle, qualitative, and complex performance drivers. This appears to be the case in the recent history of attempts to improve border security. Starting in the 1970s and 1980s, the Office of Border Patrol (OBP) introduced acoustic and magnetic sensors and video cameras to assist agents in remotely detecting illegal aliens entering the United States. In 1998, the Immigration and Naturalization Service (INS) formally established the Integrated Surveillance Intelligence System (ISIS) comprising more than 11,000 seismic and magnetic sensors, 255 operational remote video surveillance (RVS) systems, and the Integrated Computer Assisted Detection (ICAD) system. In 2003, OBP recognized the need to further improve border surveillance and remote assessment and monitoring technology, due to poor program management, technology failures, and

<sup>2</sup>United States General Accounting Office, “Fleet Ballistic Missile Program,” GAO/NSIAD-90-160, 9-6-1990.

<sup>3</sup>Ibid.

<sup>4</sup>Does not include Alaska or Hawaii.

<sup>5</sup>Source: “Estimates of the Unauthorized Migrant Population for States Based on the March 2005 CPS,” Pew Hispanic Data Center Fact Sheet, 26 April 2006. Estimate is based on U.S. Census Data; estimate of 1.5M illegal aliens per year since 2000.

poor operational results for ISIS.<sup>6</sup> Therefore, OBP began developing the America's Shield Initiative (ASI). This initiative included additional surveillance structures, upgraded and expanded surveillance equipment, and significantly enhanced detection and monitoring capabilities. According to OBP, the expanded use of surveillance technologies was viewed as an effective force-multiplier. In an April 7, 2006 hearing of the House Appropriations Subcommittee on Homeland Security, the opening statement of Chairman Harold Rogers summarized real progress over this time period:

“Since 1995, we have quadrupled spending on border security, from \$1.2B to \$4.7B, and more than doubled the number of Border Patrol Agents from 5,000 to 12,381; yet during that same time period, the number of illegal immigrants in the U.S. has jumped from five million to over 11 million.”

We have applied significant resources, financial and human, to this challenge and still have limited control over our borders. If we cannot deter or detect and stop illegal immigration, then we have no ability to stop terrorists using the same methods from infiltrating the U.S.

The massive scope of the border security issue deriving from large geographic areas and high volumes of illegal alien activity, is also technically challenging, operationally complex, and programmatically and contractually demanding for Government managers. In addition, it possesses multiple dimensions that interact in complicated ways, necessitating tradeoffs. In a December 2005 report,<sup>7</sup> the Office of the Inspector General (OIG) of the DHS reviewed existing remote surveillance technology employed along U.S. land borders. This report contains valuable insights into some of the difficulties associated with attempts to exploit technology as a major contributor to border security operations. The following findings, organized by category, are from the OIG report's Executive Summary, which highlights technical, system, operational, and programmatic/contractual challenges:

**Technical Challenges:**

- “Remote video surveillance cameras do not have detection capability regardless of whether they are used in conjunction with sensors.”
- “Current sensors cannot differentiate between illegal alien activity and incidental activations caused by animals, seismic activity, or weather. . . .”<sup>8</sup>

**System Challenges:**

- “Integrated Surveillance Intelligence System (ISIS) components are not fully integrated: e.g., when a sensor is activated, a camera does not automatically pan in the direction of the activated sensor.”
- “Data entered into OBP's primary source of ISIS information, the ICAD system, is incomplete, and not consistently recorded by OBP sectors.”

**Operational Challenges:**

- “. . . OBP agents are often dispatched to false alarms.”
- “OBP was unable to quantify force multiplication benefits of remote surveillance technology.”
- “ISIS remote surveillance technology yielded few apprehensions as a percentage of detection, resulted in needless investigations of legitimate activity, and consumed valuable staff time to perform video analysis or investigate sensor alerts.”

**Programmatic/Contractual Challenges:**

- “Deficiencies in the contract management and processes used to install ISIS equipment have resulted in more than \$37 Million in DHS funds remaining in General Services Administration (GSA) accounts; delays in installing, testing, and bringing on-line RVS sites that are operational; and 168 incomplete RVS camera sites.”

<sup>6</sup>Office of the Inspector General, DHS, “A Review of Remote Surveillance Technology Along U.S. Land Borders,” OIG-06-15, December 2005.

<sup>7</sup>Ibid.

<sup>8</sup>Nonsensor alerts along the southwest border during a five-day period generated by camera detections, vehicle stops, officer observations, other agency observations, citizen observation, air observation, or some other source totaled 780 alerts, resulting in 382 apprehensions. Over the same period, ISIS sensors generated 29,710 alerts, resulting in 252 apprehensions.

The OIG report concludes with helpful recommendations for addressing some of the identified deficiencies in the existing system and development process.<sup>9</sup> Justifiably, the OIG did not accept the charter, nor claim subject matter expertise for actually determining how an operational system could be engineered to provide adequate performance for meeting border security requirements. That is:

1. The OIG recommendations did not attempt to address specific technical solutions to problems (e.g., false alarm rates).
2. Following the OIG recommendations may not be sufficient to produce a fully functional capability.
3. The OIG report was intentionally limited in scope (i.e., remote surveillance technology) and did not incorporate other critical elements of the problem.

Therefore, while the OIG addressed certain issues that stayed within the scope of its tasking, *a disciplined systems engineering review of ISIS/ASI would have provided a better baseline upon which to build a superior follow-on system—SBI/SBInet—to position it for success.*

The DHS OIG looked specifically at remote surveillance technology. While solving the technical problems here will clearly be a major move forward, other dimensions to this challenge need to be addressed before a viable concept can be realized for securing the borders. Importantly, these other elements interact, require interfaces, and necessitate tradeoffs that impact responsibilities and resource requirements across the boundaries of multiple agencies.

#### **MULTIPLE DIMENSIONS OF THE BORDER SECURITY CHALLENGE**

Fundamental tradeoffs need to be made between technology and human resources. Technology is easily envisioned as a force multiplier, but the experience with the current ISIS system testifies to the pitfalls in ignoring the technical details. The high false alarm rates associated with the currently deployed seismic/acoustic sensors drain the supply of additional OBP agents assigned to Border Patrol operations, producing a net decrease in operational performance. Synergism between technology and human resources needs to be carefully engineered, with a thorough understanding of the capabilities, limitations, and demands of the technology. In fact, technical solutions may burden human resources by affecting operations negatively and by requiring human interaction in controlling, operating, maintaining, and repairing technology and analyzing and communicating its products.<sup>10</sup> Significantly, the marriage between technology and humans is not adequately defined until a CONOPS is developed that thoroughly defines how the technology and human resources will be jointly used operationally.

In addition to the technical, operational, and programmatic challenges, consider the impact of U.S. immigration policy on concepts for securing the borders. Non-restrictive policy may focus attention on verification and inspection at ports of entry (POE). Conversely, restrictive policy will probably result in large numbers of illegal aliens attempting to enter between ports of entry (BPOE)—in deserts, forests, and mountainous regions—keeping attention on surveillance systems, Border Patrol operations, and detention facilities. Decision-makers need to be fully cognizant of the impact of policy on the viability, cost, and schedule of any solution to this problem. Moreover, system developers must recognize that policy is a major driver in system design.

The threat itself is another dimension to the problem that must also be taken into account. The threat is not monolithic: It is composed of illegal immigration for economic and/or political reasons; trafficking in drugs, weapons, contraband, and human beings; and terrorism. The tactics employed may be different, the determination and persistence uneven, the level of desperation unpredictable, and the resources (financial, weapons) biased in favor of the most dangerous elements. We must fully account for the threat's ability to respond to our efforts and actively pursue countermeasures. As an OBP official observed, "Once illegal aliens learn where RVS camera sites are located, they may choose not to cross at those locations."

The troublesome part of the problem is that many agencies are involved, at the border and in the "interior" operations. Federal and State agencies can provide crit-

<sup>9</sup>The DHS OIG report spells out seven recommendations dealing with system integration, processes for handling data, performance measures, contracting issues, site selection, the use of Government and private structures, and mobile surveillance platforms.

<sup>10</sup>ISIS operations require three types of personnel: law enforcement communications assistants for monitoring cameras and ICAD terminals and providing radio and dispatch support to field agents; OBP agents to respond to alerts, install and maintain cameras, and monitor sector RVS cameras; and CBP Office of Information Technology specialists for on-site repairs to sensors and cameras.

ical intelligence information and actively participate in border security operations. In addition, decisions made at the border will impact federal, State, and local agencies dealing with immigrant monitoring, verification of status and employment, and apprehension.

We can design a system focusing on technology and catching people at the border, or we can take a more holistic approach to the problems of illegal immigration, trafficking, and terrorism. Working all dimensions to the border security challenge collectively requires system engineering at multiple levels. A good example of this was the revolution in the telecommunications industry during the 1970s and 1980s. AT&T developed a three-tiered systems engineering approach for converting the Nation's telecommunications infrastructure from analog to digital:

1. Tier 1, the highest level, engineered the overall network, including local access, central switching, routing, long haul transmission, and other requirements.
2. Tier 2 system engineered each of the Tier 1 components addressing capacity, reliability, calling patterns, service views (e.g., 800/900 number services, calling cards).
3. Tier 3 system engineered specific technical systems (e.g., frame relay switches, fiber-optic networks).

A study of the AT&T experience, which required \$5013 over two decades, shows how multi-tiered systems engineering can be applied to the border security challenge: taking into account tradeoffs between humans and technology; addressing operations at ports of entry, between ports of entry, and in the interior; and devising a high-level construct encompassing roles for federal, State, and local agencies.

In summary, our attempts to date for improving border security through the exploitation of technology combined with operations have not met expectations or success. The problem may seem daunting—highly variable and massive in extent geographically, technically challenging, operationally complex, and possessing multiple dimensions that require sophisticated planning, coordination, and interfacing across organizational boundaries. Accepting that there are significant shortfalls in our current response to border security, as recognized by both Congress and DHS, the issue is where to go from here.

### **THE SYSTEMS ENGINEERING METHODOLOGY APPLIED TO BORDER SECURITY**

Numerous paradigms exist for developing, producing, and operationally deploying technology and systems. Consider the “Linear Model” championed by great scientists like Vannevar Bush<sup>11</sup> and famous leaders like Franklin Roosevelt. This model starts with basic research then follows a progression through applied research, development, up through production and operations. This model pursues “discovery” first, then looks for application. It is a model used very successfully by many academic organizations, the Department of Energy (DOE) National Labs, and the services’ research laboratories [e.g., the Office of Naval Research (ONR)]. When Government funds are used for the linear model, it is not necessarily known beforehand what will be discovered (if anything) or what utility any discovery might produce. At the other extreme, the Government can procure technology and systems for which there are no unknowns that need to be resolved, and which require only straightforward engineering to design and produce. Because national security involves known problems that need to be solved, with issues that frequently tend to be technically complex and massive in scale; because there has been an explosive growth in technology since the second half of the twentieth century; and because there is a continuing need to advance technology to pace the threat, neither the linear model nor straightforward procurement can successfully address many of the Nation's security challenges. The systems engineering method was specifically developed to meet this need.

Kossiakoff and Sweet<sup>12</sup> define the characteristics of a system whose development, test, and application require the practice of systems engineering:

1. Is an engineered product and hence satisfies a specified need,
2. Consists of diverse components that have intricate relationships with one another and hence is multi-disciplinary and relatively complex,

<sup>11</sup>Vannevar Bush, “Science, The Endless Frontier,” *Time Magazine*, April 3, 1944.

<sup>12</sup>Alexander Kossiakoff and William N. Sweet, *Systems Engineering, Principles and Practice*, John Wiley and Sons, Inc., 2003.



3. Uses advanced technology in ways that are central to the performance of its primary functions and hence involves development risk and often relatively high cost.

The development of a system for securing the Nation's borders easily meets these criteria and logically needs the deliberate application of a disciplined systems engineering methodology to succeed.

The systems engineering paradigm described here is based primarily on the text of Kossiakoff and Sweet.<sup>13</sup> While specific excerpts from this reference are quoted, the majority of ideas, concepts, and examples in this section are liberally based on material from the reference. Implications of the systems engineering methodology for the challenge of securing the Nation's borders, and examples based on existing deployed systems (ISIS/ASI), are provided in italics.

As mentioned in the Preface, systems engineering is usually partitioned into three phases:

1. **Concept Development**—needs, feasibility, requirement, concept definition, detailed planning
2. **Engineering Development**—prototyping and testing for operational use
3. **Post-Development**—production, deployment, operations, effectiveness assessment

**Concept Development Phase.** This phase first establishes a need for the system and ensures that it is technically and economically feasible. Establishing the need typically requires analysis, modeling, and simulation for both the system and its operational employment. Technical feasibility generally requires that supporting science and technology necessary for developing viable system concepts are "in the pipeline." If a gap exists in a critical technology area, directed Science and Technology (S&T) may be needed, which increases the risk in system development. The second part of this phase explores potential system concepts and then formulates a formal set of requirements the system must meet. *The importance of requirements is simply stated: If requirements are minimal, it will be easy for any system to meet them.* Allowing contractors to establish requirements to encourage innovation and shorten acquisition cycles under OSD's acquisition reform did not work well.<sup>14</sup> Last, a viable system concept is selected, its functional characteristics defined, and a detailed plan is developed for the subsequent stages of engineering, production, and operational deployment of the system.

*Requirements for securing the border need to be defined for the combined use of technology and Border Patrol agents. Choice of an appropriate metric is important: It affects system design, and its sensitivities may be subtle. For example, consider as metrics the success rate for illegal entry, the absolute number of illegal entries in a given period, and the number of illegal immigrants in the U.S. at any given time. Improving border security will have a direct, positive impact on all three metrics. Improved security may additionally have a deterrent effect on those considering attempting to enter illegally. The first metric is not sensitive to this deterrence, while the last two are. Additionally, observe that the first two metrics are principally under the control of the system designer, while the last metric is heavily dependent upon other federal, state, and local agencies.*

*Once a Concept of Operations is developed for interfacing humans with technology, requirements can be established for communications and technology in the field: e.g., Personal Digital Assistants (PDAs), decision aids, and reachback (e.g., terrorist databases from the National Counterterrorism Center).*

*Numerous other technical issues arise in the concept development phase. Examples include: the existence of models, simulations, and analytical techniques for addressing the combined performance of systems and Border Patrol agents; the detection performance for sensors and cameras; system false alarm rates; potential Unmanned Aerial Vehicle (UAV) sensor contributions; the impact of law enforcement human intelligence (HUMINT) on cuing, detection, and response.*

**Engineering Development Phase.** This phase corresponds to the process of engineering the system to perform the functions specified in the system concept defined in the first phase. First, any new technology the selected system concept requires must be developed, and its capability to meet requirements must be validated. Second, a prototype is developed that satisfies requirements on performance,

<sup>13</sup> Ibid.

<sup>14</sup> Michael W. Wynne, Under Secretary of Defense (AT&L), "Policy for Systems Engineering in DOD," February 20, 2004.

reliability, maintainability, and safety. Third, the system is engineered for production and operational use, and its operational suitability is demonstrated. These last two stages require engineering development and design, defining and managing interfaces, developing test plans, and determining how discrepancies in system performance uncovered during test and evaluation should be rectified.

*Assuming that valid system requirements for border security and a system concept exist [while noting that the SBInet Request for Proposals (RFP) provided minimal requirements], gaps in critical technologies must be identified and addressed. Using the system concept for the current operational system (ISIS/ASI) as an example, critical missing technologies may include: false alarm reduction algorithms; automation/semi-automation of the detection process for sensors and video, including "Bell Ringers" that alert operators and Large Margin Classifiers; algorithms for fusing acoustic, magnetic, video, and other sensor information; creation of a common tactical scene; tactical decision aids; Unmanned Aerial Vehicle (UAV) technologies including sensors, Automatic Target Recognition, autonomous operations; integrated C<sup>2</sup>, man/machine interface, and law enforcement and intelligence interfaces.*

*Prototyping of individual system elements must be completed and performance validated through testing (e.g., are we really achieving acceptable false alarm rates from sensors?). A scaled prototype of an integrated system must be developed and tested in an operational environment with Border Patrol agents. Full-scale production and deployment should begin only after any discrepancies are resolved.*

**Post Development Phase.** This last phase includes production, operational deployment, in-service support and engineering, and continuing assessment of the operational effectiveness of the system, with feedback to prior phases and iterations as required to maintain/improve system effectiveness ("Build-Test-Build").

*Full-scale production of complex systems for providing border security is appropriate only after the system successfully undergoes operational test and evaluation. Once deployed, it is critical to determine the operational effectiveness of the system, establishing whether the system is meeting its operational requirements, and understanding discrepancies and actions needed to be taken. There is a potential wealth of information from a deployed system for addressing deficiencies and improving system effectiveness: e.g., recorded sensor data; captured performance for the combination of the analyst and system for detecting targets and eliminating false alarms; empirical understanding of the utility of command, control, and communications; the success of the marriage between technology and Bureau of Customs and Border Protection (CBP) operations. Given the lack of maturity of this mission area and the associated absence of subject matter expertise in critical technical areas (e.g., target signatures, false alarm mechanisms for sensors), a "Spiral Development" process of system capabilities could be entertained that would exploit the continually improving knowledge in this domain.*

### **Systems Engineering a Complex System with Predecessor Technology**

Descriptions of systems engineering usually appear to imply that a new system is being designed from scratch, with no regard for current systems that may have applicability. Existing systems will affect development of a replacement system in three ways:

1. Deficiencies of the existing system are recognized and may represent the driving force for a new design.
2. If deficiencies are not as serious as to make the current system worthless, the existing overall concept and functional architecture may constitute a good starting point for exploring alternatives.
3. Relevant portions of existing systems may be used in new designs, reducing risk and saving costs.

Given the significant investment in the current ISIS and ASI systems (including seismic and magnetic sensors, RYS, and ICAD), it is desirable to seriously entertain the employment of these assets in future system designs.

### **PEDIGREE OF THE SYSTEMS ENGINEERING METHODOLOGY FOR CONTROLLING PERFORMANCE, SCHEDULES, AND COST**

The systems engineering method basically consists of defining requirements, translating those requirements into functions (actions, tasks) that the system must

accomplish to meet the requirements, selecting a preferred system design that is believed to accomplish those functions, then iterating and validating the system design through successive testing. If one views each iteration as a “hypothesis” that this design will optimally meet requirements, with associated “hypothesis testing” to verify this assumption, then “the systems engineering method can be thought of as the systematic application of the scientific method to the engineering of a complex system.”<sup>15</sup> This is certainly not a rigorous proof that system engineering is an optimal method for developing complex systems, but it is a compelling rationale that appeals to the same logic that supports the scientific method for pursuing research. Would a legitimate researcher pursue discovery and invention without using the scientific method?

The systems engineering methodology has gained acceptance in virtually all acknowledged professional technical communities for the development of massive, complex systems. Figure 1, adapted from Kossiakoff and Sweet, shows the relationship between the elements of systems engineering as described here, to other prominent systems engineering life cycle models.

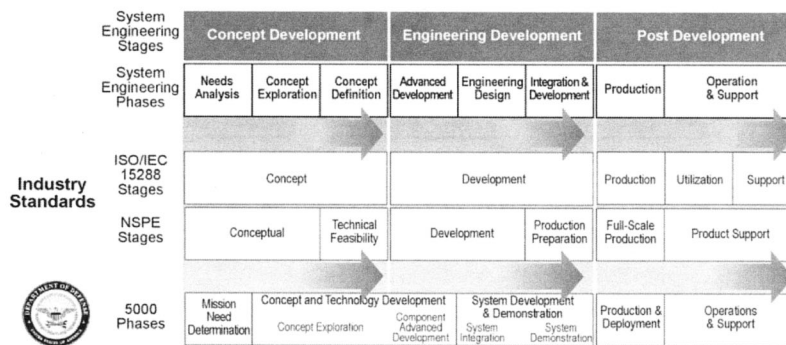


Figure 1 Comparison of system life cycle models.

Consider the extensive experience realized by the United States during the twentieth century in developing large-scale, complex military systems (ships, tanks, planes, command and control). The Department of Defense developed the DOD 5000 series of directives as a set of comprehensive system acquisition guidelines, specifically to

“ . . . manage the risks in the application of advanced technology, and to minimize costly technical or management failures. . . . In 2001, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) issued the result of several years of effort—a systems engineering standard designated ISO/IEC 15288. This model is likely to become institutionalized in U.S. industry to replace previous standards.”<sup>16</sup>

As an additional example, the National Society of Professional Engineers adopted a model “mainly directed to the development of new products, usually resulting from technological advances.”<sup>17</sup> One can simply Google “Systems Engineering” and the references will testify to the near-universal acceptance of this process for the development of complex systems. Systems engineering, arguably, has been shown to be the most effective process for the development and operational deployment of complex systems. Although a disciplined approach and technical due diligence are central to the process, systems engineering has a proven track record for realizing progress as rapidly as possible.

During the 1990s, DOD experimented with acquisition reform, looking for ways to streamline the acquisition process, decrease the development time line, and provide more latitude for innovation to contractors. “Shortcuts” were taken in the belief that less “rigor” and “discipline” may be necessary in the acquisition process. By the turn of the century, there was significantly more insight into what worked and what did not work. In 2004, the Under Secretary of Defense for Acquisition, Technology,

<sup>15</sup> Ibid.

<sup>16</sup> Ibid.

<sup>17</sup> Ibid.

and Logistics [USD (AT&L)] promulgated a new policy<sup>18</sup> mandating the use of a robust systems engineering approach for “all programs responding to a capabilities or requirements document, regardless of acquisition category.” In the words of USD (AT&L):

“Application of a rigorous systems engineering discipline is paramount to the Department’s ability to meet the challenge of developing and maintaining needed war fighting capability. . . Systems engineering provides the integrating technical processes to define and balance system performance, cost, schedule, and risk.”

Guidance for implementation followed.<sup>19</sup>

### **CONSIDERATIONS FOR IMPLEMENTING THE SYSTEMS ENGINEERING METHODOLOGY**

Equally as important as adopting a systems engineering methodology for developing complex systems, is the selection of an implementation strategy that ensures adherence to the principles of systems engineering, and verifies successful execution of each of its various phases. Ultimately, the Government is accountable for results, and must ensure adequate technical competence is brought to bear for understanding issues and making decisions. For developing massive, complex systems, the Government may need to engage third party organizations to support them in this capacity.

The systems engineering methodology is not prescriptive regarding implementation strategies. The roles played by various organizations should be considered in light of how the activities in the systems engineering methodology might best be performed. For each system development activity, specific consideration should be given to enabling key roles for Government agencies and Government Laboratories, prime contractors, associate contractors, Federally Funded Research and Development Centers (FFRDCs), University Affiliated Research Centers (UARCs), academia, non-profits, and small or minority owned businesses. In architecting an implementation strategy, especially in defining the roles of prime contractors, note that history has shown that the strength of this nation for addressing massive, complex challenges is the wealth of available domain expertise, and the power of competitive forces.

To begin with, massive, complex systems normally require major contractors because they usually have the resources for manufacturing and production that smaller businesses do not have. In addition, large organizations have infrastructure, logistics, and in-service engineering capabilities that are critical to life cycle support. The considerable scale of the challenge in securing the borders necessitates a major contractor in the role of prime for system development and deployment.

There are many smaller companies not engaged in manufacturing and production; they necessarily rely on their subject matter expertise for providing value added to their customers. These organizations can provide critical support in assessing needs and feasibility, defining concepts, exploring operations, and providing intellectual property in understanding the problem and developing technologies. Because this is all that they do, they must be very competitive in what they provide. Therefore, one would not necessarily expect to see all the domain expertise resident in a prime contractor. To access the “best and brightest,” ways should be found to include these “associate contractors” as full members of the team.

The Nation has a significant resource in its nonprofit laboratories that can operate in the best interest of the Government as “Honest Brokers.” These organizations include Government laboratories (e.g., DOD service laboratories), the “National Labs” (DOE), Federally Funded Research and Development Centers (FFRDCs), and University Affiliated Research Centers (UARCs). The absence of shareholders, manufacturing, and production allows more independence (less conflict of interest) in supporting the Government in developing requirements, planning, prototyping, testing, and assessing operational effectiveness.

There are numerous examples of disparate successful strategies for implementing the systems engineering methodology. SSP’s management of the Polaris Program, previously mentioned, included a technical staff of 450 in the program office fully dedicated to the development and production of the Polaris system. This represents an example of a model with a strong technical role played by the Government. Two of the five major features identified by the GAO as contributing to this program’s

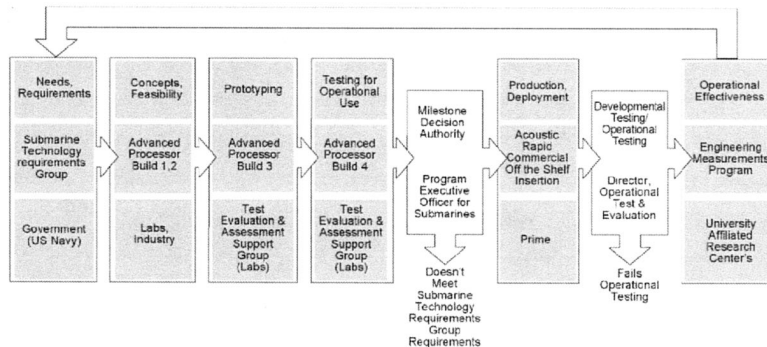
<sup>18</sup>Michael W. Wynne, Under Secretary of Defense (AT&L), “Policy for Systems Engineering in DOD,” February 20, 2004.

<sup>19</sup>Glenn F. Lamartin, Director, Defense Systems USD (AT&L), “Implementing Systems Engineering Plans in DOD—Interim Guidance,” March 30, 2004.

success are:<sup>20</sup> “(4) program office technical expertise, and (5) good management practices, such as open communications, independent internal evaluation, and on-site management representation at contractor plants.”

A considerably different model that emerged is the recognized successful<sup>21</sup> spiral development strategy used by the U.S. Navy for improving submarine sonars [Acoustic Rapid Commercial Off-the-Shelf (COTS) Insertion (ARCI)/Advanced Processor Build (APB)] starting in the mid 1990s. The Navy had made a commitment to embrace open architecture, in general, for new systems development efforts to enable a spiral development systems engineering methodology, and specifically to allow contributions from many organizations across the full spectrum of systems engineering activities. Mandating open architecture alone, while necessary, proved to be insufficient in many programs for changing the roles and contributions of organizations in the acquisition process. Progress in improving the acquisition process, had, in fact, been hampered by the continued use of traditional business practices that limit intellectual competition. In the words of the Chief of Naval Operations (CNO):<sup>22</sup> “Although we have made considerable Open Architecture (OA) investments over the past several years, we have been holding onto traditional business models and the overall progress transitioning into OA business practices is disappointing.” The CNO then cites the ARCI/APB program, as an exception, for its successful business model: “It (ARCI/APB) provides a clear and compelling example of competitive alternatives bringing reduced costs, improved capability, and increased speed of delivery to the fleet.”

The key aspect of the ARCI/APB business model cited by the CNO is how organizational roles are carefully tailored (Figure 2) to address the elements of systems engineering.



**Figure 2 The systems engineering methodology related to key aspects of the Navy's ARCI/APB business model.**

Requirements are set by a requirements group composed of Government (U.S. Navy) users. These are updated based on measured performance and changes to the threat. The broad scientific community, in general, supports the identification of concepts and assessment of feasibility. The Laboratory community develops prototypes, and as a group of peers [Test, Evaluation, and Support Group (TEASG)] assesses suitability of the concept for operational use. The results of this testing are used by Program Executive Office (PEO) Subs (Milestone Decision Authority) to validate that requirements are met before production. The Prime Contractor produces and deploys the system, and the Government [Director of Operations, Test and Evaluation (DOT&E)] verifies operational performance. During operational patrols, the Labs continuously assess operational effectiveness, and feed back results to the process to continue spiral development. Organizations do what they do best, conflicts of interest are minimized, and intellectual competition is encouraged

<sup>20</sup> United States General Accounting Office, “Fleet Ballistic Missile Program,” GAO/NSIAD-90-160, 9-6-1990.

<sup>21</sup> Winner of the Al Gore “Hammer Award for Reinventing Government” in February, 1999.

<sup>22</sup> M.G. Mullen, Chief of Naval Operations, “Navy Open Architecture,” Department of the Navy, August 28, 2006.

throughout the process.<sup>23</sup> In the words of the CNO: “My vision for OA is not limited to systems built to a set of open standards, but rather it is focused on open business models for the acquisition and spiral development of new systems that enable multiple developers to collectively and competitively participate in cost-effective and innovative capability delivery to the Naval Enterprise.”

One other basic aspect of the systems engineering implementation used by the ARCI/APB program must be mentioned because of its significance for ensuring real and rapid progress. Every concept/design/improvement is subjected to data-driven evaluation or assessment at every phase of the process to establish maturity, understand risk of implementation, and determine value added to overall performance. Key elements of this strategy are models validated with data, common data sets (real data) and common metrics, end-to-end test beds, in-situ testing, and peer review teams. This represents an example of a model that exploits the greater technical community to a very considerable extent.

### **Achieving Rapid Progress**

Given the urgency of the current national security environment, a crucial issue for any methodology and any implementation strategy is “How rapidly can one make progress?” If it takes too long to get to the 100 percent solution, one might be willing to take a 90 percent or 80 percent solution in the short-term. (Or as a worst case, one might pursue activities rapidly that consume resources and time and result in no real progress.)

Begin by recognizing that there is no magic process that can guarantee an arbitrary degree of progress in an arbitrarily short amount of time—even by throwing money at the problem. Then recognize that the systems engineering methodology, properly implemented, has the proven track record for realizing real progress as rapidly as possible. Very importantly, the systems engineering methodology can be tailored to emphasize milestone-driven development. In the ARCI program mentioned previously, the “R” stands for “Rapid.” Whereas, the traditional acquisition process for submarine sonars took 12 or more years to develop and implement improvements, the ARCI/APB spiral development process deploys a new build for sonars every year. Properly applying a systems engineering methodology to the border security challenge would seemingly offer the highest likelihood of progress as rapidly as possible. Moreover, a spiral development process for the border security challenge could reasonably produce yearly improvements in real performance.

The ARCI/APB program, initiated in 1996, deployed its first version at sea in 1998—two years. Lessons from successful spiral development programs shed light on what it takes to make rapid progress at the initiation of a program:

- Major hardware systems and infrastructure take time to develop. The more that exists, the faster progress can be made at the beginning.
- Open Architecture and COTS systems are key enablers for rapidly inserting software upgrades, and allowing any organization to “plug and play.”
- Contracting can easily delay progress. Multi-year contracting with key organizations, IDIQ contracts, and appropriate use of sole source contracting can all help.
- Technology that leads to performance improvements needs to be “in the pipeline,” and the implementation strategy should ensure accessibility to this technology, wherever it might exist in the greater technical community.
- The Government needs a key individual (Program Manager) empowered to do the right things—and it helps if he or she is a zealot.

### **RECOMMENDATIONS**

The following recommendations address the scope and complexity of the border security challenge, the impact of initial policy and requirements development with clear, holistic metrics, and proven implementation strategies.

- Recognizing the massive scale and complexity of the border security challenge, a firm commitment needs to be made to a disciplined systems engineering methodology for controlling performance, cost, and schedule and for providing the oversight tools the Government needs for monitoring performance and ensuring success.

<sup>23</sup> An unnamed staff member of the prime contractor for ARCI found competition after contract award intellectually stimulating: “I wouldn’t want to go back to the old way.”

*Even with SBlnet prime contractor selection by September 30, 2006, the systems engineering methodology can still be applied during rapid development and deployment to support operational success.*

- Policy, goals, metrics, and requirements must be defined at the beginning.

*CONOPS, policy, goals, metrics, and requirements for SBlnet should be clearly articulated to the prime early in the development process. An integrated view must be developed for the roles of federal, State, and local agencies.*

- An implementation strategy should consider enabling multiple organizations to collectively and competitively participate in all elements of system design, development, and deployment.

*Organizational constructs for SBlnet that vest too much responsibility and authority in a single prime organization may diminish objectivity and alternatives, and fail to exploit the Nation's strengths for solving its challenges—a wealth of technical resources, and an open competitive market for ideas.*

- Organizational conflict of interest must be avoided in testing and evaluation by using Government, nonprofit, and peer review organizations.

*The Nation's nonprofit laboratories (e.g., DOD Labs, the DOE "National Labs," FFRDCs, and UARCs) operate for the Government as "Honest Brokers." The absence of shareholders, manufacturing, and production in these organizations provides the Government an opportunity for independent validation and oversight of SBlnet. In particular, the Nation's nonprofit Labs can support requirements development, planning, prototyping, testing, and assessment of operational effectiveness.*

- Technology development and validation, risk reduction, testing for operational effectiveness, prototyping, limited production, and deployment—should all be performed before full-scale production and deployment.

*A scaled prototype of an integrated system for SBlnet should be developed and tested in an operational environment with Border Patrol agents. Full-scale production and deployment should begin only after discrepancies are resolved, and operators accept the system.*

- A continuing assessment of operational performance—determination of deficiencies, issues, and lessons learned—should feed back into a spiral development process for developing improved technologies and operations and improving performance.

*Given the lack of maturity in the marriage of technology and operations that support the border security mission area, a "spiral development" process should be used that exploits continually developing knowledge in this domain, adapts to technology improvements, and continually refines the CONOPS and tactical operations.*

- Given the urgency of today's national security environment, DHS should take those actions necessary to ensure real and rapid progress in the near-term.

*Secretary Chertoff has stated that SBI/SBlnet will make significant progress in two years.<sup>24</sup> What could SBlnet reasonably attempt to accomplish in that time? The current ISIS sensors, remote video surveillance, and existing infrastructure, and an imminent multi-year, IDIQ prime contract are significant resources for getting started. Importantly, there exist key technologies in the pipeline that apply to SBlnet's most critical issues: e.g., false alarm reduction algorithms, "large margin" classifiers, bell ringers, automatic target recognition, data fusion algorithms, and tactical scene generation. The data stream from existing sensors could be employed immediately for providing critical inputs to "data driven" research and development of these new technologies. These technologies, however, exist at many different organizations, and typically, outside the DHS community. So, the organizational implementation strategy used for SBlnet should accommodate—even encourage—outreach to a broad technical community. Moreover, an open architecture should be used for system development and implementation to allow any organization to "plug and play." Properly constructed and managed, in two years SBlnet could meaningfully attempt deployment of a limited prototype that demonstrates orders of magnitude improvement in critical performance areas (e.g., false alarm reduction), successful resolution of critical tech-*

<sup>24</sup> Oral Testimony by Secretary Michael Chertoff, before the U.S. House of Representatives Appropriations Subcommittee on Homeland Security, Rayburn House Office Building, July 27, 2006, reported by UPI on July 28, 2006: *Chertoff Pledges Better Border Security*, by Martin Sieff.

nical issues, and a baseline system that enables full-scale development and deployment.

### CLOSING

Again, I thank you for this opportunity to address you today on “*How Can Technologies Help Secure Our Borders?*,” and specifically how applying the discipline of the systems engineering methodology can ensure that Congress’ investment in SBI and SBInet will be rewarded with operational success. This ends my remarks concerning the applicability of a disciplined systems engineering approach to the daunting challenge of securing our nation’s borders.

### LIST OF ACRONYMS

APB	Advanced Processor Build
ARCI	Acoustic Rapid COTS Insertion
ASI	America’s Shield Initiative
AT&T	American Telephone and Telegraph
BPOE	Between Ports of Entry
CBP	Bureau of Customs and Border Protection
CNO	Chief of Naval Operations
CONOP	Concept of Operations
COTS	Commercial Off-the-Shelf
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOT&E	Director of Operational Test and Evaluation
FBM	Fleet Ballistic Missile
FFRDC	Federally Funded Research and Development Center
GAO	Government Accountability Office
GAO	General Accounting Office
GSA	General Services Administration
HUMINT	Human Intelligence
ICAD	Integrated Computer Assisted Detection
IDIQ	Indefinite Delivery, Indefinite Quantity
IEC	International Electrotechnical Commission
INS	Immigration and Naturalization Service
ISIS	Integrated Surveillance Intelligence System
ISO	International Organization for Standardization
OA	Open Architecture
OBP	Office of Border Patrol
OIG	Office of Inspector General
ONR	Office of Naval Research
PDA	Personal Digital Assistant
PEO	Program Executive Office
POE	Ports of Entry
RFP	Request for Proposals
RVS	Remote Video Surveillance
S&T	Science and Technology
SBI	Secure Border Initiative
SBInet	Secure Border Initiative (Program Component)
SSP	Strategic Systems Programs
TEASG	Test, Evaluation, and Support Group
UARC	University Affiliated Research Center
UAV	Unmanned Aerial Vehicle
USD (AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics



## BIOGRAPHY FOR GORDON DANIEL TYLER, JR.

**Company Title(s):** Department Head, National Security Technology Department  
 Business Area Head for Undersea Warfare  
 Business Area Head for Homeland Protection  
 Business Area Head for Biomedicine  
 Member APL Executive Council

**Areas of Practice/Specialization:**

With 36 years experience in research, development, test and evaluation, Mr. Tyler has been in technical, program management, and line management positions. He has supported DOD, the Intelligence Community, the Department of Homeland Security, and other Government agencies in various mission areas, including Undersea Warfare (Submarine Security, Anti-Submarine Warfare), Homeland Security/Homeland Defense (Maritime Domain Awareness, Border Protection, Counterdrug, Infrastructure Protection, Preparedness and Response), and Special Operations. His areas of technical specialization include: Sensor and System Development; System Concept Development and System Engineering; Operations Analysis, Modeling and Simulation, and Test and Evaluation.

**Honors, Degrees:**

M.S., Johns Hopkins University, 1974, Computer Science B.S., Massachusetts Institute of Technology, 1970, Electrical Engineering  
 Stanford Executive Program, Graduate School of Business, Stanford University, 2002  
 Merle Tuve Fellowship (1985)  
 Doctoral Coursework, Johns Hopkins University (1978–1985), Applied Mathematics

**Work Experience:****1970–Present: Johns Hopkins University Applied Physics Laboratory***Department Head, National Security Technology Department, 1998–Present*

Head line manager for APL department of 525 staff responsible for activities in Homeland Protection, Undersea Warfare, and Biomedicine, with principal organizational competencies in physics, sensors, signal and information processing, system concept development and systems engineering, test and evaluation.

*Business Area Head for Homeland Protection, 1998–Present*

Responsible for APL business activities in Homeland Security/Homeland Defense (180 staff years of effort), which includes the following thrusts:

- Preparedness and Response: Syndromic Surveillance/Biosurveillance/ESSENCE, for DARPA, DTRA, CDC, NCR; regional response planning, “first responder” support, and operational response T&E for DHS, NIH, MD;
- Key Facilities Protection: Mail screening and mail security activities for the U.S. Government and DOD; CBRNE sensor evaluations, pentagon security for PFFA;
- Maritime and Border Security: Portal Systems T&E for TSA; Container and In-Bond Security for C&BP; Advanced Spectral Systems for DNDO; Maritime Domain Awareness and Maritime Security for USCG;
- Special Operations and ISR: Systems engineering and analysis for SOCOM; Ops assessments and gaps evaluation for JIEDDO; special ISR projects for the intelligence community; systems engineering and analysis support for the Naval Special Warfare Development Group;
- CBRNE Detection and Defeat: CBRNE sensor/system RDT&E for JPEO CBD; sensor T&E and performance analysis for JPEO CBD; Spectral Sensing for Bioaerosols for DARPA; “gold standard” testing for HSARPA; systems engineering and analysis support for DTRA.

*Business Area Head for Undersea Warfare, 1998–Present*

Responsible for APL business activities in Undersea Warfare (350 staff years of effort) which includes the following thrusts:

- Submarine Security and Technology: SSBN Security Program; Submarine Security and Survivability Program;
- Anti-Submarine Warfare: Advanced Processor Builds for Submarine Sonar, Tactical Control, and Surface Ship Sonar; Engineering Measurements Program for Submarine Sonar (T&E); numerous ONR S&T efforts; Integrated Undersea Surveillance Systems; numerous special studies, analyses, and war games that directly support the office of the CNO.
- USW GWOT activities: Submarine In-Port and Near-Port Security; Nuclear Weapons Security; Pearl Harbor Port Security (NFESC);

Principal sponsors in Undersea Warfare include Director of Submarine Warfare (CNO N87); PEO Integrated Warfare Systems; NAVSEA; NAVAIR; SPAWAR; ONR; Strategic Systems Project Office; DARPA.

*Business Area Head for Biomedicine, 1998–Present*

Responsible for APL business activities in Biomedicine, which includes the following efforts:

- A revolutionary 22 degree of freedom upper extremity prosthetic with full neural integration (peripheral nerves, cortical neurons), and haptic feedback (DARPA); APL lead for team of worldwide, expert organizations; APL responsible for system engineering and integration;
- Biomechanics: Blunt trauma modeling and testing; Head-Supported Mass Program for the U.S. Army; vehicle and occupant response to IED detonation; Crash Test Facility testing.

*NSTD Assistant Department Head for Programs, 1994–1998*

Department supervisor responsible for program management and development activities including: fiscal year/multi-year planning; identification and development of strategic thrust areas; system concept development; program/project formulation; coordination and monitoring of program activities; identification of fiscal, human, and capital resources required to execute program activities; development of teaming arrangements with industry, academia, and government labs. The principal areas addressed consist of: Undersea Warfare technologies and systems (Submarine Security, Surveillance, Anti-Submarine Warfare, Mine Warfare); Information Science and Technology (Simulation, Modeling, Data Integration and Fusion, Signal and Information Processing, C<sup>3</sup>I, Intelligent Networking); Marine Engineering, Test and Evaluation; Counter-Drug technologies and systems; Ocean and Atmospheric Physics; technologies and systems for countering weapons of mass destruction; and Health Care Technologies.

*Undersea Surveillance Program Area Manager, 1988–1994*

Responsible for the development and management of Undersea Surveillance and Anti-Submarine Warfare systems and technologies, including: directed research, basic science and technology development; system engineering (requirements definition; modeling, simulation and analysis; system concept development; prototyping; system engineering and integration; test and evaluation; system architecture development; C<sup>3</sup>I; operational evaluation); concept of operations development. Major programs included: Integrated Undersea Surveillance Systems programs (Low Frequency Active, Critical Sea Test (Lead Lab), Air Defense Initiative, SURTASS development (Lead Lab), Advanced Distributed Systems, Full Spectrum Processing); avionics for the LAMPS helo program; BEARTRAP; Periscope Detection Radar; and DARPA simulation and modeling development.

*Acoustics Program Manager for the SSBN Security Technology Program, 1981–1987*

Responsible for eight to ten projects in the SSBN Security Program investigating the underwater acoustic detection of submarines. Projects emphasized basic physics, modeling, simulation, signal and information processing, system concept formulation, system design and engineering, test and evaluation, and operations analysis. Projects included: radiated signatures of submarines; mobile, low frequency active acoustic systems (DIANA, Standard Aura I, II, and I1I); fixed, low frequency active systems (Fixed-Fixed I, II, III); sub-on-sub operations (Standard Arrow I, II); exploitation of transient and intermittent acoustic radiation (LANTSECEX and PACSECEX testing); and sonar performance in oceanographic ducting conditions.

*Advanced Concepts Section Supervisor of the Acoustics Group, 1976–1980*

Line supervisor responsible for the development and evaluation of advanced underwater acoustic technology and system concepts for the detection of submarines. The scope of activities included: identification of key technologies; development of operational concepts; performance of scoping calculations with performance models; identification of critical issues and the conduct of analytical or experimental efforts for resolution.

*Assistant Program Element Manager of the Acoustics Group, 1979–1980*

Assistant Program Manager for the acoustics projects in the SSBN Security Program. Supported the Program Manager in planning, executing, and monitoring major acoustics projects including Standard Argo (exploitation of acoustic noise field anisotropy with high resolution sonar arrays), LANTSECEX 302–80 (detectability of specific signature components in acoustic surface ducts), and special analyses of Sonar Evaluation Program data.

*Protect Leader for SSBN Security Program Efforts, 1976–1980*

- *Standard Aries Sea Test and Analysis*: Exploitation of underwater acoustic surface ducting conditions for submarine detection. Directed project team performing environmental surveys and test area selection, pre-test performance predictions, test geometry designs, identification of critical issues associated with physics of acoustic propagation and scattering, measurement designs, signal processing, and overall analysis plans.
- *Advanced Concepts Analysis Project*: Directed team of analysts investigating advanced acoustic concepts for submarine detection as part of the SSBN Security Program. Specific concepts included inter-array processing (IAP), low frequency active acoustic sonars, planar arrays, distributed sensors, oceanographic exploitation, and the utilization of loud, intermittent acoustic evolutions.
- *Skeleton Array Exercise (SKELEX)*: Principal analyst and Project team lead, for planning, conducting, and performing analysis for the SKELEX at-sea exercise addressing maximum achievable gains for passive sonar towed arrays.

*Associate Engineer, Acoustics Group, 1970–1976*

Designed and developed digital signal processing hardware, algorithms, and software in support of analysis of underwater acoustics data, for assessing sonar performance in support of the SSBN Security Program. Designed and developed high-speed programmable array processor. Designed and implemented high-speed frequency domain algorithms for correlation, beamforming, and automated detection. Principal investigator for infrasonic detection of submarines, surface scattering effects on sonar performance, and Inter-array Processing.

**Publications:**

The Emergence of Low Frequency Active Acoustics as a Critical Anti-Submarine Warfare Technology, *Johns Hopkins APL Technical Digest*, Vol. 13, No. 1, 1992.

An Overview of the Critical Sea Test Program, *U.S. Navy Journal of Underwater Acoustics*, Vol. 42, No. 2, 1992.

Array Signal Gain Measurements for a Large Aperture Acoustic Array Operating in a Convergence Zone Environment, Proc. 32nd Navy Symposium on Underwater Acoustics, 1978.

Measurement of Signal Coherence, Propagation, and Array Dynamics with a Large Acoustic Array, APL/JHU POR–3143, April, 1976.

**Associations:**

Naval Submarine League

National Defense Industrial Association

Armed Forces Communications and Electronics Association

JOHNS HOPKINS  
UNIVERSITY

**Applied Physics Laboratory**

11100 Johns Hopkins Road  
Laurel MD 20723-6099  
240-228-5000 / Washington  
443-778-5000 / Baltimore

September 8, 2006

BY FACSIMILE AND REGULAR MAIL

The Hon. Sherwood Boehlert  
Chairman, Committee on Science  
U.S. House of Representatives  
Rayburn House Office Building, Suite 2320  
Washington, DC 20515-6301

RECEIVED  
SEP 21 2006  
COMMITTEE ON SCIENCE

RECEIVED  
SEP 21 2006  
COMSU

RE: Financial Disclosure Letter – *“How Can Technologies Help Secure Our Borders?”*

Dear Chairman Boehlert:

As required by the Rules Governing Testimony for witnesses testifying before the Committee on Science for the 109<sup>th</sup> Congress, as Department Head of the National Security Technology Department of The Johns Hopkins University Applied Physics Laboratory (JHU/APL), a private entity and not representing a government entity, I hereby submit the following financial disclosure information.

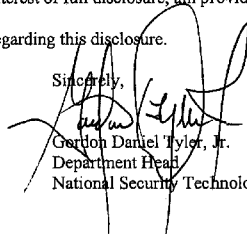
I have been invited to testify at the hearing entitled *“How Can Technologies Help Secure Our Borders?”* The specific subject matter I have been asked to address and on which I will testify is *“The Application of Systems Engineering Methodology for Helping to Secure America’s Borders.”* The sources of federal funding which directly supports that subject matter received by JHU/APL and/or me during the current fiscal year or either of the two preceding fiscal years is as follows:

JHU/APL and I have received no federal funding which directly supports the subject matter of my testimony *“The Application of Systems Engineering Methodology for Helping to Secure America’s Borders.”*

JHU/APL is working on a task entitled *“Independent Verification & Validation (IV&V) Effort for a Modeling & Simulation.”* APL’s efforts were to independently verify and validate a model developed by another non-government, non-profit research organization. This model could be used by DHS/Customs and Border Protection to determine optimal placement of border security assets. Federal funding received from DHS was \$265,000 in FY06. I believe that this work does not directly support the subject matter of my testimony, but in the interest of full disclosure, am providing the information.

Please let me know if you have any questions regarding this disclosure.

Sincerely,



Gerton Daniel Tyler, Jr.  
Department Head  
National Security Technology Department

Chairman BOEHLERT. Thank you very much, Mr. Tyler.  
Dr. Worch.

**STATEMENT OF DR. PETER R. WORCH, INDEPENDENT CONSULTANT, MEMBER OF THE U.S. AIR FORCE SCIENCE ADVISORY BOARD**

Dr. WORCH. Chairman Boehlert, distinguished Members of the House Committee on Science. I am, indeed, honored to be asked to provide you my comments relative to technologies for border security. I would like to point out that these are my opinions and not necessarily those of either the Air Force Scientific Advisory Board or the Air Force.

I look at this border security as a system problem, and so it is fitting that I follow Dan here. It is a set of layered systems, layered elements. And it starts with information and it ends with information, by the way. At the front end, and I hear this too seldom, we need to have the information on the people that might cross the borders, their culture, their behavior, their motivation, their training. We need to know about the terrain, the topography. We need to know about the motivation or the possible routes that the people might take. And we need to know about the objectives.

Call this intelligence, if you will, but it is not to be considered as a separate element. It is an integral part of the surveillance problem. And I have seen too little mention of that important role. And where it helps, right from the start, it tells where to put the sensors and how to use the sensors, and that is important.

The next piece I see is a tripwire. It can successfully protect our borders, yet remain within the limits of acceptable behavior of a broad area. Unattended ground sensors happen to be my favorite along with unmanned air vehicles that can detect just motion—not imagery—just motion at this point, we are trying to detect.

The next level is to investigate those detections, and that is where images come into play from UAVs, which I will repeat several times here, seem, to me, to be the best way to go about it.

And finally, people. And what we need to do is think about these technologies, I believe, in how they aid the human, the human that is the agent, the human that is operating the command center, the human who needs to have the information brought to him and put in the proper form that he can make a rapid and effective and correct decision. The consequences of bad decisions here are severe, and one needs to take into consideration the need to aid people, not replace them.

On UAVs: UAVs clearly, in my mind, offer significant advantage over all other platforms. They can rapidly deploy to an area in which there is a suspected or a real intrusion. They can investigate that area. They can provide persistent surveillance, 24/7, and no one gets tired. And they can provide relentless tracking of individuals or vehicles that may have crossed the border. So I think they play a key role.

Let me switch gears now to the technology part.

I see technology needs really in three areas: sensors, and UAVs, and again, in the information management portion. Call it intelligence, if you will. It is some of both, really.

In the sensor area, I think there is much to be done in area of unattended ground sensors. There has been some good work done in the field. There has been some good work done by Sandia Laboratories and other activities, the military labs, and in industry, and in the universities, Berkeley, for example. This sort of work in the basic, unattended ground sensors is essential, because they can provide a very low-cost tripwire, if you will, and eventually even some level of identification.

Other work needs to be done in multi-spectral and hyper-spectral sensors and in radar processing, radar processing to extract these slow-moving, small radar cross-section people from the background that is there. A very difficult problem.

And finally, automatic target recognition, not as a replacement for an individual, but again, to aid that individual making the right decisions.

UAV technologies fall in two areas: human system integration, the ability to give the man on the ground the same feel for the aircraft, the same indications, the same situational awareness he would have if he were in the aircraft himself. Not enough work has been done on that. We can build wings, we can build engines, but we have got to deal with the human finally and do that at a much better rate.

The other area is really a group of projects that are necessary for air safety. Many of these projects have been pursued for manned aircraft. Some of them are unique for unattended aircraft, UAVs. And those are the areas that need to be pushed. Unfortunately, much of this was funded by NASA and since they have reduced the budget in that area, we definitely have a shortfall. They have some very good programs specifically aimed at operating UAVs in manned airspace.

The third area is that of information management. And yes, connectivity communications is part of this, but the more difficult thing is to gain knowledge out of data that comes from a large number of sources, a large number of independent sources, and some of it may be history, some of it may be real-time from the sensors, but to put that in a form where the decision-maker can make a quick and accurate decision.

So those are the three areas: sensors, UAV technologies, and information management technologies.

Now getting there.

Very quickly, I think it is important to partner with the military laboratories. I think the military problem is very similar to this. It may not have been five years ago or five years and a few days ago, but it is now, both from what has happened in this country and what we are dealing with in Iraq. Very similar. There needs to be cooperation much better than there is. Fortunately, there is one good example where this is happening. The National Law Enforcement and Corrections Technology Center Northeast is partnering with the Air Force Research Laboratory Information Director at Rome, New York. They are in adjacent buildings. They are working together. The technology is flowing in both ways, but it is a small operation, and much more needs to be done in that regard.

In the area of systems, I am in favor of evolutionary approaches to system acquisition, not—I am disappointed, quite frankly, in a

turnkey, large system integrator approach that we have or large system approach that is on the streets now. I feel a contract—and it is backed up in some of the appendixes. Contractor A is going to put contractor A's equipment on the line. Contractor B is going to put contractor B's equipment. We don't know whether either one of those are the right ones. But that is—a piece of this evolutionary acquisition needs to be brought to this table, and it builds on what is there now and gradually improves this. I think we need to insist on integration of information, not integration of systems.

That concludes my remarks.

[The prepared statement of Dr. Worch follows:]

PREPARED STATEMENT OF PETER R. WORCH

Chairman Boehlert, distinguished Members of the House Committee on Science. I am honored to be asked to share with you my thoughts on the difficult topic of border security. To successfully protect our borders, yet remain within the limits of acceptable behavior of a democratic society is indeed a challenge.

To set the record, my background is in the development of technology to support military operations, based on 24 years of an Air Force career involving both operational and technical experience, followed by a second career in unmanned aerial vehicles (UAVs) and associated sensors and communications. Many of the systems lessons learned, as well as the technology developments, could contribute to the border security problems. My expertise is not the entry-point problem; I concentrate on the remote border problem.

**Overview**

The detection of border security violations has some similarities to the military border and area security challenges faced in Iraq and many other locations today. The differences are sufficient, however, that the system solutions are quite different in most cases. But, the technologies that have been developed and tested in military applications deserve consideration for homeland security, and the benefits and savings achieved by joint endeavors are significant.

In this paper, I attempt to review the technologies that, in my opinion, offer promise for significantly improved detection of border incursions. I will urge the homeland security and military laboratory teams to work together on these technologies.

**A Context**

I was asked to make assessments and compare, or evaluate technologies for border security. I find it most useful to consider technologies in the context of system concepts, and hence I would like to spend a few moments on the system aspect.

Border security is much like what the air forces call time-critical targeting. In the battlespace, a detected target must be attacked within a time frame (typically 10 minutes) determined by the possibility that the target will act or escape or both. The 10 minutes must be budgeted across numerous actions—Find, Fix, Track, Target, Engage and Assess.

In the case of border security, the objective is to intercept the detected intruding individual or vehicle before it can escape.—Detect, locate, identify, decide, intercept. Once again, the time must be budgeted across these elements. If a human moves at five mph, you have just 12 minutes to catch that human if you want to limit travel to one mile from the border. I say this to emphasize that one minute saved in the detection and reporting process is a minute that the border agent has to get to the point of intrusion.

Human eyes and reasoning are essential in order to avoid fratricide—but a system of shoulder-to-shoulder border agents is not possible, and it is not practical to continuously watch images of the entire border from airborne or surface sensors 24/7 across 8000 miles of border on the chance an intruder will be seen. Though a bank guard can view the few camera images of the bank access points, the vault, and perhaps the cashiers, the problem of monitoring sensors that may themselves be moving (creating a dynamically changing background), and the large area being guarded suggest a challenging situation. Yet, direct viewing or high resolution imagery is the only acceptable means of verifying that an unwanted intrusion has occurred. Automated target recognition (ATR) techniques may be able to determine that a human has been detected, but nothing more about identification or intent, given today's state-of-the-art.

I see no magic—no single solution—The system solution must be a layered sensor approach, tailored to the nature of the specific border situation. It must include:

- An interagency information system that can point to likely areas of intrusion
- A “trip-wire” to detect an intrusion and alert the system. A means to aim or focus an imaging sensor at the point of intrusion or other alerting cues
- A communication of an image containing the suspected intruder to a human agent for confirmation
- Collaboration of information from available sources, including the sensors, to expedite and improve the analysis process
- Presentation to the human decision-maker in a form that is immediately sufficient to make an informed decision
- A means to expeditiously dispatch an agent to intercept the intruder
- An effective concept of operations, with the associated procedures and training to accomplish the above.

There are a number of options for systems that meet this construct. Table 1 depicts some of the more powerful techniques.

Air intruders are an additional threat. These could be manned aircraft—perhaps a Cessna 172 piloted by a terrorist or a smuggler of narcotics or humans, or could be an unmanned aircraft, ranging in size and complexity from a miniature radio-controlled (RC) hobby model capable of carrying a few ounces of a deadly chemical agent to a Cessna 172 aircraft that has been rigged for unmanned operation, perhaps looking like a conventional manned aircraft with a mannequin in the cockpit seat but carrying 500 lbs. of explosive. The Air Force Scientific Advisory Board has recently studied this problem.<sup>1</sup>

Low and slow small aircraft pose unique challenges to our air defense system. Often the radar features that improve the ability to discern aircraft from background ground traffic by remove the slow movers (judged to be ground vehicles) on the basis of speed, would similarly gate out the UAVs and slow manned aircraft. Technology efforts are in order to address the processing of slow-moving small aircraft from background clutter.

The second key challenge for air targets is to determine intent. Given that the goal will be to force the air vehicle to the ground or shoot it down, we must be quite certain that this air vehicle has a hostile intent. This will be extremely difficult to determine and sensors are not available to accomplish the task. Intelligence will be the best indicator.

It will be especially important to provide air defense for the National Capitol Region and National Special Security Events, but borders must be considered as well.

The key to effective border surveillance and security is the intelligence that allows the security team to concentrate their search efforts and prepare the agent team. This cannot be over-emphasized, and includes intelligence information gained from the point of origin of the would-be intruders as well as the local intelligence information on staging areas and transportation means. The information may be gained over a significant time and geographical span, thus requiring both an effective network and an efficient correlation and dissemination process. This will be addressed in a later section.

---

<sup>1</sup>Air Force Scientific Advisory Board Study, “Air Defense Against UAVs,” 2006.



	Intruder				
	Human	Vehicle	UAV	Aircraft	Boat
Tripwire	Intelligence UGS EO/IR* GMTI Radar	Intelligence UGS GMTI Radar SAR Radar	Intelligence AMTI Radar	Intelligence AMTI Radar	Intelligence MTI Radar
Investigator	EO/IR	GMTI Radar SAR Radar EO/IR	EO/IR	EO/IR	EO/IR
Tracker	EO/IR	GMTI Radar SAR Radar EO/IR	AMTI Radar EO/IR	AMTI Radar EO/IR	EO/IR
Interceptor	Heli-borne Agent	Heli-borne Agent	Heli-borne Agent	Heli-borne Agent Fighter a/c	Heli-borne Agent

\* where penetrations are concentrated and terrain/foilage permit

**Table 1 – Techniques for Border Security**

### Sensors

Sensor technology for airborne applications is very well developed. The experiences in Iraq have demonstrated the advanced capabilities, and have generated yet further improvements in sensor systems, driven by the unique nature of the operations of the adversary. The military laboratories and industry have succeeded in gaining high resolution and compact packaging such that even small UAVs can carry the sensors and associated communications equipment. Table 2 shows the common sensors for this application.

Sensor Technique	Advantage	Disadvantages
Microwave MTI Radar	Excellent for detecting moving vehicles Good in weather Wide coverage area; good revisit Fair for vehicle target classification (w/HRR)	Marginal value in foliage Moving Targets (>MDV) only Limited capability against humans
Microwave Synthetic Aperture Radar (SAR)	Excellent for target classification Can be used with coherent change detection Good for target identification Good in weather	Marginal value in foliage Limited coverage rate Limited capability against humans
VHF Foliage Penetration (FOPEN) Radar	Good for detecting targets in foliage Can be basis for coherent change detection	Must operate at high grazing angles Long dwell time Not suitable for Tgt ID Limited capability against humans
EO/IR	Excellent for search small areas Best choice for detecting and tracking humans Best choice for target ID	Marginal performance in foliage Limited standoff distance Poor performance in weather
High Resolution LADAR	3D information for target ID Some foliage penetration	Small Field of Regard Marginal performance in weather Requires near-nadir look Requires close-in viewing
Hyperspectral Imaging	Good choice for facility detection Some foliage penetration Wide coverage area	Marginal performance in foliage Marginal performance in weather Requires near-nadir look Little data on detecting humans Poor target identification
SIGINT	Excellent for target ID Could pick up cell phones Good against aircraft data links	Unlikely personal signal emanation

**Table 2 Key Airborne Sensors**

Despite the fact that Unattended Ground Sensors (UGS) have been in development for many years,<sup>2</sup> the state-of-the-art is still lagging. The military services have been slow to develop and employ ground sensors, largely due to wariness as to the performance. The DHS Customs and Border Protection has reportedly placed some 11,000 (11,000 sensors spaced 100 feet means approximately 200 miles of ground-sensor monitored border) along the northern and southwestern borders. The false alarm rate has been uncomfortably high for sensor detections (animals, sun glint, etc.), and short battery life. Yet, their have been successes in other government laboratories<sup>3</sup> the commercial world including the development of grape-size sensors that are capable of self-organizing and robust networking. Table 3 provides advantages and disadvantages of the ground sensors.

<sup>2</sup>Perhaps one of the most widely-publicized failures of ground sensors was McNamara's attempt to stall supply flows along the Ho Chi Ming trail in Vietnam during that conflict.

<sup>3</sup>Sandia National Laboratories has an excellent unattended ground sensor program.

Sensor Technique	Advantage	Disadvantages
Acoustic	Can detect human talk, breathing, motion Some target classification capability Suitable in heavy foliage Low operating cost	False alarms (as single sensor) Short Range Must be proliferated
Seismic	Can detect vehicle movement Some target classification capability Suitable in heavy foliage Low operating cost	False alarms (as single sensor) Short Range Must be proliferated
Tilt	Can detect large vehicle movement Some target classification capability Suitable in heavy foliage Low operating cost	False alarms (as single sensor) Short Range Must be proliferated
Magnetic	Good for detecting vehicles Some target classification capability Suitable in heavy foliage	False alarms (as single sensor) Short Range Must be proliferated Minimum communications
Multispectral	May provide target identification May be able to analyze dangerous items	Practicality questionable Limited range High communications requirements
EO/IR Imaging	Some target classification capability Low operating cost	
IR Non-imaging	Good for detecting warm bodies Suitable in medium foliage Low operating cost Minimum communications needs	False alarms (as single sensor) Short Range Must be proliferated

**Table 3 Key Ground Sensors**

The false alarm rate was the Achilles's Heel of the Southeast Asia application of ground sensors. More recently, the use of combination sensors (acoustic with seismic, for example) coupled with the progress in miniature processing hardware has shown great promise for low false alarm rates and long battery performance. This unattended ground sensors offer great promise for the monitoring for border intrusions, particularly in areas of dense vegetation and rough terrain.

There remain some important areas for further technology development. These tend to be more in the effective utilization of current sensing regimes

- **Multi- and Hyperspectral Imagery sensors for detection and identification of humans from airborne & UGS platforms.** Hyperspectral imaging offers the capability for identification of vehicles and, perhaps, humans. Moreover, it has shown promise in the identification of packages and equipment being transported across borders.
- **Automatic Target Classification/Recognition techniques for EO & IR imagery.** The key to improving the efficiency of the limited number of border agents is to provide tools, such as the ability to scan images for humans or targets, to provide alerts with low false alarm categorization of the detection to the operator.<sup>4</sup>
- **Low cost, miniature, self-organizing, multi-sensor unattended ground sensors for detection and classification**
  - Acoustic
  - Seismic
  - EO
  - Imaging IR
  - Thermal IR

This is perhaps the most promising area of technology development for the border surveillance. The sensing elements should be developed further to re-

<sup>4</sup>The gambling casinos are now using automatic recognition techniques to spot undesirable participants.

duce size and battery power, and the processing of multiple complementary sensors for improved recognition or reduced false alarm rate is important.

- **Radar processing techniques for extracting small slow moving air and ground targets** from background low speed clutter. To date, MTI radar has been very effective in generating a situational awareness picture of a battle area, including the tracking of supply and equipment movements, but the slow speed and small cross-section of humans has limited effectiveness against humans. There is now hope for the detection of slow moving humans, and that area needs a technology investment.

### UAV Platforms

The unmanned aerial vehicle has revolutionized the airborne sensor world. The aircraft and propulsions are mature and efficient. The vehicle mission management systems are reliable, partly due to improved hardware and software and partly due to the redundancy now being included in such aircraft as Predator B. They have the advantage (over manned aircraft) of long endurance—30 to 50 hours. UAVs (like manned aircraft) tend to avoid failures once airborne, so the long endurance affects reliability as well.

The experiences of the Air Force and CIA in operation of long surveillance flights have been excellent. Predator and Global Hawk UAVs have been instrumental in gaining surveillance information around the clock. Both have been paired very successfully with attack aircraft. The Predator UAV has been successful in lingering in harms way to monitor suspected hideouts and laser designating targets for buddy strike. There have been cases of Predator surveillance of IED placement that resulted in many saved lives.

Even within the Border Patrol mission, UAVs have shown their value. The Predator B has been quite successful in its operation, being given credit for finding, tracking and the eventual capture of border crossing intruders. There have been a minimum of failures.

There are some advocates for aerostats as sensor platforms. In view of their inability to cope with higher winds, they seem to be achieving a 60–70 percent airborne rate. The UAV can move closer to an area to increase the look-down (grazing) angle, providing a better opportunity to view areas of vegetation, structures and terrain. Aerostats do not have that flexibility. In my mind, the low rate, combined with the need for substantial real estate and ground support equipment suggests the UAV for the mission.

An area of possible technology investment would be in the development of a hybrid aerostat that could morph to a parafoil kite when winds increased, and thus stay on station.

Table 4 shows the classes of UAVs suitable for border surveillance. Within the classes of possible UAVs for border security, the medium altitude endurance UAVs are most suited because they give the best trade between cost and endurance, with the border surveillance mission.

UAV Class	Examples	Payload (lbs)	Nominal Endurance (hrs)	Loiter Altitude (ft)	Loiter Airspeed (kts)
High Altitude Endurance	RQ-4A Global Hawk	1000	40	60000	250
	RQ-4B Global Hawk	2000	40	60000	250
Medium Altitude Endurance	MQ-1A Predator A	500 Internal 250 External	40	20000	85
	MQ-9A Predator B	750 Internal 3000 External	30	40000	85
Low Altitude - Medium	Lewk, Shadow	3000	4 - 8	10000	60 - 100
Medium Altitude - High Survivability	X-45, X-47	2000 - 5000	4 - 8	40000	300 - 500
Rotorcraft	Fire Scout, Hummingbird	500 - 1000	4 - 8	20000	60 - 200
Low Altitude - Small	Dragon Eye, FPASS, etc.	10 - 25	4	1000	40 - 60

Table 4 – UAV Classes

But there remain UAV technology issues deserving attention. Developing and operating UAVs present unique technology needs that go beyond the airframes and propulsion (and border surveillance flights):

- **Human-System Integration**—situational awareness, controls and displays, health management, and emergency procedures all require improved HSI.
- **Detect, See and Avoid techniques** that are highly automated, vision-based systems are needed for UAV operations (and would benefit civil and military aircraft).
- **Automatic Traffic Alert and Collision Avoidance System (TCAS)** to do the tasks of the current TCAS, but translate the alerts into control commands suitable for avoiding collisions.
- **Automated landing systems** based on GPS but tailored for UAVs suitable for alternate precision landings at all airports.
- **Automated voice** for declaration of position and intentions for lost-comm or other emergency situations, and for receiving emergency comms from disadvantaged nodes.
- **Communications networks** that support machine-to-machine connectivity between ATC and UAV operators.

One might have expected NASA to pioneer in developing many of the technologies listed above, as UAVs have both military and commercial applications in addition to those of the DHS. The UAV National Industry Team (UNITE) and the NASA ACCESS 5 Project were addressing the issues. With the reduction in the NASA aeronautics budget, ACCESS 5 was canceled and it appears this will not happen. The military services and DHS are not funded to accomplish this either.

Certification of new systems will be rigorous, and is beyond the means of the UAV industry to fund. Here the Government should support this process, as it is long and costly.

#### Intelligence and Information Management

While I see much to be accomplished in the development of new sensors, our major shortfall, both in the military and in homeland border security, is the inability to effectively and efficiently deal with the large amount of information that is collected by our sensors or is available from other sources. This problem starts with the gathering of that information which will help us determine when and where sensors should be placed. This needn't be tapping of telephones or bugging residences, but is a matter of understanding the nature of the border (e.g., what is the terrain like; where are access points from highways; did it snow heavily in this area today), monitoring locations that might give indications of impending activity, and understanding the nature and behavior patterns of the individuals being sought.

From this analysis, the limited resource budget of sensing systems and responding agents can be efficiently deployed. The notion of 24/7 surveillance of the entire border (or even 10 percent of the border) from the air is just not practical.

A good analogy is that of the ardent deer hunter. The deer hunter doesn't go out and sit at the first stump to wait for a deer. He (or she) has analyzed the general hunting area and selected an area most likely to be productive. Further analysis will tell the hunter which paths the deer will likely take under what conditions of weather and time of day. The deer doesn't worry about deer coming across a river or lake (though it sometimes happens). The hunter selects a location from which to observe, and uses his natural sensors wisely—usually motion or noise are the tipoff, and the combination of the two—eyes sensing a movement as the noise emanates from the same spot. The hunter then casts a focused eyeball on the source of the movement or noise will confirm the target, and track that "target" to the point of "intercept." Those same eyeballs couldn't possibly "image" all the area all the time.

The second information shortfall is that of communicating sensed data to a location(s) at which these data can be fused, analyzed, compared to stored data, stored, and presented in a coherent picture to the operator—Thomas Friedman terms this "connect and collaborate." At the current time, information is available, but difficult to access. Information is located within various organizations and many locations. The information may be seconds old or years old. Data formats are different. Scales may be different on different images. The sources may have different levels of credibility.

The presentation to the decision maker is the final level of information management. The agent who must decide on a course of action has little time. He cannot search databases for relevant information. He, or she, must be presented with a fused picture that includes the material with appropriate indications of the reliability and nature of the information. It may be necessary to discuss the information with another individual, so the information must be shared, whether the distant individual has a 21-inch screen at the command center or a PDA he has carried into the movie theater.

Little attention has been given to information management. The Air Force Scientific Advisory Board has recently completed a study<sup>5</sup> which makes the case for inter-operability and the integration of information. In that study, it is pointed out that recent programs have created "stovepipes" of information, and solutions that lean toward integrating stovepipe systems will simply create further stovepipes. Instead, inter-operability, achieved by metadata tagging (recording the data about the data—time and location, context, content descriptions, format) of all data can make it accessible to all. Moreover, the use of a service-oriented architecture providing the common tools for transferring, storing, fusing, and disseminating data assures a coherent management of the information.

I see the following areas as important information technology investment areas:

- **Communications networking**
  - Internet Protocol (IP) based communications sensor networking
  - Self-forming/self healing network management
  - Low power dynamically variable bandwidth comms for ground sensors.
- **Data management and knowledge generation**
  - Descriptive metadata (i.e., content, context, and structure)
  - Semantic matching
  - Geospatial and temporal registration (co-registration of multi-sensor data)
  - Fusion
  - Real-time publish-subscribe-query service
  - Rules and tools for constructing metadata vocabularies
  - Automated metadata insertion into legacy databases
  - Rules for information sharing
  - Performance issues when scaling to many COIs and operational users.
- **Visualization technology**
  - Aids to interpretation of large amounts of imagery
  - Aids to human interpretation of machine data

<sup>5</sup>Air Force Scientific Advisory Board, "Domain Integration," 2005.

- Aids to developing a concise and complete situational assessment picture in a timely manner for the decision-maker.

### **An Approach**

It seems fitting to make some comment relative to achieving the improved border security capitalizing on the technology advancements.

In so far as developing the pertinent technologies is concerned, there are some fundamental science issues and as the science is matured, there are some prototyping and experimentation phases. To be sure, there will be a need to focus resources. I am concerned that the costs, both direct and overhead, associated with a new/expanded DHS sensors laboratory program will be significant. I see the need to partner with Service laboratories<sup>6</sup> in the technology program, not only in capitalizing on the lessons learned in long years of military endeavor in sensor development, production, deployment, and employment, but also in using facilities and other resources already in place. Some arrangement to, perhaps, provide funding and tasking to the military laboratories for sensor developments, or to co-locate DHS scientists with military laboratory teams should be pursued.

Testing should also be conducted in conjunction with military. Once again, sharing the cost of the tests will lead to joint management and sharing the results. Over and above that, there exist test ranges, experienced test managers, and procedures that could be used jointly to satisfy the needs of both DHS and the Military.

For the development of a system of advanced sensors, processing systems, and command centers, I strongly recommend against turn-key integrated systems. Much of the past work addressing integration has actually been focusing on creating monolithic large scale systems. This a costly approach that inevitably restricts the introduction of new elements to those provided by the integration contractor. An end user only requires *virtual integration*—he needs to receive integrated data. He does not require actual domain integration nor does he have the responsibility and resources to accomplish it. For this reason, and many others, it is prudent to define an architecture that is flexible and is inter-operable with the legacy systems. Quality of Service should be the metric, and hence a service-oriented architecture (SOA) is in order. A service-oriented *architecture* is an approach to defining integration-architectures based on the concept of service. A *service* is a collection of applications, data, and tools with which one interacts via message exchange.

### **Integrate information, not systems**

Finally, It is important to adopt an evolutionary acquisition approach. I quote from an Air Force Instruction:

*“Evolutionary acquisition (EA) is a nontraditional, overarching acquisition strategy that a program can use to develop and field a core capability meeting a valid requirement with the intent to develop and field additional capabilities in successive increments.”<sup>7</sup>*

*“The simple goals of EA for systems are to achieve modernization and deployment efficiently and quickly. Use of an EA strategy for systems will deliver a core operational capability sooner by dividing a large, single development into many smaller developments or increments. EA allows a program to quickly respond to changing conditions by allowing each increment to accommodate the following three activities: 1) develop new capabilities supporting the operational requirements and goals of the system, 2) exploit opportunities to insert new technologies that reduce cost of ownership or accelerate fielding of new capabilities resulting from experimentation or technology demonstrations, and 3) refine current capabilities based on user feedback, testing, or experimentation.”<sup>8</sup>*

### **Summary**

There have been shown to be several border security technology areas worthy of increased emphasis by the Department of Homeland Security Customs and Border Protection service. For the most part, the developments are not breakthrough basic science, but rather a matter of applying science and making it available in a deployable form for application to the borders. More importantly, it is a matter of processing the raw data from multiple sensors, along with intelligence information data, in such a way as to extract the full content of knowledge from the data. This is not a job for sensor developers, but for information experts with a strong under-

<sup>6</sup>The partnering of the National Law Enforcement & Corrections Technology Center—Northeast Region with the Air Force Research Laboratory—Information Directorate is a good step.

<sup>7</sup>From Air Force Instruction 63-123, “Evolutionary Acquisition of C2 Systems,” 1 Apr. 2000.

<sup>8</sup>Ibid.

standing of the sensor outputs. It seems we have radar experts and EO/IR experts and UAV experts, but lack in “find the human” experts.

This testimony is formulated to suggest the maturation of the technologies be conducted jointly with the U.S. military services. The techniques for the detection of humans entering the United States are, with minor variations in employment, essential to the protection of U.S. Forces and U.S. interests abroad.

#### BIOGRAPHY FOR PETER R. WORCH

##### **EDUCATION**

Oklahoma State University, Ph.D., Electrical Engineering  
 Oklahoma State University, M.S., Electrical Engineering  
 Union College, B.S., Electrical Engineering

##### **PROFESSIONAL SUMMARY**

Dr. Worch is a senior systems scientist with over forty years R&D experience in the areas of avionics, communications, navigation, intelligence, command and control, emitter location, identification and surveillance; as well as overall military technology research and development management. He has been assisting in unmanned air vehicle (UAV) development programs and in UAV payload development efforts. Dr. Worch is a member of the Air Force Scientific Advisory Board.

Dr. Worch is a Research Scientist with George Mason University, conducting research in command and control systems concepts.

##### **EXPERIENCE**

###### *Consultant (1994 to Present).*

Dr. Worch provides assistance in operational, technical, and program analyses as well as both strategic and tactical sensor, electronic warfare, and C<sup>3</sup>I architecture studies. He conducts analyses in time critical targets, UAVs, reconnaissance sensors, C<sup>3</sup>I interface for advanced weapons systems, avionics, data links, smart weapons, navigation; LPI/LPE communications, electronic warfare and information warfare. He is also an advisor in the SIGINT technologies.

###### *Manager, Defense Systems Technology Operation, SAIC (1989–1994).*

Dr. Worch directed the activities of three Divisions involved in advanced research and development programs. The activities were primarily in the area of advanced C<sup>3</sup>I and reconnaissance/surveillance technology with emphasis on sensor technology for the detection recognition of ground and air targets that are hidden or possess reduced observables characteristics. Dr. Worch served directly as a technical advisor to ARPA on numerous program areas relating to C<sup>3</sup>I.

###### *Manager, C<sup>3</sup>I Technology Division, SAIC (1982–1989).*

Dr. Worch was involved in operational and technical analyses as well as both strategic and tactical sensor, electronic warfare, and C<sup>3</sup>I architecture studies corporate-wide. He conducted analyses and managed programs in relocatable targets, RPVs, reconnaissance systems, C<sup>3</sup>I interface for advanced weapons systems, data links, smart weapons, navigation; LPI/LPE communications, electronic warfare and C<sup>3</sup>CM. He was active in C<sup>3</sup>I R&D for strategic, tactical and special operations forces.

###### *U. S. Air Force (1957–1981).*

Dr. Worch served in numerous roles as an Air Force officer including both development and maintenance of communications and electronics systems; weapons systems; and avionics equipment of tactical and airlift aircraft. He served as project engineer responsible for research and exploratory development of electromagnetic signal reconnaissance techniques, communications and navigation projects at Rome Laboratory (formerly Rome Air Development Center). Dr. Worch completed his service as Vice Commander of Rome Air Development Center at which he was principal assistant to the Commander and shared responsibility for command and direction of the Center research and development in command, control, communications and intelligence.

###### *R&D Program Manager, Tactical Technology Office, DARPA (1973–1976).*

Managed and technically directed multi-service exploratory development efforts of critical importance to defense programs. Initiated, planned, directed and evaluated programs in electronics intelligence, advanced communications, advanced LPI airborne radar, target identification, navigation, and low observables aircraft. Directed and participated in OSD studies, symposia and panels of technical and operational



nature. Dr. Worch conceived and managed a program for precision emitter location from remotely piloted vehicles (RPV) and participated in RPV communications and sensor system developments. He formulated and directed programs in bistatic radar and low probability of intercept airborne radar.

## PUBLICATIONS

### Reports

- Worch, P.R., et al., *Strategic Conventional Standoff Capability (SCSC) C<sup>3</sup>I System Architecture (U)*, AAMRC-TR-86-031, SECRET/NOFORN, 1987.
- Worch, P.R., et al., *Mission Electronic Equipment for Special Operations Forces (U)*, SAIC Report to DARPA/TTO, SECRET, 1984.
- Worch, P.R., et al., *Joint STARS Radar Review Final Report (U)*, SAI Report to DARPA/TTO, SECRET, 1984.
- Worch, P.R., et al., *Far Term Fighter Force Modernization (U)*, SAI Report to U.S. Air Force Aeronautical Systems Division, SECRET, 1984.
- Worch, P.R., et al., *System Options for an Enduring Strategic C<sup>3</sup> Capability (U)*, Institute for Defense Analyses, Report S-548, TOP SECRET, 1983.
- Worch, P.R., *LPI Communications; Background and Solution Concepts (U)*, SAI report to DARPA, SECRET, 15 April 1983.
- Worch, P.R., et al., *System Options for Improving Joint Tactical C<sup>3</sup> Capabilities (U)*, Institute for Defense Analysis, Report S-545, SECRET, 1983.
- Worch, P.R., *Communications and Navigation Technology for Remotely Controlled Vehicles*, A Part of the RADC RCV R&D Study, 25 April 1972.
- Worch, P.R., *Communications and Navigation for Remotely Piloted Vehicles*, RADC, 16 July 1971.
- Worch, P.R., et al., *Laser Communications Study*, RADC, 30 December 1970.
- Worch, P.R., (Ph.D. Dissertation), *An Experimental Investigation of Generation—Recombination Noise in Double-Injection Diodes*, Oklahoma State University Graduate College, 1970.
- Worch, P.R., *Transverse Mode Studies in a Helium-Neon Gas Laser*, Oklahoma State University School of Electrical Engineering, Department Report, 1965.

## MAJOR ADVISORY ACTIVITIES

- 2006 Co-Chair, AFSAB Summer Study, “Air Defense Against UAVs”
- 2005 Member, DARPA Study, “Vertical Dominance”
- 2005 Member, AFSAB Quick Look Study, “Automatic Target Recognition”
- 2005 Member, Air Force Operational Test and Evaluation Advisory Group
- 2005 Co-Chair, AFSAB Ad Hoc Study, “Domain Integration”
- 2004–2005 Member, DARPA J-UCAS Senior Advisory Group
- 2004 Vice Chair, AFSAB Summer Study, “Networking to Enable Coalition Operations”
- 2004 Member, Aerospace Command, Control, Intelligence, Surveillance, Reconnaissance Center (AC2ISRC) Commander’s Advisory Group
- 2004 Member, Air Combat Command Commander’s Advisory Group
- 2004 Member, Air Force Operational Test and Evaluation Center Commander’s Advisory Group
- 2003 Panel Chair, AFSAB Summer Study, “Unmanned Aerial Vehicles in Perspective”
- 2003 Chair, Air Force Special Operations Command Commander’s Advisory Group
- 2002 Chair, AFSAB Quick Look Study, “Low Observable Aircraft Maintenance Technologies”
- 2002 Member, AFSAB Summer Study, “Immediate Attack Deep in Hostile Territory”
- 2001 Chair, Concealed Targets Panel, AFSAB Summer Study, “Sensor Technology for Difficult Targets”
- 2000 Member, ASD C<sup>3</sup>I Joint Services Advisory Group (JSAG) on C<sup>3</sup>I
- 2000 Chair, AFSAB Summer Study, “Air Force Command and Control—The Path Ahead”
- 1999 Co-Chair, AFSAB Summer Study, “Technology Options to Leverage Aerospace Power In Other Than Conventional War Situations”
- 1998, 2000, 2006 Chair, AFSAB S&T Review of Sensor Programs

- 1998 Member, AFSAB Summer Study, "Aerospace Operations in the 21st Century: An Investment Strategy"
- 1997 Member, AFSAB Summer Study, "Global Air Navigation System"
- 1996 Chairman, AFSAB Summer Study, "UAV Technologies and Combat Operations"
- 1995 Member, Sensors Technology Panel, AFSAB Summer Study, New World Vistas Long Range Forecast
- 1995 Chairman, AFSAB Study, "F-22 Electronic Combat Effectiveness Testing"
- 1994 Member, SAB Ad Hoc Study on Technology Opportunities for Wide Area and Local Area Communications
- 1994-1996 Member, C<sup>3</sup>I Science & Technology Panel, Air Force Scientific Advisory Board
- 1994 Chairman, Special Missions Aircraft Panel, Air Force Scientific Advisory Board Summer Study, "Mission Support and Enhancement for the Foreseeable Aircraft Force Structure"
- 1993 Member, C<sup>3</sup> Panel, Air Force Scientific Advisory Board Summer Study, "Options for Theater Air Defense"
- 1992-1993 Member, Air Force Studies Board "Committee on Counterforce Options Against Tactical Missiles"
- 1992 Member, Space and C<sup>3</sup>I Panel, Air Force Scientific Advisory Board Summer Study, "Concepts and Technologies for Global Power—Global Reach"
- 1990-1991 Chairman, DARPA Advanced Targeting Technology Program Red Team
- 1991 Member, Communications Architecture Panel, Air Force Scientific Advisory Board Summer Study, "Off-Board Sensor Data to Support Military Combat Air Operations"
- 1985 Member, ECM, Sensors & Navigation Panel and C<sup>3</sup> Panel, Air Force Scientific Advisory Board Summer Study, "Enhancement of Special Operations Forces (SOF)"
- 1982 Member, C<sup>3</sup> Panel, Air Force Scientific Advisory Board Summer Study, "Enhancement of Airlift in Force Projection"
- 1978 Member, The Technology Cooperation Program (TTCP), Subgroup K, Radar Technology
- 1977-1979 Group Member and Subgroup Chairman, NATO Project 2000, Phase II. Study on Target Detection, Location and Identification
- 1975 Co-Chairman, Joint Services Emitter Identification Conference
- 1975 Panel Chairman, EUCOM Target Acquisition Seminar
- 1975-1976 Associate Member, Air Force Scientific Advisory Board Panel on TDOA Emitter Location Sorting
- 1975 Associate Member, Defense Science Board Task Force on Identification, Friend, Foe or Neutral
- 1975 Co-Chairman, DOD Integrated Tactical Information System Study Group
- 1975 Member, CIA Study Group on Precision Guided Munitions
- 1974 Chairman, DOD NAVSTAR Weapon Guidance Workshop
- 1974 Co-Chairman, Tri-Service Millimeter Wave Workshop
- 1974 Member, DOD Intelligence Research and Development Council Task Force on Intercept and Position Fixing

#### **MISCELLANEOUS**

- Commercial Pilots License with Single, Multi-engine and Instrument Ratings
- First Class Radiotelephone License
- Senior Member, IEEE
- Member, Eta Kappa Nu
- Top Secret and SCI Clearances

**Peter R. Worch**  
41393 Philip Lane  
Leonardtown, MD 20650

7 September 2006

U. S. House of Representatives  
Committee on Science  
Rayburn Office Building 2320  
Washington, DC 20515

This is to advise you that over the last three years, I have been a member of the Air Force Scientific Advisory Board, and as such, have been a Special Government Employee and have been compensated in that position.

Sincerely,



Peter R. Worch

Chairman BOEHLERT. Thank you very much.  
I am quite familiar with the Rome——  
Dr. WORCH. Aren't we both.  
Chairman BOEHLERT.—enterprise. Yes.  
Dr. Prado.

**STATEMENT OF DR. GERVASIO PRADO, PRESIDENT, SENTECH,  
INC.**

Dr. PRADO. Good afternoon, Mr. Chairman and——  
Chairman BOEHLERT. Your microphone, please, Doctor. I don't think the microphone is on.

Dr. PRADO. Okay. Good afternoon, Mr. Chairman, Members of the Committee. I am very honored to have been invited to testify and share some of our experiences in the area of sensors, in particular in the protection of our borders.

Because the time is short here, I would request that my written statements be introduced into the record. I will now just address a few of the points in a more informal way.

My company and I have been involved in the area in the development of unattended ground sensor systems for some years now. We have had support from DARPA, Sandia National Labs, and various other government agencies. We have been able to participate in

some of the more important sensor programs and demonstrations that have been conducted over the last decade.

Unattended ground sensors is an area that combines the use of passive sensors. The ones which we specialize in are acoustic, seismic, and electro-optic imagers, you know, like either day imagers or thermal imagers, and combining them into an integrated system that can work together and produce actionable intelligence. These sensors, of course, have to operate. They will be designed with an extremely low power consumption, be able to operate in extremes of weather conditions of hot and cold. They have to operate in concert, several different types of sensors together, to produce the best intelligence possible and to extract the most useful critical properties of each of these types of sensing technologies. Finally, they have to be networked and—so that they can communicate that information to the user, sometimes over extremely long distances.

And I would like to just discuss an application that we have worked on where it involves the use of multiple sensors to survey an area of terrain in a very remote location. You would have acoustic and seismic sensors detecting the presence of people or personnel along a road or a trail. These sensors would alert a communications gateway device that is connected to a thermal imager, and that imager would then take pictures of the intrusion, you know, whether it is people or vehicles, track those vehicles, select the images that are most useful in terms of clarity and sharpness, compress them, and then pass them onto the communications device that can transmit that information, literally, to the other end of the world where that will appear on the desk of an analyst as in the form of an e-mail with a picture and the detection data.

This type of technology has been made possible visually by using various off-the-shelf technologies that have been developed, like GPS, communications satellites. A lot of the sensing technology that we use, for example, is derived from Navy projects dedicated to acoustic detection underwater. And all of this is now being put together. We need to work on the way to implement it more reliably at an affordable cost. We realize that when we put these sensors out on the field, we cannot rely on the abundant infrastructure that we have available in—you know, in the cities or, you know, populated areas.

So finally, you know, the real emphasis in terms of new research and development that needs to be applied here is not so much in the research on new transducers or cameras but in the application of intelligence that is embedded on the processors, the signal-on-image processing technologies that allow us to extract the information from the sensors and communicate them to the users in a form that is actionable.

I would like to conclude my statements by saying that, from a personal perspective, as an immigrant from Cuba, I am very aware—it has given me a perspective on the intense attraction that this country has for people that are seeking freedom and opportunity. And that creates an enormous demand for entering the country, some of which is channeled in legal means, but unfortunately, a lot of it is channeled through illegal immigration. And we have to address that problem, because it causes severe socioeconomic problems in our society.

I want to thank the Committee for inviting me, and that concludes my remarks.

[The prepared statement of Dr. Prado follows:]

PREPARED STATEMENT OF GERVASIO PRADO

Good Afternoon, Mr. Chairman and Members of the Committee; I am very pleased to have the opportunity to share with you my perspectives on the use of technology to improve the security of our borders.

I am Gervasio Prado, President of SenTech, Inc., a small defense contractor in Stoneham, Massachusetts. My working career spans 35 years spent at various research and development institutions. During the last 20 years I have specialized in the development of Unattended Ground Sensors (UGS), the last thirteen of them at SenTech, the company I founded in 1993. Over the last decade, we have participated in many UGS programs funded by DARPA, the U.S. Army and other agencies. I came to this country with my family from Cuba in 1960. We were able to enter the United States legally and my family's success is a testimony of the opportunities that this country offers to people coming here from all over the world.

I would like to talk about a technology widely used to survey border areas both here and overseas. Unattended Ground Sensors (UGS) are devices that can be placed in remote areas, where they will operate for a long time detecting, processing and transmitting information to military or law enforcement personnel that can act on that information. This technology has a long history that started during the Vietnam conflict, with a variety of acoustic and seismic devices being developed and deployed along the Ho Chi Minh Trail. After the Gulf War in 1991, there was considerable interest in using UGS to detect and locate mobile missile launchers and other high value targets. In recent years, the emphasis has turned towards the detection and localization of civilian vehicles and personnel. This change in emphasis coincided with the increased need and interest in using sensors along the border as an alternative to expensive physical barriers.

A variety of these types of sensors exist and some are in limited use along the Southwest border of the U.S. The preferred sensing technologies are passive (sensors that do not emit radiation to detect the targets) because they use less power and are more difficult to detect than active sensors. The technologies employed are acoustic, seismic, imaging—both infrared and visual and passive infrared.

*Acoustic sensors* are very effective in detecting ground and air vehicles. They are easy to conceal, do not need line of sight to the target and generally have very low power consumption. Their performance is affected by changes in the atmospheric conditions, but generally they will detect most vehicles at several hundred meters and heavy trucks or military vehicles at ranges of one kilometer or more. Acoustic sensors are not very effective at detecting personnel.

*Seismic sensors* are effective against both vehicles and personnel, although their detection range is more limited than that of acoustic sensors. They can be completely buried, making them very good for stealthy deployment. Seismic sensors can generally detect a person walking at ranges of 30 to 50 meters. However, their performance will vary greatly from site to site.

*Passive Infra-Red Sensors* are very effective as trip-line sensors. They are very inexpensive and economical, however they have to be carefully emplaced and are harder to conceal.

*Visual Imaging Cameras* provide excellent resolution pictures and are very reasonably priced if they are meant to be used during the daytime or twilight hours. In extremely low light conditions *Infra-Red Imagers* have a definite advantage. Their main drawback is that they are very expensive, although the price of IR cameras with un-cooled detectors has been coming down in the last few years.

At the heart of an Unattended Ground Sensor System there is a capable digital signal or image processor that has the task of extracting the relevant information from the transducer outputs. It is in the programming of this device that the art and science of sensor design is based. Sensors must also communicate their results in a reliable and economical way. Sensors are typically linked in a network to a communications Gateway that is used to concentrate the collected data and transmit it over a long haul link (typically a satellite link). The design of distributed sensor networks has become a very active field of research because of its many military and commercial applications. Distributed sensor networks are certain to find an important role in border surveillance.

The most effective utilization of Unattended Ground Sensors involves the use of multiple sensors of different types in order to exploit the unique capabilities of each. For example: Several seismic sensors can be placed to detect people walking along

a trail. These sensors, which can operate with minimal power consumption, will send a signal to a Gateway unit connected to a visual or infrared imager. The imager, which has relatively high power consumption, is only turned on when there is a potential target in its field of view. A built-in image processor on the imager detects the moving target, compresses the picture and hands it over to the Gateway to be sent to the user. Coordinating or fusing the data from sensors with very dissimilar capabilities increases the reliability of the reports, and reduces false alarms. It is important to remember that sensors cannot determine the intent of the targets detected, only their presence, location and direction. In this respect the use of imagers acquires a special importance when trying to allocate limited human resources over an extensive border area.

When we are considering the possibility of large numbers of sensors spread over a large area, the amount of information that can be generated could easily overwhelm the communications links and the personnel monitoring the sensors. The biggest challenges to the design of an Unattended Sensor system are: first to limit the number of false alarms to an extremely low rate; second, to extract and condense the relevant information as much as possible. To achieve these objectives, sensors need to be endowed with as much local signal and image processing capability as possible to make sure that only the essential information is reaching the user.

In summary, Unattended Ground Sensors is a mature technology that is available to provide surveillance over large areas of our borders and enhances the capability of our law-enforcement agents. We now have to apply our organizational skills to fund, deploy and utilize this technology.

Small companies are often at the cutting edge of technology development. They take risks that larger companies avoid and thus form one of this country's most valuable resources. From our perspective, the Department of Homeland Security can play an important role in furthering the development of new technologies that are being conceived on a regular basis at these small companies.

Some specific suggestions that would further these goals are:

- a) Providing better access to DHS personnel at the operational level in order to get first hand feedback of the utility of new technologies.
- b) Making test and evaluation facilities available to small companies, where they can get access to locations and scenarios that would otherwise be available out of their reach.
- c) Allowing small companies to keep more of the Intellectual Property Rights developed under Government Contracts as a way to stimulate participation in programs of critical national importance.
- d) An increase in the funding allocated to small companies through the use of Broad Agency Announcements, SBIRs, etc., would always be helpful. Equally helpful would be a reduction of earmarked funds and allocation of those funds through open competitive procurements.

I would like to conclude with the observation that securing our borders requires solutions that are well beyond the purely technical. While legal immigrants make a very valuable contribution to our society, illegal entries cause serious socio-economic problem. The flow of undocumented aliens across our southwestern border is driven by the lack of freedom and opportunity in their countries. The irresistible desire to immigrate to our country will only be eliminated when their countries have improved substantially their living standards and political institutions.

Securing our borders against terrorists and criminals involved in the drug trade is also a matter of the greatest urgency. Unfortunately, these individuals have the resources to gain entrance to our country legally as tourists, students or businessmen. Deducing the intent of a person arriving at one of our entry points is a most difficult problem without a purely technical solution. We simply need to remember that most the 9/11 terrorists entered the country with legitimate passports and visas.

Thanks again for the opportunity to share my thoughts with you today.

#### BIOGRAPHY FOR GERVASIO PRADO

Dr. Prado is President of SenTech, Inc., founded in 1993. He led the design of the acoustic-seismic sensor for the Steel Eagle and Steel Rattler sensors. He has also participated in the IUGS and Sniper Detection programs with DARPA. His company is currently participating in the development of the Intelligent Munition System for FCS and developing affordable hand-emplaced acoustic and electro-optic sensors.

From 1986 to 1993 Dr. Prado served as Manager of the Acoustic-Seismic Sensor Group at Textron Defense Systems where he led the development of the sensor for the Wide Area Mine. He has also held positions at Bolt Beranek and Newman, MIT Lincol Laboratory and the Charles Stark Draper Laboratory.

Dr. Prado received his Ph.D. From the Massachusetts Institute of Technology in 1971 and a B.S. in 1966. Dr. Prado was born in Havana, Cuba.

## **SenTech, Inc.**

38 Montvale Ave, Suite G-80, Stoneham, MA 02180  
(781) 279 9871 (781) 279 1873 (Fax) [g.prado@sentech-acoustic.com](mailto:g.prado@sentech-acoustic.com)

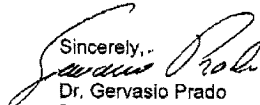
September 14, 2006

The Honorable Sherwood Boehlert  
Chairman, Science Committee  
2320 Rayburn Office Building  
Washington, DC 20515

Dear Congressman Boehlert:

Thank you for the invitation to testify before the Committee on Science of the U.S. House of Representatives on September 13, 2006 for the hearing entitled "**How Can Technologies Help Protect Our Borders.**" In accordance with the Rules Governing Testimony, this letter serves as formal notice of the federal funding I currently receive related to the hearing topic.

- \$3,189,441 Prime Contract DAA05-03-C0021, U.S. Army Morris Acquisition Center, acting for the Technical Support Working Group), from FY2003 to FY2006.

Sincerely,  
  
Dr. Gervasio Prado  
President  
SenTech, Inc.

Chairman BOEHLERT. Thank you very much.  
Dr. Pottie.

**STATEMENT OF DR. GREGORY J. POTTIE, ASSOCIATE DEAN  
FOR RESEARCH AND PHYSICAL RESOURCES, HENRY  
SAMUELI SCHOOL OF ENGINEERING AND APPLIED SCIENCE,  
UNIVERSITY OF CALIFORNIA, LOS ANGELES**

Dr. POTTIE. Mr. Chairman, distinguished Members, thank you for inviting me here. I am going to depart a little bit from my writ-

ten testimony, in order to respond to some of these things, but I am not secure enough to depart from my PowerPoint.

So I am basically going to tell a bit of a story about my own research in wireless sensor networks beginning in the mid 1990s and walk you through some of the lessons we learned from our initial enthusiasm to some continued enthusiasm but in new directions.

[Slide.]

So up here is a picture of some of the nodes that have been developed. A sensor node basically includes a sensor of some type, signal processing, a communications means, and some way of networking this all together so that you can do some processing in site, save energy, and potentially build larger networks. And our—over the years, sensor nodes have developed in two directions, basically trying to get the initial functionality made smaller and also just adding new capabilities as technology moves along. And we have been involved in both directions.

[Slide.]

Our early idea was that large numbers of nodes could—with limited capabilities could be deployed and collectively the network would be very powerful. As it turns out, this original vision had to be modified.

[Slide.]

So where we are now, I am Deputy Director of a—of SENDS, an NSF-supported STC, where we are deploying sensor networks for basic science applications, including contaminant transport and other environmental issues. Our thesis in forming the center was that only with the close cooperation of the end users, in our case the scientists and the engineers, would we end up with tools that would be very useful. And it turns out, this has been right. Our initial ideas about what the scientists would find useful were pretty well wrong, and over four years, we have really changed our direction radically in proceeding forward.

[Slide.]

So the—I am not going to read through all of this, but the basic lesson is that the original vision of thousands of unattended nodes was not realistic. The logistical issues in deployment are much larger than we thought, and in fact, as some of our other speakers have said, you need to include other components. In particular, you need infrastructure and support and a lot more attention to the user interaction: how does this fit in with what the end user really wants? And to that end, they need to be involved in basically all stages of the development.

As an example of a successful test, we ended up with a robotic node that is quickly deployed, and the scientists determined which instrument package had to be developed, and it resulted in something that was feasible. The kind of data we got out of this would not have been possible with a pure ground sensor deployment. We needed to think about infrastructure and other ways to support what they needed.

[Slide.]

I have also been involved in military-supported research, in this case DARPA, and this is an example of a deployment in the year 2000. And here there are two major lessons to draw from this. One is the logistics were really hard. Even deploying this small number



of nodes was difficult in the year 2000. We have progressed since then, but it is still not something to take lightly. And then the second thing is it works pretty well in finding vehicles. Finding vehicles at distance, relatively simple nodes will do the job, because the vehicles are loud, big, and generate wonderful signals.

But if you are trying to detect personnel, the matter is quite different. What you are trying to find is small. It is affected very much by the environment. Is a person walking on soft sand? Are you trying to listen in wind? Are you listening at night? Are you listening in the day? All of these things have a huge impact on the range you have with the sensors. And so, as has been pointed out by previous speakers, what you need is a complete system where you have, perhaps, ground sensors as tripwires, but you supplement it by imagers, UAVs, and most critically, the personnel who know where you should place the sensors. Just as an example of a border security possible application, one could think of a dense network of sensors running along a fence for a boundary, but the other deployments at choke points specifically designed to find vehicles, say, in locations where the Border Patrol suspects or knows that there is likely to be traffic. And this whole system has to interact with the users. I completely agree with Dr. Worch that this is an information integration problem, and it needs to fit in with what the agents do so that you don't end up with a system where the Border Patrol agents are supporting the technology rather than having the technology support the agents. And to that end, how do we get there with a practical research program? So this isn't simply a matter of letting out some contracts and saying, "In six months, you will deliver this. In one year, you will deliver the following," or down-selecting on that basis. This is something that requires an interaction between multiple research teams and the Border Patrol and other responsible agencies so that you have this direct user-technology developer interaction so that you end up in the end with a system that meets their needs.

Our experience is that the tools we develop may seem really cool to the engineers, and that is why we do them, but may be totally useless for the end users. It is only if they are involved in telling us how they are using the system, what is deficient in it that we can produce the tools that they really want and need.

And with that, I will conclude.

[The prepared statement of Dr. Pottie follows:]

## Multiscale Sensor Networks For Border Security

September 13, 2006  
United States House of Representatives  
Committee on Science

Prof. Greg Pottie  
[pottie@icsl.ucla.edu](mailto:pottie@icsl.ucla.edu)  
<http://cens.ucla.edu>

We gratefully acknowledge the support of our sponsors, including the National Science Foundation, Intel Corporation, Sun Inc., Crossbow Inc., Agilent, Microsoft Research, and the participating campuses.

Early sensor network work reported here supported by DARPA, and carried out by researchers at UCLA, RSC, and Sensoria Corporation

1

Greetings. I'm Greg Pottie, Deputy Director of the Center for Embedded Networked Sensing. I've been active in research in sensor networks in a variety of capacities since the mid-90s, and have published a textbook detailing what I've learned. I'll briefly describe what a sensor network is, some relevant experience in developing and deploying systems, and what I see as the main challenges for border security networks.



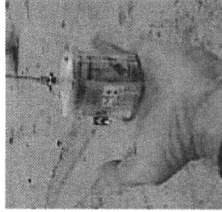
CENTER FOR EMBEDDED NETWORKED SENSING

## Early Sensor Nodes

LWIM III

UCLA, 1996

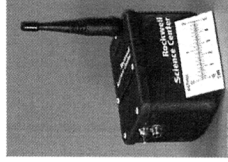
Geophone, RFM radio, PIC, star network.



AWAIRS I

UCLA/RSC 1998

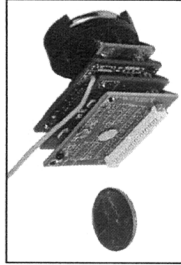
Geophone, DS/SS Radio, strongARM, Multi-hop networks



Sensor Mote

UCB, 2000

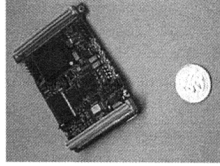
RFM radio, PIC



WINS NG 2.0

Sensoria, 2001

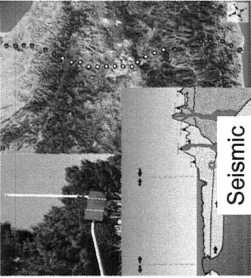
Node development platform; multi-sensor, dual radio, Linux on SH4, Preprocessor, GPS



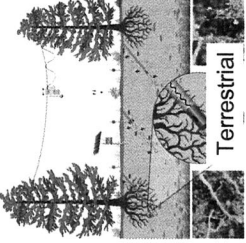
**Processor**

UCLA USC UCR CALTECH UCM

The simplest sensor node consists of one or more sensors, an energy source such as a battery, a computational engine such as a microprocessor, and communications capability such as a radio. Over the past dozen years, nodes have gone both in the directions of smaller size and increased capabilities. Some of these are now to the point that they are supported by commercial vendors. Our early idea was that large numbers of nodes could be deployed, and while individually not that useful, the network of nodes would be powerful. Practical experience, as we'll see, has modified this vision.

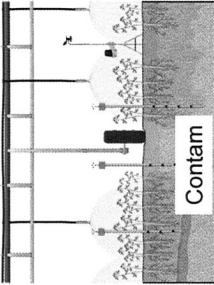


**Seismic**

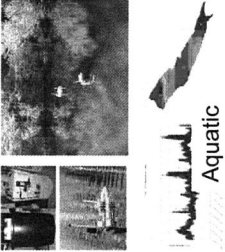


**Terrestrial**

*create  
programmable,  
autonomous,  
distributed,  
multi-modal,  
multi-user,  
observatories to  
address compelling  
science and  
engineering issues*




**Contam**



**Aquatic**

*...and reveal the previously  
unobservable..*



**CENS**

**Sensing at CENS**

CENTER FOR EMBEDDED NETWORKED SENSING

UCLA USC UCR CALTECH UCM

CENS is an NSF-supported STC, with the goal of developing sensor networks for basic science applications in seismology, contaminant transport in ground water, terrestrial ecology, and aquatic ecology. Our thesis in forming the center was that only with the close interaction of engineers and the end-users, the scientists, would useful instruments result. Four years into the life of the center, our technical research agenda has been radically changed by this interaction, with increased emphasis on robotic elements, humans in the sensing loop, and design for reliability.

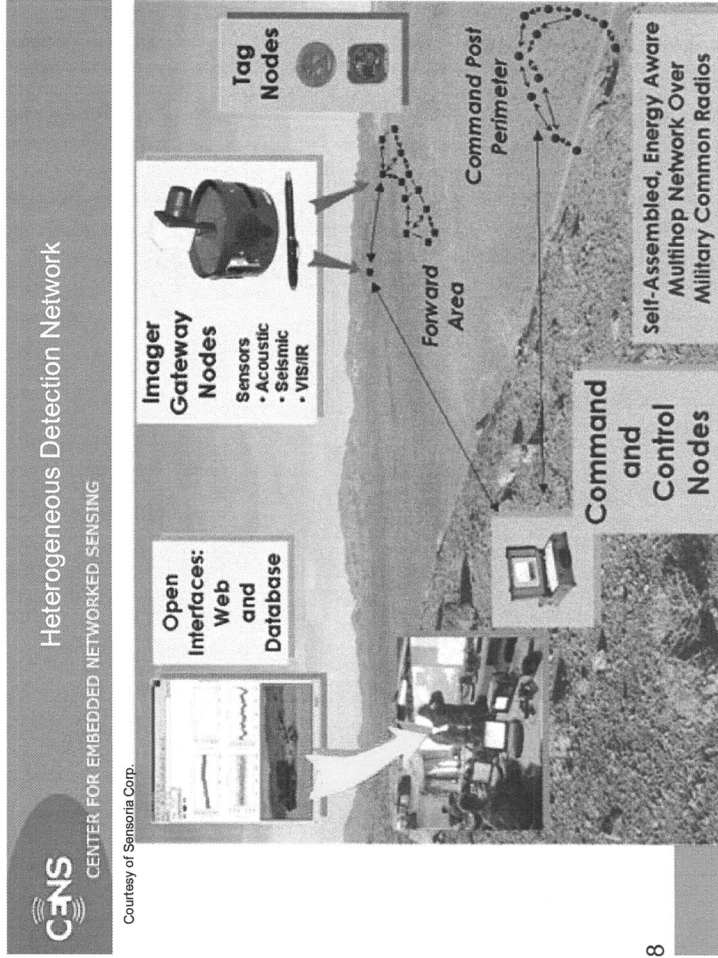
*Early themes*

- **Thousands of small devices**
  - Minimize individual node resource needs
  - Exploit large numbers
- **Fully autonomous systems**
- **In-network and collaborative processing for longevity: optimize communication**

*New themes*

- **Heterogeneous systems**
  - Tiered systems: optimize system as a whole
  - Inevitable under-sampling (in time or space)
  - Exploit multiple modalities (including actuation) and multiple scales
- **Interactive systems**
  - Design for human tier as well
- **In-network and collaborative processing for responsiveness, data quality, and data control (privacy): optimize sensing**

In essence, the original vision of thousands of simple autonomous devices was both unrealistic and incomplete. Small nodes continue to have a role, but only as one tier in a layered system with an emphasis on interactions with the expert human user. This leads to faster progress in meeting user objectives, and more flexibility in applying lessons learned from field deployments.



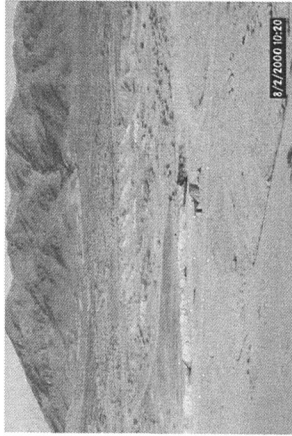
As an example, to study high altitude plant ecology, engineers and scientists collaborated to develop a robotic system with a suite of sensors specifically tuned to answer the science questions. This provided data at unprecedented spatial scales, in a form that would have been extremely costly to collect with static nodes. Variations of the rapidly deployable system have been used in other application areas.



## SITEX: Data collection for SensIT Program

CENTER FOR EMBEDDED NETWORKED SENSING

- SITEX August 2000 at MGAGCC  
29 Palms, CA
  - 37 Nodes
  - Operating for 2 weeks



Courtesy of Sensoria Corp.

6

UCLA USC UCR CALTECH UCM

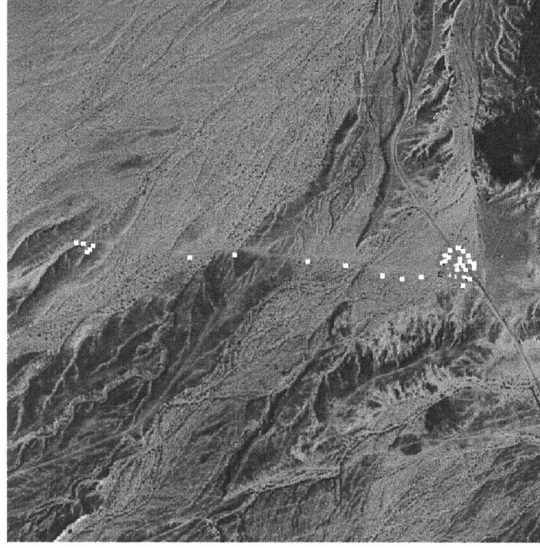
Another direction of sensor network research has been sponsored by DARPA. These pictures are from a deployment of static nodes, with the objective of tracking and identifying military vehicles. At the time, deploying even the 37 nodes was a major logistical task. Things have since improved, but long-term deployments in harsh conditions remain challenging.



CENTER FOR EMBEDDED NETWORKED SENSING

## AAV Traveling North to South

- SenseIT Sitex2000 data drives a java GUI
  - AAV in red
  - Nodes in white
  - Green circles are detections
    - Acoustic are magenta dots
    - Seismic are cyan dots
    - IR are blue dots



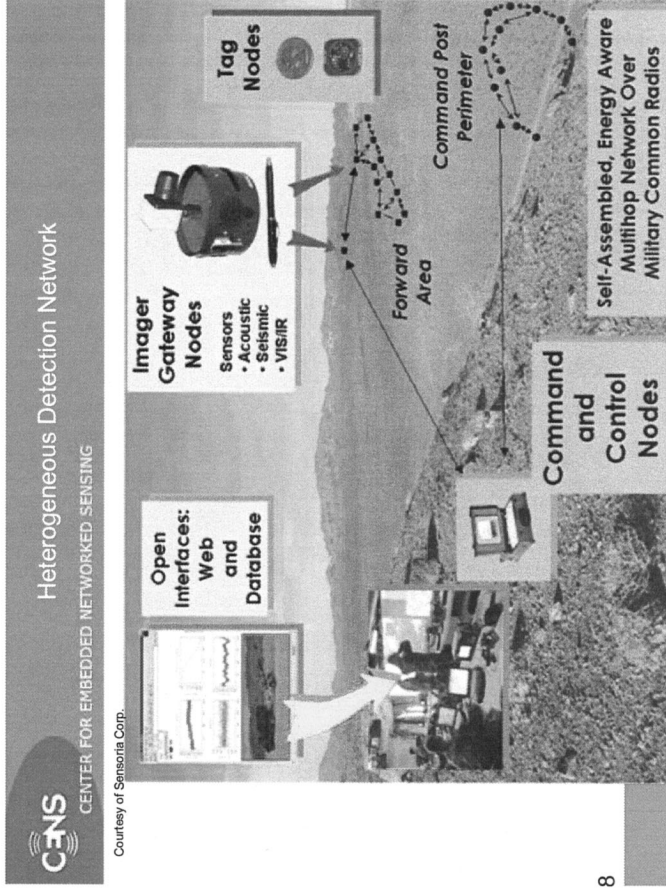
7

Courtesy of Sensoria Corp.

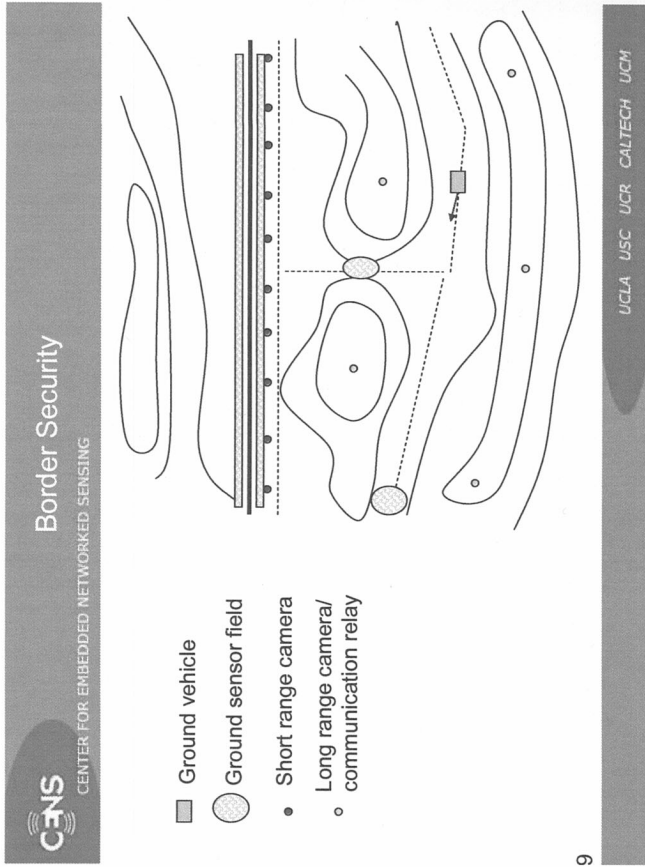
UCLA USC UCR CALTECH UCM

Illustrated here is a successful test in tracking an AAV. The message is that relatively simple sensor networks can be effective in tracking vehicles, sometimes at significant range.





But for personnel, the story is different. Instead of generating lots of noise, heat and vibrations, people produce only small signals and so a dense network would be needed. This density will strongly depend on terrain and obstructions, and even with sophisticated signal processing will produce false alarms. Thus, simple sensors must be part of a tiered network that includes imaging devices such as pan/zoom/tilt cameras and infrared rays. Humans monitoring the network at a distance then make the final detection decisions and determine what actions to take.



9

For example, along a border installation there may be ground sensor fields supplemented by short-range imagers. The fence may have sensors registering contact or strain, with power and other infrastructure supplied along its length. Terrain features may be such that vehicles are limited to particular regions or choke points, where additional sensors are placed. Longer-range imagers may also be placed at higher elevation to provide supplemental views, along with communication relays. Border Patrol agents in vehicles and on foot will provide important supplemental information, and the entire system must be designed so that it works for them, rather than they having to work to support a system (for example, wasting a lot of time on maintenance tasks and false alarms).

## Conclusions

- People/animals are difficult to reliably sense in outdoor environments with acoustic/seismic/IR sensors
  - Many confounding effects
  - Difficult calibration issues
- Cameras/IR arrays required, with humans making decisions
  - Goal of processing and simple sensors is to reduce number of humans required, and trigger attention on interesting things
- Redundancy and detection in depth is required
  - Sensors will malfunction
  - Choke points for vehicles can be intensely monitored
    - Trusted vehicles can have transponders for ease of ID
- Work closely with Border Patrol for system design
  - Design must be an iterative process, in which agents play major role in determination of components/placement/interfaces

To conclude, it's very difficult to reliably detect personnel with simple sensors. Wind, soil conditions, obstructions and a variety of other factors present many challenges. A better approach is to have simple sensors focus the attention of imaging devices. Signal processing will then reduce the image set, with humans making the final decisions. Due to the many ways systems can fail, and to deal with active countermeasures, redundant deployments are needed both with respect to sensor type and location. But in any case, it's almost certain that systems designed without the expert end-users, the Border Patrol, will not work in the intended manner. Our experience with multiple generations of deployments is that the end-users must be involved through multiple stages of prototypes and deployments. This is because what people think they need at the beginning is seldom what they realize they really need after seeing the capabilities and limitations of new tools. Thus, a phased development program is the most likely path to success.



CENTER FOR EMBEDDED NETWORKED SENSING

## References

- D. Estrin et al., *Embedded Everywhere: A Research Agenda for Networked Systems of Embedded Computers*. CSTB, NRC Report. National Academy Press, 2001.
- G.J. Pottie and W.J. Kaiser. *Principles of Embedded Networked Systems Design*. Cambridge University Press, 2005.
- [www.cens.ucla.edu](http://www.cens.ucla.edu)

### BIOGRAPHY FOR GREGORY J. POTTIE

Gregory J. Pottie was born in Wilmington DE and raised in Ottawa, Canada. He received his B.Sc. in Engineering Physics from Queen's University, Kingston, Ontario in 1984, and his M.Eng. and Ph.D. in Electrical Engineering from McMaster University, Hamilton, Ontario, in 1985 and 1988 respectively. From 1989 to 1991 he worked in the transmission research department of Motorola/Codex in Canton MA, with projects related to voice band modems and digital subscriber lines. Since 1991 he has been a faculty member of the UCLA Electrical Engineering Department, serving in vice-chair roles from 1999–2003. Since 2003 he has also served as Associate Dean for Research and Physical Resources of the Henry Samueli School of Engineering and Applied Science. His research interests include reliable communications, wireless communication systems, and wireless sensor networks. His current focus is on the information theory of sensor networks. From 1997 to 1999 he

was secretary to the board of governors for the IEEE Information Theory Society. In 1998 he received the Allied Signal Award for outstanding faculty research for UCLA engineering. In 2005 he became a Fellow of the IEEE for contributions to the modeling and applications of sensor networks. Dr. Pottie is the deputy director of the NSF-sponsored science and technology Center for Embedded Networked Sensing, a member of the Bruin Master's Swim Club (butterfly), the St. Alban's Choir (2nd bass), and is a co-founder of Sensoria Corporation.

UNIVERSITY OF CALIFORNIA, LOS ANGELES

UCLA

BERKELEY • DAVIS • IRVINE • LOS ANGELES • RIVERSIDE • SAN DIEGO • SAN FRANCISCO



SANTA BARBARA • SANTA CRUZ

DEPARTMENT OF ELECTRICAL ENGINEERING  
56-125B ENGINEERING IV, BOX 951596  
UNIVERSITY OF CALIFORNIA  
LOS ANGELES, CA 90095-1596

PHONE: (310) 823-8150  
FAX: (310) 206-8495  
EMAIL: pottie@ee.ucla.edu

September 8, 2006

Chair,  
US House of Representatives Committee on Science.

Greetings:

On September 13, 2006 I will be testifying in my capacity as a professor of electrical engineering at UCLA, and deputy director of the NSF-funded Center for Embedded Networked Sensing. Recent research contracts that are relevant to this testimony are:

NSF: Center for Embedded Networked Sensors, CCR-0120778, 2002-2007, \$20M  
NSF: NETS-NOSS—Algorithms and System Support for Data Integrity in Wireless Sensor Networks CCR-0520006, 9/1/05-8/31/07, \$400K  
NSF: ITR-Fundamental Limits in Sensor Networks CCR-0217620, 9/1/02-8/31/06, \$427K  
NSF: ITR-Networked Infomechanical Systems (NIMS) CCR-0307675, 10/1/03-9/30/08, \$15M

Many of these projects involve multiple investigators. A further basis for this testimony is older research funded by DARPA (outside the three-year reporting window).

Regards,

Gregory J. Pottie  
Professor, UCLA EE Department  
Associate Dean, Research and Physical Resources

## DISCUSSION

Chairman BOEHLERT. Thank you very much. And thank all of you very much.

I tend to be very simplistic as I approach some of these problems, and I think I speak for a lot of people when what we are really looking for is some master plan with all of the technologies and the integration with people using those technologies that we can put down on the paper and just implement the plan. If it was easy, it would have been done by now. It is not easy. I understand that.

And Admiral, one of the things that I like to get out of the hearings is, and we are privileged to have some of the most distinguished people in the business before us on these panels down here, as we have today, is we learn an awful lot. And I would hope that you would take away an awful lot from this meeting.

So I would like to begin the questioning by asking the non-government witnesses what you think the top couple of research priorities ought to be for DHS. And incidentally, I didn't sense anybody mentioning DHS. You talked about DARPA funding and NSF funding. Nobody was talking about DHS funding. But I would like to know what you think the top couple of research priorities ought to be at DHS and the border security area and whether you think those priorities are being adequately addressed. And then, Admiral, I would like you to respond to what the witnesses say.

You and I are in the same business. We are not short of people with ideas on how we both can do a better job. And you are the new guy on the block, and so I want to use this as an opportunity to help and—your education from the outside world.

So let us start with—well, let us go in the reverse order. Mr. Pottie, you go first.

Dr. POTTIE. Okay. Thank you.

So there were a couple of questions there. The first is why didn't I mention DHS funding. And the answer is because we don't have any. In preparation for this hearing, I looked at the website, and indeed, there are a lot of contracts that have short-term objectives and so on and oriented to COTS technology. And I can understand why that would be, but there haven't been large, long-range programs in the style of the way DARPA was in the '90s, oriented towards academia. But a more blue sky. Okay. And I can't responsibly put Ph.D. students on a contract that could end in a year. I, you know—except—so I—to engage in it, we need contracts that last longer, and that is why most of our funding is now NSF, because it matches to how we train the next generation of scientists and engineers.

As to what the priorities should be, I think it is reasonable that a large fraction of their resources are now going towards short-term, what can be done to plug the holes, because it is a problem that was neglected for a long time. And so a focus on commercial off-the-shelf technology is not bad, in itself. It is really more a question of proportion. So how much of the total pie is going to be given towards long range so we can train the engineers and scientists—

Chairman BOEHLERT. Pause right there. Admiral Cohen, can you respond to that?

Admiral COHEN. Absolutely. And you know me well enough, Chairman, we are not going to get into tit for tat, because I found myself agreeing, in large measure, as you would imagine, with the other witnesses.

What I found at DHS S&T Directorate when I got there was that the Directorate was aligned, in large measure, around projects and because of the horrendous events of 9/11. And as we go back in time and we think about those planes going into the towers and in the Pentagon and I was there, and we think about the Anthrax attack going on, there was a sense of what was the risk and what were the priorities. And so probability of occurrence versus consequence. The probability of occurrence in our mind before 9/11 of those events happening or chemical attack on our homeland or a biological attack other than the occasional hoof-and-mouth disease that we see agriculturally, was really not on our horizon. We understood the consequences, but we didn't think it would happen. And so the Administration and the Congress, in a bipartisan way, went ahead and focused on the consequence: the chemical, the biological, the nuclear, and the radiological.

And so the initial thrust of much of the research and development in S&T in the Department of Homeland Security focused on those four areas.

Chairman BOEHLERT. How are we changing?

Admiral COHEN. What—I briefed your staff, and I will put up, very quickly, one—just one chart is if you execute—

[Slide.]

Chairman BOEHLERT. I can read that clearly.

Admiral COHEN. I will read it to you, sir, but you don't need to worry about the black line.

Chairman BOEHLERT. Yeah.

Admiral COHEN. And we are working on improved vision.

Chairman BOEHLERT. Yeah.

Admiral COHEN. For me, not you, sir.

If you are aligned to project execution, as the projects change, you must constantly realign. This is not how effective, world-class S&T management organizations operate. And so what you see here is six departments with enduring disciplines of energetics, in my case, that is not nuclear and radiological, chem-bio, C4ISR, and I must tell you, as I went forward with this, people said, "Oh, no, that is too military. It should be command and control." But I will tell you that Dr. Worch has it exactly right. It is command, control, computers, communication, intelligence, surveillance, and reconnaissance. I don't have an air department. If need a platform, as Dr. Worch has so eloquently described, that is a UAV, that is in C4ISR. I have borders and maritime. Even though those are two 8,000-pound gorillas, customs and border protection and the Coast Guard, if they are put together, they encircle our borders, land and sea. Human factors. That was addressed. Man-machine interface. Critically important. Understanding the psychology of terrorism. And then finally infrastructure, and to me, transportation is infrastructure that moves—

Chairman BOEHLERT. Admiral, with all due respect—

Admiral COHEN. Yes, sir.

Chairman BOEHLERT.—I want to focus more narrowly. And I know the broad mission. And it is just—well, it is the biggest restructuring of government since the post-World War II era.

Admiral COHEN. Yes, sir.

Chairman BOEHLERT. Twenty-two agencies, 180,000 people. And I am not talking about all of the other stuff. We are focusing on border security. Should there be more of a mix with short-term and long-range projects? I think Dr. Pottie's suggestion—

Admiral COHEN. Well, he is absolutely right, and that is why I started out my testimony by telling you I now have three portfolios that cut across this with time, risk, and investment. Those are acquisition enablers. The HSARPA prototypical demonstrations to leap ahead. And then finally, the basic research, which gives us, in the eight- to ten-year timeframe, where the Ph.D.s and post-doctorates are investing their time, the change in paradigm. And that is how you will see, initially, the 2008 budget when it comes to you in February, and then more fully filled out in the 2009 budget. I have gotten the permission from OMB and from the Department to go ahead and make those changes as best I can in the existing budget structure now. We have Centers of Excellence, as you are well of, that—where we do invest the basic research dollars, but that is not universal—

Chairman BOEHLERT. Well, let me ask you this. Now you are the new guy on the block, so—

Admiral COHEN. Yes, sir.

Chairman BOEHLERT.—I mean—and your evaluation of where we have come so far in this new Department of Homeland Security, your Directorate specifically. You talked about projects, individual projects. You talked about consequences.

Admiral COHEN. Yes, sir.

Chairman BOEHLERT. Was there someone sort of concerned about integrating those projects and integrating the use of people and technology? Was there a master plan, did you find? Or is that still in the development stage?

Admiral COHEN. I will tell you that it varies, but in the area of borders, I have Merv Leavitt, who is now my Department Head of Borders and Maritime, because of his demonstrated performance in supporting the customer, which is Customs and Border Patrol, in this case, on SBI.net. And he has an eloquent brief that shows you—incorporates all of the technologies, near-term, mid-term, and long-term, as well as the integration, the common operating picture, the man-machine interface, the use of unmanned as well as manned vehicles, et cetera.

So in this area, we have been literally aligned with my customer, which is CBP, for this. But that, to me, is not adequate to get us to the next stage, and that is why I felt I had to restructure.

Chairman BOEHLERT. All right. I—Dr. Prado, would you care to share some observations?

Your microphone again.

Dr. PRADO. I agree with Dr. Pottie here that the reason that we didn't mention any DHS funding is because we haven't seen any, at least at my level. Most of our funding has come from sources like DARPA and the U.S. Army and so on. But what—



Chairman BOEHLERT. Give me your top one or two priorities for—that you think DHS should focus on—

Dr. PRADO. Right. Well, the first priority that I think we need, from my perspective, is to get a picture of how this border security problem is going to be structured and how we are going to decide what technologies would be best to use, how they would be deployed, and get a sense of, you know, what the operational utility of these sensors are, by having—letting us get some direct feedback from the agents in the field as they use the sensors so that we learn, you know, where it is that we need to add more intelligence or condense the data or transmit it faster.

Chairman BOEHLERT. But—

Dr. PRADO. That, to me, is the first priority.

Chairman BOEHLERT. Right. And you two should be comforted by Admiral Cohen's response. And I would think that maybe a year or two from now, when we have another panel like this to talk about this very subject, Admiral Cohen will be able to report, "Yeah, we have got the mixture, short-term, long-term, and we do—we have heard them. And we have learned from them. And we are investing both."

Dr. PRADO. Yeah. I don't envy his job as the—

Chairman BOEHLERT. It is tough.

Dr. PRADO. The amount of—range of problems that you have to address are so wide, you know, from the catastrophic 9/11 type events to the steady drip of illegal immigrants that are crossing the borders.

Chairman BOEHLERT. Well, one of my closest friends, we were elected together, we came to Congress together, and we are just close friends, was given a God-awful job. Tom Ridge. He was the first Director of Homeland Security. "Make our nation safer." Good gosh. I don't think he got to sleep—any sleep any night, any day of any month or any year.

Dr. PRADO. That is right.

Chairman BOEHLERT. All right. Dr. Worch, how about you?

Dr. WORCH. I am not privileged to know about the relative amounts of funding in the DHS. I am just not familiar with that part of it.

Chairman BOEHLERT. Well, I—quite frankly, I think I will agree with Admiral Cohen. They are modest, and we ought to put more into that Directorate, and this committee is trying to do that.

Dr. WORCH. Going into the areas where I think more work—where the high priorities should be, certainly one is information integration, as I mentioned. As Thomas Friedman put it, "Connect and collaborate."

Chairman BOEHLERT. Yeah, that is right. The world is flat.

Dr. WORCH. They need to get on with that. The world is flat. Right. The other area—and that involves interagency connection of information, and to do that, one needs to get common databases, data tagging, and so on. I would refer the panel to the Air Force Scientific Advisory Board's study on domain integration, which talks about how do you get information available in a form so that everybody can use it that needs it without the battle that we have now. And interagency is certainly part of that.

The other part is that airspace safety. Something needs to be done with that. The sensors are coming along for the UAVs. They are coming along because of military needs. There is one area that hasn't been worked hard enough, that hasn't been mentioned here, and that is defense of the borders against slow, slow aircraft, including unmanned aircraft that someone else might have to deliver goods across the border. That is another subject.

But the sensors, in general, for the UAVs are coming along quite nicely. The resolution is improving, their ability to detect even humans, but we need to get that airspace safety that—on—get FAA on board and get these airplanes in the air.

Chairman BOEHLERT. Admiral Cohen.

Admiral COHEN. That is exactly right. We have regulatory issues that I believe are "handle-able" with the authorities. I would tell you that the common operating picture that we are basically talking about is critically important. We do that today on the Web. You know. You don't worry about who you are communicating with or what program they are using, because in the marketplace, if people want to communicate by e-mail or send you attachments, it has to be compatible. We have to figure out how to be able to do that, not only on the borders, but throughout the government. And I would just tell you, 20 years after Goldwater-Nickles, there are still challenges with interoperability amongst the other department, of which I am no longer—

Chairman BOEHLERT. Oh, I know.

Admiral COHEN.—associated.

Chairman BOEHLERT. Mr. Tyler—I have extended my time, but I would hope my colleagues would agree that this is a good way to open it up, and then I will shut up for a while.

Mr. Tyler.

Mr. TYLER. Chairman Boehlert, I think your question was what should we invest in S&T in the short-term for this problem. The SBInet solicitations said an SBInet is supposed to do four things: detect entries, identify what they are, classify the level of threat, and then respond. With 10,000 miles of borders, that has to be automated. If it takes a lot of people, you haven't helped the problem. There is a lot going on in all of those areas.

In automated detection, there are a lot of algorithms that have been developed, not just for things like radar and sonar, but things in the desert for a whole lot of applications, and that needs to be brought to bear on this problem.

For identification, the big issue is false alarms. The current system out there, the ISIS sensors that are seismic and magnetic, they alarm every 44 seconds. They are probably driving the Border Patrol agents crazy. There are a lot of algorithms that exist right now to look at how you can reduce false alarm rates, both in the acoustic and magnetic sensors, as well as on the video, if you can get this—the video to pan.

So I think these are really two key areas for that.

For classifying the threat, once again, you need to look at how you would automate that. And for responding, there are decision aids. There are a lot of technologies.

So I think if you took the four areas that SBInet is supposed to go after, looked at what the key technical issues were, it would drive what the S&T is.

Chairman BOEHLERT. Admiral Cohen?

Admiral COHEN. And that is exactly the plan that has been in place for over the last 18 months. That is what Merv Leavitt has devoted his life to. And I think when the solicitation is fulfilled, you will see much of that in place, but again, it will be a phase.

Chairman BOEHLERT. Thank you very much.

And I have gone well over my time.

Mr. Gordon.

Mr. GORDON. Thank you, Mr. Chairman.

You did lay a good foundation for us.

Mr. Giddens, let us give you a chance to get involved here.

What is the state of the SBI strategic plan? Has it been completed? And if not, why not?

Mr. GIDDENS. I—sir, the plan is in development. We have, at least pending. As far as on the House side, there was language in appropriations to deliver that this November. We are on track to that and are working that hard to deliver that strategic plan, including the resulting programs and metrics that would go along with it.

Mr. GORDON. Well, do you see a problem in initiating the SBInet contract before completing the strategic plan?

Mr. GIDDENS. No, sir. We think one of the key cornerstones of this issue is being able to address the capacity and the capability we have at the border to address the issue. We don't think we can address the issue only by looking at the border. We see it as a continuum that speaks beyond the border in terms of what Dr. Worch talked about and in terms of intel and understanding what is coming. But there is clearly a big aspect of this that has to be addressed at the border, and we are comfortable that there is going to be a fifth to that—

Mr. GORDON. Well, won't the plan help to influence the kind of technologies you are going to need?

Mr. GIDDENS. Sir?

Mr. GORDON. Won't the content of the plan influence the technologies that will be incorporated into this SBInet?

Mr. GIDDENS. No, sir. Our intent is to be somewhat technology-agnostic in that we don't want to get linked into a certain technology, and as Secretary Cohen mentioned, the changing world of technology, I don't know what it will be 18 months from now or 24 months from now, but it is going to probably be different than it is now. But the performance and the objectives that we need in order to be able to detect, identify, classify, and respond, those are the things that we wanted to focus it on.

Mr. GORDON. And Admiral Cohen, what role do you see the S&T Directorate playing in selecting the contractor for the Net?

Admiral COHEN. I do not have a role in selecting the contractor.

Mr. GORDON. Providing any information? Any kind of—they are not going to look to you for some assistance there?

Admiral COHEN. I am—I will leave the acquisition to Mr. Giddens, but I am not on the source selection. And customarily, S&T is not on the—

Mr. GORDON. Is that a good custom here? Is that a good custom here?

Admiral COHEN. I believe it is, yes, sir.

Mr. GORDON. To not—for you not to be providing technical assistance?

Admiral COHEN. No, I do provide technical assistance. I am not on the source selection.

Mr. GORDON. Well—and then what will be your role in the oversight, the technical oversight of the system?

Mr. GIDDENS. As the Secretary Cohen indicated, his organization is providing technical assistance and support through the evaluation process.

Mr. GORDON. And oversight, also?

Mr. GIDDENS. And they will also be engaged—as we have looked at S&T to be our systems engineering arm. Mr. Tyler talked about the focus of systems engineering and the need for that. And early on, we partnered with S&T in order to lay that systems engineering foundation and also support the activities in terms of technology-sniffing.

Mr. GORDON. And how—I am sorry. I should know, but how long have you been in your position now?

Mr. GIDDENS. Since last November.

Mr. GORDON. And so what—I mean, I guess, would you concur that there were a variety of mistakes made in previous systems?

Mr. GIDDENS. I think we looked at it as the learning organization.

Mr. GORDON. Okay. Well, that is all right. Well, that is what I want to get. So what have you learned from those previous mistakes, and how do you see doing things differently?

Mr. GIDDENS. A couple things.

Mr. GORDON. That was a good answer. I mean, that was—you are—I think that is the right thing to do.

Mr. GIDDENS. And we are going to learn as well. I am——

Mr. GORDON. Right.

Mr. GIDDENS.—not going to sit here and say we are going to get everything right. And we intend to continue to be a learning organization.

Mr. GORDON. Well, what are some of the mistakes that you have learned from, and how do you intend to do things differently?

Mr. GIDDENS. One thing is we don't need to have a segregated approach to the problem set. In the past, we tried to look at this from a very particular aspect, a very technology-focused, and even maybe cameras and technology. In another avenue, we would go off and look at staffing. In another, we would look at tactical infrastructure. And that would give you a great answer from a technology perspective, but not from the system level and then trying to get a value solution. And I think that is one of the big lessons that we learned. And we have to take an integrated, comprehensive approach at solving this big, complicated problem.

Mr. GORDON. Well, I think it is healthy to—for that to occur, but I would certainly hope that the S&T Directorate does have a strong role, particularly in the oversight, and we hope you are going to do better, and we expect you, you know, to do better, but I think there continues to—there needs to be a technical oversight there.

Mr. GIDDENS. Sir, I look forward to you holding both of us accountable for that. I could not have asked for a better partner for S&T, and as Admiral Cohen, Secretary Cohen mentioned, he and I have known each other before. I am delighted to be able to work with him.

Mr. GORDON. Thank you. And just real quickly, Dr. Worch. You had mentioned that the reduction in NASA expenditures in some of these areas was harmful. Just quickly, could you give us some examples?

Dr. WORCH. Well, the most important example was this Access-5. It is not an acronym, to my knowledge, but it is a program that was started by NASA along with the UAV National Industry Team, I think it was called, Unite. And together, they were working this problem of the airspace management and how one could integrate those. Now that Access-5 has been terminated because of funding, and I don't see the laboratory—the military being able—or industry, being able to pick it up. It is expensive to do this research, but it is even more expensive to do the comprehensive testing that is necessary.

Mr. GORDON. Thank you.

Chairman BOEHLERT. Mr. Akin.

Mr. AKIN. Thank you, Mr. Chairman.

I, unfortunately, had to step out for a minute, so I may be plowing some already plowed ground. I just wanted to ask. I have heard you talk about sensors and detecting. I spent a couple days down at the border at El Paso and Juarez and just kind of watched the operation there. They had the cameras, chain link fence and all. Chain link fence, I would like to have the contract in the wire that they used to repair all the holes that people cut in it. And it seemed to me that one of the solutions is to come up with some type of fence that you can't cut holes in. and one of the technologies is the concept that I think the military has used to—for, like, enclosing compounds, which is a microwave technology, which generates a tremendous amount of pain if you get into the field, but it doesn't do you any physical harm. So you just basically create a shield of microwaves. Is that something you have talked about, and is that practical in the sense that you can't cut holes in it? Where is that technology?

Dr. WORCH. I am aware of that technology. It is relatively short-range. It is clearly effective. The question is, is this something that a democratic society would want to do. I mean, I am out of my ballpark now, out of my league, so I ask your forgiveness for that. But I—yes, it can—

Mr. AKIN. So you think the technology works. The question is the politics?

Dr. WORCH. I would say so. Now the technology is not long-range. It is relatively short-range.

Mr. AKIN. And if you had to do a border—can you make a screen of these things, put a whole series of towers or whatever it is, in a row?

Dr. WORCH. You would need a large number of them, because you have the near-far problem. That is you want to inflict some pain on the person that is far away, but you don't want to fry the one that you aim it at that is nearby, right?

Mr. AKIN. Right.

Dr. WORCH. So you have to be very carefully in the use of that technology, and you better be sure that it is an intruder that is not—that is—that it is truly an intruder and not an American citizen that has gone astray here.

Dr. POTTIE. There is also—

Mr. AKIN. How about expense on that? Is that very expensive or—

Dr. WORCH. It is relatively expensive, particularly when you consider how close these would have to be deployed. It is nice if you have a point defense problem. I want to defend this radar site or this ammunition storage area. It is not so good when you want to create a fence.

Dr. POTTIE. There have also been issues with microwave at high levels where communication towers have caused cataracts before it was well regulated. So I am not—I think there would be a lot of people who would be unhappy about long-term exposure issues, particularly near populated areas.

Dr. PRADO. I would like to comment, also, that any use of active sensors, like microwaves or radar, that sort of thing, are very power-intensive, and they are usually relatively simple counter-measures that people can learn fairly fast to protect themselves. The best sensor—the best way a sensor can work is if the intruder does not know that the sensor is there, in other words, that operates in a stealthy way and it can be hidden from sight so that not only the current intruder but the next one and the next one get—trip that sensor, and it doesn't get destroyed by the people who are trying to come across. So, you know, more cost-effective is a network of, like, unattended ground sensors that will alert the law enforcement personnel that somebody went by. You want to be able to apprehend that person and send him back to where he came from. You don't want to particularly pick up a dead body on the field from some border protection measure that you use.

Mr. AKIN. Yeah. I guess the thing I saw was you have got a whole crews of people with vehicles stationed all along a long line, and you have to replace them every shift. There is a whole new group of people. And that looked to me to be a pretty expensive solution, too, so you have got a sensor that says somebody has come across. Now you have got to go find them, and they are hiding in somebody's field or whatever it is. It is—does that look to be expensive, too? So that is why I was asking. But thank you for responding.

Admiral COHEN. Congressman, one of the things that all the comments take you to and that is power and infrastructure. And you talked about unattended ground sensors, et cetera. For them to work, they require power, and people have come forward to me, even in the short time I have been on the job, with e-mails and phone calls and face-to-face, and we had one proposal of—for being able to get electrolytic power from a cactus. Now these are small, low-power sensors, but because of microelectronics, they will do the job. Or from a tree, because of the chemistry within there. So in that sense, we heard earlier from Dr. Pottie, the numbers. He talked about 10,000 sensors. Sandia lab has done a lot of this kind of work. Small, little sensors, all linked, but you have got to power

them, and you have got to power them for the long-term. So we need to look not only at the microwave, which was a joint Navy-Air Force initiative that we have been looking at, and it does work, high power, we need to look at the low power, otherwise, it is all about batteries and electrical cables.

Chairman BOEHLERT. Mr. Lipinski.

Mr. LIPINSKI. Thank you, Mr. Chairman.

Everyone who is on the Committee knows I have a background in engineering, a mechanical engineer. I spent a little time as a systems analyst. So I appreciate all of the technical background and the details that all of you have gotten into here. Unfortunately, when I go home and talk to people, they say, "Secure the borders." In looking a little more at it, can we secure the borders? I mean, that is, essentially, the question. So all I want to do is ask, can this really be done. Can we really secure the borders? Because we talked about all of the technical aspects of it, but I am not yet convinced from all of this that what—or I should say, I am not really sure that all of you believe this can be done in terms of technologically, and there is also the political question, which got into some of those ways of possibly securing the border, ways that we may or may not want to do. You know, people say crazy things like, "Mine the borders," or something like that. I mean, it is outrageous, obviously. But thousands of miles of borders. Can we secure it? And how long will it take to do it? and I know especially all of you—this is putting you—and I am not here—and I am not asking this question to bring you back here in a few years and grill you on this, your answer, so I know you all are probably going to have to dance around this a little bit. But I am looking for you to give me an honest answer. Can we do it? How long will it take? And we will start with Secretary Cohen.

Admiral COHEN. Well, to the best of my ability, I always give an honest answer. I do that for two reasons: one, it tends to work, and two, at my age, I don't have to remember what I said.

But the short answer is, yes, the borders can be secured. The land borders, the sea borders, the air borders, the under-land borders. The question is, to what degree do you want to have them secured. Do you want them absolutely secure? I mean, we don't like speeding. We don't like drunk driving. I mean, there are many things that we try and control and alter, et cetera, and we decide what level. Even prison breaks, from our maximum security prisons, occur. So this is really a policy, political resources decision. But I think what you have heard and with your engineering background, you will appreciate this, the beauty of America is we are very optimistic. If the President says we are going to put someone on the Moon this decade, then we believe it. And do you know what? We put a man on the Moon. So we can do this, but at what cost and on what timeline and to what degree of fidelity.

Mr. LIPINSKI. No one has talked anything at all—and they are not just talking about all of you here, but no one in the government has talked about it, any kind of timeline. Okay. So I say 95 percent—I want to stop 95 percent of the people coming in who are coming in now. Five percent can still—you know, we will allow that. What will that take? How quickly can we get that done?

Mr. GIDDENS. As you somewhat indicated as you asked the question, probably at least those of on this end of the table are probably not going to give you a completely satisfactory answer to the timeline. A large—let me answer the first part of the question first. Can it be done? Absolutely. And I don't just say that because that is part of my role and that is my job at DHS is to put together a systems comprehensive approach to do that. So—but I believe that can be done. I am convinced it can be done. We are working hard to lay out that plan to deliver to the Congress later this year on how to do that. The speed of that is going to largely be governed by the Nation's will to invest treasure to make that happen. It is not going to be an inexpensive undertaking. I am not going to sit here and say you are going to get it by rubbing two nickels together to secure the border. This is going to take investment, and it is going to take a well managed investment, but it can absolutely be done. There is clearly going to be some point, whether return on the investment to get the last one or two percent is going to engage a lot of discussion about whether to continue that. Is 95 percent good enough? Is 94? Is 96? That is clearly going to be a national level debate, but it can absolutely be done.

Mr. LIPINSKI. Okay. Will someone venture 95 percent—how many billions of dollars in how many years if we want to get it done? Any of the four of you venture?

Dr. POTTIE. Okay. So my answer is that, in the short-term, it would be enormously expensive. And you would need physical barriers, probably cameras everywhere, and you would need people behind those cameras until the detection algorithms get better, and you would need other measures to deal with bad weather when your cameras aren't working all that well. And so if—but over time, this is the point of doing research, you would hope to make that whole process cheaper. By working with the end users, you would develop systems that would work better over time and hopefully make this both less expensive and more effective. So it is—I—well, I can't really give you a timeframe, because I never designed anything in this scale.

Mr. TYLER. Congressman, if I might offer. At the beginning of the Cold War, we had a real problem with Russian submarines right off our own coast. And Admiral Cohen is an old Cold Warrior, as I am. We are talking about 10,000 miles of border here. And in the Cold War, at the peak, we surveyed 12 million square nautical miles of ocean and did it exquisitely. And it took a decade to get SOSUS and SURTASS and other Navy systems up. And what it took was commitment. It took money, and the money was measured in the billions, but it was not exorbitant. But it took, basically, a spiral development. It took S&T and commitment over a longer period of time. Now if we want to solve this problem in three years, it could cost us a fortune, and we are likely to make a lot of mistakes. If we have got commitment and we are willing to see those numbers come down with time reasonably, then I think this is a solvable problem, and it is one that is going to be solvable with the kind of money that we might want to put towards it.

Mr. LIPINSKI. Well, I certainly think it is something that we need to do, we must do, and I know it is a very difficult question to answer for all of you, but I thank you, Mr. Tyler. That is something



that I can go home and I can tell my constituents. That is something I can tell them and explain to them that makes a little bit of sense.

But thank you.

Dr. PRADO. Let me make a comment, also.

Mr. LIPINSKI. Yes.

Dr. PRADO. With regards to making the borders really secure, to make it—do it by purely technological means would end up being extremely expensive, and these are questions that don't really have a purely technical solution. The desire to enter this country by millions of people who don't have the same opportunities that we do is just too great. And so you know, we would be spending enormous amounts of money trying to stop those people. I wonder if some of that money would be better spent in fostering economic development in the other countries so that once their centers of living and political systems are at least, you know, farther along and they have more hope, they—there is not so many people who have a desperate desire to risk their lives and come into this country.

Mr. LIPINSKI. Well, I think you are very right about why people are coming—most of the people are coming into this country, and of course you—these other parts of it we don't deal with here on the Science Committee, but I—

Dr. PRADO. Exactly. I am just pointing out that this is a—

Mr. LIPINSKI. There is no question. Yes, you are—

Dr. PRADO.—problem that has a non-technical—

Mr. LIPINSKI.—correct.

Dr. PRADO. That—a part of a solution that is not technical.

Chairman BOEHLERT. Thank you very much.

Mr. LIPINSKI. There is no question about that.

Chairman BOEHLERT. The gentleman's time has expired.

Isn't it really fair to say that the technology exists? We know how to guarantee that we have security of our borders, but then you cost it out, and it is a jillion dollars. I mean the technology exists, so what we have got to do is invest in lowering the cost of doing what we know we can do right now. Is that a fair statement? I mean, there—some people would make this Fortress America, put a fence all around America. The—I don't know who wants to do that. I am sure there are some people who say, "Why don't you just do that?" Well, I don't think that is a very good idea, and I don't think probably any of you do, either. And—but you could cost—that we know how to do it, and we could cost it out, and we could get a price tag, but—so it is not so much a technological question. It is a policy question that is going to be settled in the halls of the Congress, not in the laboratories of America. But what we have to do, it seems to me, and one of the reasons why I got so excited about insisting that we go forward with a hearing like this a couple of months ago, and today is a result of that, is we have just got to pay attention to this subject in a very meaningful way. And we can't expect miracles. We can't be unrealistic. But we have got to be very practical.

Admiral COHEN. I think you are exactly right, Mr. Chairman. One size will not fit all. In an urban environment, we will most likely need physical barriers, because the time from crossing the border to being able to go into buildings or mass transit is very

short. Whereas in the more rural, whether it is the northern or the southern border, we have the ability to have defense in depth. And an initial trip point, monitoring—and Border Patrol does this every day. They follow, and then when it is convenient or it is dangerous to the individual, they make the intercept and proceed from there. And that is—we talked about not only the timeline, we have talked not only of the technology, we have talked not only of policy, we have talked not only the cost, but it is also the environment and how we want to go about doing that. So the comments that have been made on system of systems and system integration and giving the analogy to the Polaris program and other things of that nature are right on the mark. This is tough stuff. And as we have already heard from Dr. Pottie, it is not until you have it in the field and the customer-to-customer, the Border Patrol agents and the Coast Guardsmen are actually operating this and seeing how we can improve that we will get to the next stage. But we are in this for the long haul, and I believe that Congress is and the American people are, also.

Chairman BOEHLERT. I see Dr. Pottie on the edge of his chair. Did you want to intervene at this—

Dr. POTTIE. Oh, no. I was going to agree with him.

Chairman BOEHLERT. And Dr. Worch, you had—

Dr. WORCH. Well, I am less optimistic about the 95 percent, but I would say that if we can go for the 80 percent solution and deter another 15 percent of the individuals from attempting it, then we may be back up to the 95. That is to say there are a lot of portions of the border that are going to be very tough to put sensors in to maintain a sensor field. But I think if we can start, we can evolve a capability at some percentage, whether it is 80 percent or 90 percent, and then hope that some of the other—some of the individuals that are part of the other 20 percent or 10 percent are encouraged to proceed in a more legal way.

Mr. GIDDENS. Mr. Chairman, if I could quickly add to the point about the 15 percent. The Department is into the practice of catch-and-release, and we have seen some great results in terms of deterrence as a result of that. And I think it is going to be incumbent upon us not to just look at where the solution set at the line on the border but understand what happens beyond the border, at the border, and in the interior in the way that we work with private industry and work site compliance and making sure that we are hiring people that are documented and authorized to work.

Chairman BOEHLERT. Mr. Gutknecht.

Mr. GUTKNECHT. Thank you, Mr. Chairman.

That is a nice segue to what I wanted to talk about, because I think if you focus purely on defining the border and defending the border, I think you are sort of missing the biggest part of the equation. Let me give you an example. I am aware of this only because of some of the employers in my district where—and I will give them the benefit of the doubt. They are trying their best to hire legal employees. But the trade right now in illegal or counterfeit documentation has become phenomenal. In fact, the local law enforcement know how much it costs to buy a counterfeit driver's license. As a matter of fact, I learned that in one town in my district, you can buy a Puerto Rican birth certificate for about \$600. And

of course, if you are born in Puerto Rico, you are a U.S. citizen. So this business has gotten incredibly sophisticated, and it starts not just at the border.

I just want to throw out this question, I guess, and perhaps one or more of you can comment on this. One of the things that many of the folks who come here illegally know is that it will take upwards of 11 months before Social Security will notify an employer that there is an employee working under a Social Security number, which does not exist, or a Social Security number under which someone is working in Worthington, Minnesota and Laredo, Texas at the same time. Do you believe that creating an electronic system that would respond a little faster than 11 months is technologically possible? And could it be done at relatively low cost? And that is a loaded question, because we know it is done. It is done every day. A few years ago, I had the unfortunate circumstance where I lost my billfold, and by the time I realized what had happened, I had already gotten a call from my credit card company that I was making some rather unusual purchases. And so I knew what was going on, and the law enforcement knew what was going on. And more importantly, the credit card company knew long before I did. It didn't take them 11 months. It took them about 11 hours.

And so I want to come back to this. One of the areas where we have got to focus more of our attention on is some kind of an ID system and an electronic surveillance system within the government itself, with the systems we already have. I mean, we have Social Security cards. We have Social Security numbers, and yet, we are just painfully out of step. Does anybody want to comment on that, what we can do to make sure, number one, that employers have confidence that the documents that they are getting are real, and number two, that we track these people so that if they are using a false Social Security number, we can get that information to the employer much, much faster?

Mr. GIDDENS. Sir, I will start with that, and then part of this I may look for Secretary Cohen to elaborate on an aspect of it.

But clearly, you have touched on a nerve that, while we focus on the border and it is a very visible aspect, it is not the only thing that we can focus on. We have to work with private industry and find a way that is fast and efficient for them to verify the employment eligibility for people that they want to employ. The Department currently has a program called Basic Pilot that is trying to do that where private industry sends in basic information and there is a check to see if there are any mismatches with that, and response back for that is pretty quick. Now that is not nationwide deployed, and it is currently a voluntary program, but it is something that we are doing to try to provide private industry some tools. We think it is going to be very incumbent upon us to do that. If we are going to look to private industry and say, "You should only have people that are authorized to work," okay, how do they know? That is a big problem for us. We are working that hard, and we are looking to expand the use of Basic Pilot.

You talked about document fraud. There are efforts ongoing within the Department that S&T is involved in as well as ICE. An organization within DHS is involved with that in document fraud. Customs and border protection is working this issue hard at ports

of entry. It is a big problem with the printers and the capability now that people can just set up, you know, in their bedroom with their computers and printers. It is really going to be a hard problem to tackle. But we have got to take that on and be able to really address that. We work very hard with the Social Security Administration to try to find the right way to get some access to the data they have. As you said, I think it would be interesting to go through and have somebody to run a routine and find out how many people are posting income in ten different zip codes. That would probably be a fruitful area to go—

Mr. GUTKNECHT. Well—and that would be relatively easy to do, I would think. I mean—let me just make this point, because my time is about expired. And I want everybody here to think about this. You know, what happened on 9/11 happened five years ago. Okay. And as far as I can tell, and one of the reasons we are concerned about this, obviously, it is affecting our labor markets. You know, I think it is artificially holding down labor rates. It is increasing costs for schools and hospitals and everything else. Illegal immigration is a big issue. And that is certainly one concern.

But according to the statistics we have seen is that about four percent—the estimates are that four percent of the people who cross our borders are coming across either for illegal purposes, in other words they want to sell drugs or they are involved in crime, or they are from nations of interest. That should be a real chilling concern to everybody in this city and everybody in this room. So you know, five years into this, I don't think we are much further along than we were five years ago in terms of securing our own border, and part of it is we have got to come up with ID systems that slow down the influx, and we have got to do more to use whatever technology is available to protect our borders and ultimately to protect the American people.

Mr. GIDDENS. Sir, that four percent is one of the reasons that we think part of the comprehensive program should include some type of temporary worker program to allow us to try to funnel those people through the legal means so that we can really focus on the four or so percent that are really the ones of interest.

Mr. GUTKNECHT. Let me just say, in response to that, I mean, I am not totally adverse to that, but I think until this Administration demonstrates that they are serious about controlling our borders and enforcing the laws that are currently on the books, that is really tough sell in my district.

I yield back.

Chairman BOEHLERT. Thank you very much.

Mr. Green.

Mr. GREEN. Thank you, Mr. Chairman and Ranking Member.

And I would like to indicate as well, Mr. Chairman, that you do a thorough job, you really do. And you will be missed. You will be missed greatly. I—the only consolation that I have is that—knowing that I may be in the majority. Thank you for your work.

Chairman BOEHLERT. I never pay.

Mr. GREEN. Well, you know, fairy tales come true. It can happen to you and me.

Thank you so much, members of the panel. You were—provided us a wealth of information. And much of what I wanted to talk to

you about has been discussed, but I will just simply say it another way, I suppose.

In my fair city, who had a regional mobility plan, or a mobility plan that was proposed, and this plan, if 100 percent placed—put in place such that we had it 100 percent effective, would only impact five percent of the traffic. That was the plan. And I mention this to you, because if our plan here is 100 percent effective to impact 100 percent of those who will try to cross the borders and it costs us about 100 percent of our capital, I don't know that we have really spent our money as wisely as we should have spent our money. The Chairman said a kajillion, or some large number, of dollars. And that causes me a lot of concern, because one of the panel members indicated that it is judicious, it is prudent to look at the conditions where most of the people are coming from and try to be my brother's keeper, to some extent, and see if I can help improve the conditions so that I don't have as many people to contend with. If we are securing ourselves now from people who want to harm us as opposed to securing ourselves from people who want jobs. At some point, we have to decide why are we securing ourselves so as to understand why it is necessary to spend a kajillion dollars. I think that, in the long run, to get to the 95 percent level, based upon what I am hearing you say, it is going to be exceedingly expensive. Exceedingly expensive. I never like to use the term "too expensive" when it comes to securing our country, so I will not say that it would be too expensive, but I would hope that we will include in our security efforts—someone has talked about ID, identification methodologies, but also looking at what is happening to cause people to find themselves coming in in the middle of the night, living in the shadows of life, leaving to go back home to see people that they care for dearly and then try to come back into the country under the cover of darkness again. There is a lot going on here that securing the borders will not, as we are talking about it, the technology just won't offset. I don't see how it will offset it, given the needs of some of our brethren in some of our border countries, or at least one.

And finally, we—this conversation seems to be so focused on Mexico. Perhaps I am wrong, but it just seems that way to me. It just seems like it is. And we have had some folks to try to come in through the northern border who didn't mean us a lot of good, and it seems like we ought to talk a little bit about the northern border. And it seems to me like before we had a lot of these concerns about the southern border, we were having people to come in across the Gulf of Mexico. And we have got policies, wet foot, dry foot, whatever. We—some of those things create an inducement for people to come, knowing that I can get one foot on dry land. "If I get one foot on dry land, I can go on and work my way into the country and become—possibly become a citizen." And I don't begrudge anybody, but I think inconsistent policies create a lot of the problems that we have when you don't have consistent policies and people can see the inconsistencies. But also, I think these inconsistent policies create a lot of disrespect for policies, and people can clearly see that some are being treated better than others, and they can't rationalize it.

I thank you for your kindness, and I appreciate very much your indulging me.

And Mr. Chairman, I yield back the balance of my time.

Chairman BOEHLERT. Thank you very much, Mr. Green.

Mr. Rohrabacher.

Mr. ROHRABACHER. Thank you very much.

And first and foremost, I would like to recognize Admiral Cohen for the great job that he did at the Office of Naval Research and suggest that he is a fine selection for someone who should oversee the technology and the technology development that we need for our national security in terms of homeland security. And I have worked with him in the past, and I look forward to working with you in the future on this.

With that said, I just—frankly, Mr. Gutknecht said it well. And I think we do have the technological capability, for example, to have the identification cards and the identification systems, not only for people who are seeking employment or people who are seeking government benefits, but also for people who are trying to enter our country through our legal portals, in terms of visas, et cetera. We have that capability, and we have not perfected it. I think that is a black mark on this Administration, and we should have perfected it already. I mean, frankly, five years into 9/11 we don't have that system perfected. It is ridiculous.

Second of all, in terms of the border, I would like to just tell you, gentlemen, it is not a matter of funding. And I am sorry. And I say that to the Chairman, as well. He—we probably disagree in this. This is a matter of will. Every—you know, every time we—people come here to Washington you hear it, “Well, just spend more money. Spend more money. It is a matter of how much you invest.” I am sorry. That is not it. The fact is that we have two Border Patrol agents right now who are on—who are being prosecuted for attempted murder for shooting at an illegal immigrant who was trying to smuggle 743 pounds of marijuana into the country, and as he ran away, they shot at him, and now, they are arrested. Now what do you think that does to the Border Patrol? Think. How much technology can make up for that type of demoralization that you are going to have when you have got two veteran officers, who are targeted by our U.S. Attorney's Office, and bringing the drug smuggler back from Mexico to testify against them? You know, this is—we can do things in this country. We have the ability to do things in this country, especially on our border, if we had the will to do it. This Administration has not wanted to do it, and right now, even with the technology that we have, and again, what I would suggest is—Admiral, your job should be basically how do we get the technology that you know already exists into play rather than how do we develop new technologies for the future. How do we get it in play so we can capture more illegals at the border and secure those borders? And we have got that capability now. We have got plenty of sensors. We have got plenty of drones. Now if there are some regulatory issues that I heard about earlier about using some of this technology, that is when we can work together. That is what we can do. You don't have to spend more money on the budget for that. That is just a matter of willpower and committing ourselves to do the work. Now that border could be secure, and it could have

been secure all of this time, but there has not been a will on the part of this Administration or the past Administration to do it. So for example, we are talking about—look, we have got the Civil Air Patrol. We have got the Boy Scouts. You could have veterans organizations. You could have volunteers for the border that could help be the eyes and ears of people to make sure that our country is safe and secure. And I will tell you, after 9/11, we would be flooded with volunteers if someone tried to organize something like that. Low cost. Limited—you know, technology that is already there.

So I just, you know, leave you this thought. I am looking forward to working with you, Admiral, but on the putting the technology we have got to work rather than research programs. Now in the past, let me note that the Admiral has been really great and a visionary about the potential of—if someone comes to him with a plan, what that potential would be. Now we have got to look at it in a different way. Let us put what we have got to work, and we don't—and instead of just looking at this as more investing money, let us just commit ourselves to getting the job done. And to me, that is the only thing that is stopping us from controlling our borders. It is not a lack of technology information, not a lack of research, but a lack of the willpower.

So I am sorry I am—if—you are welcome to shoot that down or agree with it, but I thought I needed to make that statement.

Thank you very much.

Chairman BOEHLERT. Thank you much, Mr. Rohrabacher.

Ms. Johnson.

Ms. JOHNSON. Thank you very much, Mr. Chairman.

This is a very timely hearing for somebody who is from Texas. I guess what I would like to know is how close are you to securing the border. And where are we receiving the most people coming in without permission?

Mr. GIDDENS. Ma'am, we have a long way to go. I am not—we do. It has been something that, for whatever reason, we have not focused on. We are making progress, but we have got a long way to go. We would be happy to take, for the record, to provide you some information about the traffic and where that comes in on the—from my memory, the bulk of that is in the Arizona, Tucson corridor, that we would be happy to take it for the record and get you a breakdown of those numbers.

Ms. JOHNSON. Thank you.

This is one of the major concerns of my constituents, and it seems to me, the entire area where I am from, Dallas. And I really don't know what to do, because once people get here, most of the ones that I see are just looking for a job. And if—you know, if it is some of the others, I don't have—I have not yet had the opportunity to see them. And it seems to me that we ought to have in place something now that could at least separate that whether they have illegal drugs or—you know, that most people—I don't want to say most people, a lot of the people that write me think that most of them have illegal drugs. The people that I see most often do not. They are just looking for a job.

Mr. GIDDENS. That is not—I think you are correct on that. Most of the people that are coming here, I don't think, are intending us harm and they are not bringing contraband with them, but if you

have got 150 people lined up at the border and they are coming across, it is hard to sort those out at the border. As we apprehend people and our Customs and Border Protection are fingerprinting those people so that we are establishing the database so that we can track that and understanding and those that we prosecute, we can work with Justice, if there is criminal activity above the illegal entry. But I think that, by and large, the people that are coming in are seeking to better their lives and the lives of their families, but they are still entering the country illegally.

Ms. JOHNSON. Yes. Thank you, and good luck.

Mr. GIDDENS. Thank you, ma'am.

Chairman BOEHLERT. Ms. Johnson, just let me point out that the magnitude of the problem—and last year, DHS apprehended over one million, one million people attempting to cross the border illegally. That is how many were apprehended.

Ms. JOHNSON. Yes, but Mr. Chairman, two million of them stopped in the Dallas/Fort Worth area.

Chairman BOEHLERT. Do you have any more, Ms. Johnson?

Ms. Biggert.

Ms. BIGGERT. Thank you, Mr. Chairman.

I chair the Subcommittee that has jurisdiction over the National Labs, and how closely have these labs worked with DHS on that—on the border security technology, and how can they be more helpful?

Admiral COHEN. I am going to let Merv Leavitt answer how closely they have worked, and then I would like to come back and explain how very much involved I am with the National Labs and how much I treasure them.

So Merv.

Mr. LEAVITT. Yes, ma'am. We have—Sandia is one of our centers that we use extensively for sensor work, radar, fiber optic sensors, new advanced sensors. We have used the Homeland Security Institute. There is also a BAA out to universities that may partner with some of the labs for a border security Center of Excellence that, you know, we will use in the future.

Admiral COHEN. If I may follow up. At the start of my testimony, I indicated the courage and the wisdom I thought of the enabling legislation, especially in S&T, for the Department of Homeland Security. And as I read those 19 pages over and over as part of the confirmation process and getting my feet on the ground here and putting an organization in place, as we have discussed, it became pretty clear to me, and I have discussed this with staff, and both sides of the aisle have confirmed this to me in both bodies, that the intent, and I think it is a very wise intent, of the Congress and the Administration, was that DHS S&T should not attempt to recreate the National Institutes of Health, should not attempt to recreate the National Science Foundation. Those are full, robust organizations. But in your wisdom, you went ahead and you assigned the DOE labs, which are wonderful in the basic sciences. Incredible intellectual capability there. I have many dealings, of course, with Argonne National Laboratory as the others from my past service in Naval Research, and not only that, but in the legislation, it is just one little line in there that I read as you telling me that I can, without any incremental increase in the cost, leverage all depart-



ments of government: Department of Transportation, Department of Defense, et cetera, where annually we invest tens and tens of billions of dollars in basic, applied, and advanced technology research. That is something that has not been exercised by my Directorate. I plan on exercising that so I use my precious dollars with the universities and the National Laboratories throughout my range of investment to add onto those underlying technologies that the government and the taxpayer have already paid for but focus them then on Homeland Security missions.

Ms. BIGGERT. Well, that is the way I read the law, that we really included the provision giving DHS the access to the expertise, the facilities, and the technologies at DOE's National Labs, and I hope that you will take full advantage of that, because I think they do have the expertise in the sensors and modeling and systems materials, and many other areas that could help improve our border security.

So I thank you.

Admiral COHEN. I might say, my first day in the job was the 10th of August, and that was the—you know, the liquid explosives threat to our airliners. The very next day, I established the Rapid Response Team, led by a program manager in my office who understood energetics, Dr. George Zarur, who is a long-time scientist very familiar with the National Labs, and Susan Hallowell, who is my director of my Transportation Security Lab. And that team, on the 11th of August, we had our first video teleconference with all of the lab directors from all of the DOE labs and our university Centers of Excellence, and together, we went ahead and put together a request for information, which went out within the week, SAFETY Act protection went out with the RFI, and we have gotten over 40 respondents in the month, and we are getting ready to test at both Sacorro, New Mexico and Tyndall Air Force Base against 500-milliliter Gatorade bottles of the actual formula, which I won't share here publicly, based on the technologies that came back from that RFI and those that we have been working on. But some of the stuff that has come out of the national labs, even in this last month, is eye-watering, and I think will be of great value to Kip Hawley in TSA and his screeners.

Ms. BIGGERT. Thank you.

Thank you. I yield back, Mr. Chairman.

Chairman BOEHLERT. Ms. Jackson Lee.

Ms. JACKSON LEE. Thank you, Mr. Chairman, to you and the Ranking Member.

As we speak, Admiral Cohen, there is another Homeland Security Committee going on, so I thank you for your indulgence. I am going to ask, because there are enormous experts, I was just in a hearing where we were missing the permanent Assistant Secretary for Cyber Security, so obviously personnel is a matter that goes, more or less, hand-in-hand with technology. And the reason I say that is because there has to be a vision of the leader to be able to help the Department focus on the right kinds of tools.

I have been down to the border. I have walked along the border in the light and in the dark. And certainly, it is, I think, a reality that our border at the southern border is a porous border. And it is that reason for many reasons. We have interacted with South

and Central America for a very long time of our history. The northern border, similarly situated. But that doesn't give comfort to the American people that although we have had longstanding friendships with our northern and southern neighbors, that we live now in a different climate. And frankly, I think technology is certainly the key. And I am sure that questions have been asked and answered.

But I would raise the question of matching human resource to technology. You are talking about Border Patrol agents, and there are two facets of this. There is the Border Patrol agents that are literally on the dividing lines. There are those who are called Customs and Border Protection that are the ports of entry that have the difficult challenge of being alert for 4,000 cars coming through, whether it is the northern or southern border, and then having the responsibility of what we call secondary search. What are the—there are many individuals here, but where are we with matching human resource training so that we are into—Members of Congress, I have put forward legislation that talks about night goggles and laptops and a number of others. But where are we with infrared? Where are we with the training of the personnel that will then understand the technology? Now I guess I want you to speak a lot about the technology, because this is the Science Committee, so I know that you are not here to talk about personnel. But what more can we get in the hands of individuals who are on the front lines that we already have not asked for? And I would appreciate it if each of the gentlemen would answer the question. Some level of sophisticated technology that we may not be aware of. The night goggles are sophisticated for us, but there are obviously other coordinating factors from what is at the home base and what you can tell to the person on the front line that they should be either seeing or looking for, quick intelligence getting to them.

So I will yield to the first panelist, and I thank you very much for your indulgence.

Mr. LEAVITT. Ms. Jackson Lee, we have a pilot going on in the Douglas station that provides the—Arizona that provides a station. The agents are on the border with PDA capability that—

Ms. JACKSON LEE. Now what kind of capability?

Mr. LEAVITT. A personal digital assistant, handheld capability that lets them query databases to determine if a certain individual has a criminal background. It gives them situational awareness on where they are in relation to their other Border Patrol agents and also sensors. That same capability is provided in their vehicles. So primarily focusing on providing information and situational awareness—

Ms. JACKSON LEE. In real time? And this equipment is in hand right now?

Mr. LEAVITT. Yes.

Ms. JACKSON LEE. Do you need more of it? Do you need more?

Mr. LEAVITT. I—we need to prove that it works and understand what the final configuration needs to be. It is a pilot right now.

Ms. JACKSON LEE. Okay. Let me just move down to the different panelists. Thank you.

Admiral COHEN. I will give you an uncharacteristically short answer. As you know, I am focusing on human factors as one of my

six departments. This is critically important. And the area of hostile intent, what are the characteristics of someone who is coming in with drugs, someone who is a terrorist, a suicide bomber, et cetera. I am not going to go into what those characteristics are or details in the public fora, but I can tell you that we are investing money in that. This needs to be done remotely. It needs to be done holistically. It is part of the system of systems. It goes to the kind of pilot that you are seeing. And as we demonstrate the efficacy of these within the confines of our laws and our traditions, we then will move into the acquisition world, which is Greg Giddens, and I will have de-risked it and he will buy it and deploy it. And the training of our agents is going on right now, not just TSA screeners, but Border Patrol and across the enterprise.

Chairman BOEHLERT. Thank you very much.

The gentlelady's time has expired.

Mr. Sherman.

Mr. SHERMAN. Thank you, Mr. Chairman.

As you may know, I am the Ranking Democrat on the Subcommittee of IR that deals with proliferation. And some have argued that it doesn't—we shouldn't go into absolute conniptions if the wrong people get nuclear weapons, because we will be able to prevent those weapons from reaching our cities. Now one issue is delivery by missile and the whole missile defense and whether that would work and whether you could hit a bullet with a bullet, and that is outside the scope of these hearings. The other possibility is to remark that you may not need to be a rocket scientist to smuggle a nuclear weapon into the United States. And you could do so by air or water or over the border, in the sense of not coming into a legitimate port but rather to areas of our coast, land the plane legally or illegally, or just walk across the border where it is illegal to do so. And—or you could focus on coming through our airports, come—bringing it in a truck over a designated border crossing area or into an airport. And the real question that my constituents would want to know is, is it any harder to bring a nuclear weapon into this country—or much harder to bring a nuclear weapon into this country than, say, a really big bale of marijuana, because a nuclear bomb is about the size, physically, of a really big bale of marijuana, and my constituents are aware that it has happened, that marijuana has come across our border. And you know, there is the size and weight, but obviously drugs and other contraband of that size—the size and weight of a nuclear device has come across, so the question is, really, does the nuclear properties of the bomb or device itself make it highly—much easier to catch than an equal size or weight of illegal drugs? Is there a device available, Admiral, to your department that could detect, say, a nuclear material, whether that be highly-enriched uranium or whether it be plutonium, from, say, half a mile away so that if somebody was bringing in an SUV full of marijuana you might not catch them but you catch the nuclear because, from a mile away, half a mile away, you could sense that there was nuclear material?

Admiral COHEN. Well, Congressman, the short answer is yes, there are technologies. There are multitudes of technologies, many of which are well proven for many years.

Mr. SHERMAN. From a mile away?

Admiral COHEN. There are numerous technologies that have varying ranges and sensitivities. I am not going to discuss in open fora those capabilities. I will—

Mr. SHERMAN. The experts I have talked to have said, “Forget about it.” I mean, you can make—look, now and then, even the experienced marijuana smuggler screws up and gets caught. And even the foreign intelligence agency smuggling a nuclear weapon in this country has a one in ten chance of getting caught, the same way the experienced drug dealers—drug smugglers occasionally get caught. But I am told that if it is shielded in water, shielded with lead, that you are not going to be able to detect this from even 100 feet away.

Admiral COHEN. I really don’t want to cross any line here, but when you are looking for nefarious objects, you may look for other telltale signs. You may look for the shielding instead of the radioactivity. I think in this particular area, Congressman, I would feel much more comfortable asking—

Mr. SHERMAN. Let—if you could come by, and we will arrange to have a briefing—

Admiral COHEN. Yes, sir.

Mr. SHERMAN.—on this—

Admiral COHEN. Yes, sir.

Mr. SHERMAN.—because I—you know, I have told my constituents it is a little harder than bringing in an equivalent weight of marijuana, but not much harder, and in any case, you didn’t need to be a rocket scientist to—

Admiral COHEN. I will ask our defense—excuse me, Domestic Nuclear Defense Office, the DNDO, which has cradle-to-grave responsibility for this in Homeland Security, similar to the naval reactors in the Department of Defense for nuclear propulsion. We will arrange with your staff to have them come by and so someone who is knowledgeable can—

Mr. SHERMAN. I look forward to that, both for gamma detection and neutron detection, both shielded with water, shielded with lead, and not shielded, and both with regard to trying to come in here legally—or not legally, but through a legal crossing—

Admiral COHEN. Yes, sir.

Mr. SHERMAN.—point into our country—

Admiral COHEN. Yes, sir.

Mr. SHERMAN.—or the Canadian or Mexican border at a place at which you are not supposed to cross. I have got a lot of friends who just go skiing across the Canadian border, and nobody has ever questioned them in or out.

And with that—

Admiral COHEN. Yes, sir.

Mr. SHERMAN.—I will yield back.

Chairman BOEHLERT. Thank you very much.

Two quick questions I have, and one—and I think I know what the answer is going to be, but I would like to get a response from Admiral Cohen. Dr. Worch, I will ask you this: as a member of the Air Force Science Advisory Board and fellow Vice Commander of Rome Lab, how can we better leverage the expertise of Defense laboratories, like Rome, to help secure our homeland? And should DHS fund more research at laboratories, like Rome, and it doesn’t

have to be Rome specifically, other laboratories, but our world leaders in things like C4ISR technologies, which are critical for our border security system?

Dr. WORCH. Well, I think it is a matter of setting up a memorandum of agreement with those particular laboratories. Now with—probably with the Air Force between the Air Force and the Department of Homeland Security. The funding, I think—now, again, I can't speak for the Air Force, but there is joint funding. There are technologies that are there in the laboratories that they can make themselves, DHS, aware of directly, and I am sure they are trying to do this, but—

Chairman BOEHLERT. Admiral, are you aware of the Rome Laboratory?

Admiral COHEN. I am aware of the Rome Laboratory, but that is from my prior life.

Chairman BOEHLERT. Yeah.

Admiral COHEN. I am a big believer in competition. I believe in the best offer being rewarded. And as I indicated, this very wonderful authority that you gave had not been previously exercised. I plan on making myself a nuisance to the other departments so that the monies they have invested, we can harvest those technologies and then, either with those laboratories or other providers, go ahead and mature it and focus it for the unique requirements of Homeland Security.

Chairman BOEHLERT. That is another observation that Dr. Worch made. You were somewhat critical the way the SBInet contract is being handled, you know, as one great big contract. How do you guys respond to that one?

Mr. GIDDENS, you are the acquisition man.

Mr. GIDDENS. So it seems, sir.

That was clearly one of the issues that, as we were putting together the strategy, back earlier this year, that we wanted to address, and we believe we have addressed and mitigated that risk and the solicitation and the requests or proposal that we put out, we have had very strong language in that the offers had to provide their subcontracting plan. We have very strong language in there about oversight on their make-or-buy process. So when they decide, as he mentioned, company A is going to bring company A's goods to the table, they have to convince us. They have to present that make-or-buy decision to show us that that is where the value is. And we are ultimately in control. I don't want to make any mistake about who is working for who. The integrator is working for the United States Government and not the other way around, and we will make those calls. And they have to bring that to the table. And we put very clear and explicit language in the solicitation for them to identify how they would work that, how they would address conflicts of interest. I am not going to tell you it is not—we believe we put in the correct contractual language to allow us to mitigate and manage that risk but not avoid it.

Chairman BOEHLERT. Dr. Worch, do you have any response to that?

Dr. WORCH. Well, I certainly hope you have the freedom to have on board technical experts on the government side.

Chairman BOEHLERT. Well, that can help with this. It can't just be program managers. It has got to be people who have an intimate knowledge of those technologies that can be critical and make a decision. I am sure you are doing that. I—you know, you are nodding your head "yes."

Admiral COHEN. Yes, sir. We have to be intelligent—

Chairman BOEHLERT. Nodding your head "yes" means "yes."

Admiral COHEN. I think Dr. Worch has it exactly right, and my people will be at the table and showing alternate or better or different solutions to what the prime integrator may be proposing, and then it will be up to the customer, the acquisition official, to decide what level of risk, cost, or schedule upset that they are willing to take to get the best solution at that time, but that will continue year-in and year-out. And in fact, in the Navy we did this on, basically, a three-year cycle, and that is not an unreasonable cycle for technology insertia.

Chairman BOEHLERT. Thank you. Our goal was to wrap this up at 4:30, but Ms. Jackson Lee wanted another minute, because she wanted some other comment, I think, maybe on her question. And then I will—

Ms. JACKSON LEE. Mr. Giddens—thank you, Mr. Chairman.

Mr. Giddens, you had a comment on my earlier—I hope you remember the question that I asked earlier about human resource and technology. Would you want to just expand?

Mr. GIDDENS. Yes, ma'am. I was, actually, also thinking back to the hearing we had in the spring on the Subcommittee on Management Integration Oversight.

Ms. JACKSON LEE. Yes.

Mr. GIDDENS. And as we said then and the Subcommittee was interested in the lessons we had learned from ISIS and other activities and were we indeed going to pull this off in the SBInet by the end of September, we are still on track to do that. But as we have been in that source selection mode, I have been hesitant to get involved in the technology side, because we need to keep the purity of the source selection process. S&T has been doing that for us, and they have been very gracious at sort of segmenting people that were technical advisors to us and then segmenting people that could still stay in touch with the technology. As we are looking to award SBInet, we will have, then, a better ability to come, and we will be happy to come and brief you or your staff on some of the technology that is involved in that. But I am really not in a position to detail those out today.

But your point about training, we have already engaged with the head of training at CBP and involved them early and started thinking about how can we prepare the men and women who are at the pointy end of doing the king's business on how to use these tools and not just throw those tools at them and expect them to figure it out. And you have made a very key point, and we need to train early and often.

Ms. JACKSON LEE. Do you have a sense of urgency?

Mr. GIDDENS. Yes, ma'am.

Ms. JACKSON LEE. Thank you.

I yield back. Thank you very much.

Chairman BOEHLERT. Thank you very much.

And as is the custom here, we will have some additional questions that we, perhaps, will submit to you individually in writing, and we would appreciate a timely response.

For the closing word, now let the record note that we give the closing word to Mr. Gordon.

Mr. Gordon.

Mr. GORDON. Unless the Chairman doesn't like the word.

First, let me thank all of you for spending two and a half hours with us. These hearings aren't intended to percolate up elegant answers to or, you know, complete answers to these problems, but rather to start our job of oversight, to put some fresh eyes on what goes on here. We have been able to witness a lot of successes, but we have also—we have discussed seeing a lot of the taxpayer money wasted and a lot of important programs bungled. And our great hope is not to say, you know, "We told you so," later, but to, again, put a little extra oversight so you have to work a little harder and know that you can't be, you know, cavalier.

The second point I want to make is that, again, this is, obviously, an important problem, and the solution isn't—is going to be more than just on the border. It is going to take systems existing now and maybe created that will integrate with that, and I am sure you are going to be dealing with that.

And finally, I suspect it will take ten times or more than that or 100 times the dollar figure to go from an 80 or 90 percent penetration to a 100 percent. And it may—you know, and it—you know, the East Germans did a pretty good job, but they didn't stop folks from getting through. And I don't think that our country is going to be harmed too much if, you know, a half a dozen brick—you know, future bricklayers get through. But we are going to be harmed if—as Brad Sherman was talking about, if there are those folks that are coming through with bad intentions. Now I hope that, as you go through this process, that—I am more interested in 100 percent bad guys than I am 100 percent everybody kind of solution. And we really need to put our attention on that. You talked about some of those characteristics. I think, you know, they may take multiple folks and they may take materials and a variety of things, and this is north border as well as south border. So as we go through and we have to make compromises, and as we have to pay the bills, that is my highest priority, and hopefully it would be yours, too.

Chairman BOEHLERT. Thank you very much.

And thank all of you. We really appreciate it.

The hearing is adjourned.

[Whereupon, at 4:34 p.m., the Committee was adjourned.]





Appendix:

---

ANSWERS TO POST-HEARING QUESTIONS

## ANSWERS TO POST-HEARING QUESTIONS

*Responses by Admiral Jay M. Cohen, Under Secretary for Science and Technology, U.S. Department of Homeland Security; Accompanied by Mr. Gregory L. Giddens, Director, Secure Border Initiative Program Executive Office, U.S. Department of Homeland Security*

**Questions submitted by Chairman Sherwood L. Boehlert**

*Q1. Dr. Worch testified that there continue to be issues with the safe operation of unmanned aerial vehicles (UAVs) in commercial airspace. Specifically, he emphasized the need to develop reliable anti-collision technologies and the fact that the National Aeronautics and Space Administration has ended much of its work in this area.*

*Q1a. Do you agree that this is an issue? If not, why not? If so, what UAV-related air safety research does DHS Science and Technology Directorate intend to sponsor or perform?*

A1a. The S&T Directorate agrees that one of the most pressing needs for allowing unmanned aircraft to operate safely in commercial airspace is the development of reliable anti-collision technologies. To that end, the S&T Directorate is working cooperatively with the Federal Aviation Administration (FAA) and with the Department of Defense's (DOD's) Unmanned Aircraft Systems Airspace Integration Joint Integrated Product Team (JIPT) to define requirements for automated collision avoidance systems that would be suitable for use in unmanned aircraft. In FY 2007, the S&T Directorate is taking a significant step by funding the Massachusetts Institute of Technology's Lincoln Laboratory to begin developing a simulation capable of modeling the broad spectrum of air traffic that Unmanned Aerial Vehicles (UAV's) will encounter and must avoid. This will be a first-of-its-kind simulation, more complex and capable than those used over a decade ago for the development of the Traffic Alert/Collision Avoidance System (TCAS). When completed in FY 2008, the simulation will be used to validate requirements, test various automated sensing and avoidance schemes, and help the FAA certify the most effective one(s) for adoption and use in UAVs. The S&T Directorate is also actively participating in two committees that are engaged in developing standards for collision avoidance systems. These standards will form the foundation for FAA policy and regulatory action. Finally, as a full member of the JIPT and its Collision Avoidance Sub IPT, the S&T Directorate is systematically evaluating ongoing DOD collision avoidance efforts as potential solutions to the U.S. Customs and Border Protection's and Coast Guard's UAV needs in this area.

*Q1b. Since the SBInet announcement was made and it appears that UAVs are not integral to Boeing's short-term plans, will this change your plans for supporting UAV-related research?*

A1b. Boeing has reviewed Customs and Border Protection (CBP) Air and Marine's Strategic Plan and CBP's plans for UAV's and, in particular, for use of Predator-B UAV's. The CBP A&M plans are integral in the Boeing solution and will: (a) provide coverage in ground-based sensor gaps; (b) provide immediate response to classify and identify problematic targets; and (c) extend tactical tracking capability to improve apprehension. In addition, Boeing also proposed a small, portable launch UAV (Skylark) with limited range (and low altitude) to provide agent-based reconnaissance and point-to-point search for response and apprehension teams in the field.

*Q2. How do you plan to improve the interagency coordination of research, development, testing, and evaluation relevant to homeland security?*

A2. As part of the alignment of the S&T Directorate, an Agency and International Liaison Office was established. In accordance with the *Homeland Security Act of 2002*, this division will help the S&T Directorate fulfill its responsibility for "coordinating with other appropriate executive agencies in developing and carrying out the science and technology agenda of the Department to reduce duplication and identify unmet needs." The Agency and International Liaison Office will have responsibility for building relationships and improving coordination with executive agencies and our international partners to leverage homeland security research, development, testing and evaluation (RDT&E) efforts across the government. A small cadre of talented professionals will serve as the "ambassadors" to executive agencies—expanding the S&T Directorate's breadth and depth of work with other federal agencies' laboratories and the laboratories of our international partners.

Q3. *At the hearing, the non-governmental witnesses described the key priorities for border security research and development as work on information integration, common operational languages, algorithm development, and airspace safety. They also stressed the importance of improving the communication of needs and testing and evaluation feedback to the private sector and training the next generation of scientist and engineers in critical areas by supporting long-term research.*

*Please describe the DHS S&T priorities for research on border security technology and how they align with the areas recommended by the other witnesses. How were your priorities determined?*

A3. The S&T Directorate's priorities for research on border security technology align well with the priorities described by the other witnesses. They include developing:

- Improved technology for detection, classification and interdiction of illegal activity, identification of individuals with hostile intentions, and enhancing the ability to make rapid strategic and tactical response decisions;
- Technologies that enhance the Common Operating Picture (COP) of the border environment for tactical and operational planning with other federal, State and local law enforcement partners;
- Tools to provide homeland security personnel simultaneous and uniform access to information—both at and between ports of entry—to ensure that an agent's geographic location does not limit his or her access to actionable intelligence;
- Rapid response capabilities to effectively respond to cross-border violations. These include pursuit-termination technology and command, control, and communications technologies that improve situational awareness and provide decision aids for commanders;
- Technologies that aid in the deterrence and channeling of illegal cross-border activity;
- Technologies that improve voice and data connectivity in remote field areas; and
- Airborne detection and surveillance technologies.

These S&T Directorate border technology priorities are based upon the requirements of our DHS component customers. Priorities are established through an Integrated Product Team (IPT) approach among the S&T Directorate's border security customers that include U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), United States Coast Guard (USCG), and others.

Q4. *What role will DHS S&T Directorate play in determining what technologies are to be deployed along the borders as part of SBInet? What role will it play in evaluating whether those technologies are effective?*

A4. The S&T Directorate identifies (through a requirements-based process), develops, tests and facilitates the transition of advanced homeland security technical capabilities to SBI and SBInet. Specifically, the S&T Directorate supports SBInet through: (a) technical risk reduction by exploration of alternative technologies, (b) technology insertion into acquisition programs significantly enhance performance or reduce costs, and (c) pursue specific high risk / high payoff innovations. The S&T Directorate will mature technologies through a proof-of-concept testing, and then, if proved, SBInet will incorporate them into the SBInet integrated technical solution. Because we expect our nation's adversaries to adapt to SBInet systems, the S&T Directorate's continuous infusion of new technology is absolutely essential to providing a sustainable long-term capability.

#### **Questions submitted by Representative Jo Bonner**

Q1. *In looking at the successful use of UAVs in the Middle East and the Global War on Terrorism how effectively would UAVs serve the United States along our southern border in what some may consider a non-combat zone?*

A1. The CBP Air & Marine UAV plans are integral to the SBInet solution to: (a) provide coverage in ground based sensor gaps, (b) provide immediate response to classify and identify problematic targets, and (c) extend tactical tracking capability to improve apprehension. In addition, SBInet is proposing a small, portable launch UAV (Skylark) with limited range (and low altitude) to provide agent-based recon-

naissance and point to point search for response and apprehension teams in the field.

*Q2. Under Secretary Cohen, in your opinion, what are some of the most affordable, effective and available technologies that we should consider for border/coastal security?*

A2. The S&T Directorate is developing border security technologies and will transition to its customers both affordable and effective capabilities that improve the security of our nation's borders. Its goal is to develop and integrate information management, officer safety and sensor technologies necessary to prevent the entry of terrorists, weapons of mass destruction (WMD), criminals, and illegal aliens through our nation's borders. We will address a range of technologies such as advanced surveillance systems (including automated scene understanding, advanced ground and maritime radars, and advanced ground sensors), pursuit termination technology, and remote determination of intent capability for checkpoints. These technologies will be integrated into the Secure Border Initiative (SBI) program as capabilities mature.

#### **Questions submitted by Representative Judy Biggert**

*Q1. Who in the world do you feel we can learn from in terms of their border security? Which countries use their technology most effectively? How is our technology similar? What can we learn from countries like Israel and even Mexico and Canada on their border security?*

A1. There are a handful of countries that use a variety of technological solutions, such as innovative electro-optical systems for surveillance and tracking, optical fiber technology for security, video communication and control systems alongside image-processing and smart systems for electronic fences, etc. The technological components proposed by Boeing for the SBInet first Task Order, which is a twenty-eight mile section of the Tucson sector, is primarily the same technology that is deployed along the Israeli border.

*Q2. A recent Governmental Accountability Office report on the Visa Waiver Program highlights several recommendations for increased security at ports of entry against individuals using lost and stolen passports. Among the weaknesses highlighted in the report are the following: (1) DHS has not established adequate operating procedures for countries to report stolen or lost travel documents and (2) DHS has not given U.S. border inspectors automatic access to the International Criminal Police Organization (Interpol) lost and stolen travel document databases at primary inspection points.*

*What technology is needed at ports of entry to correct this deficiency? What is the cost of this technology? How has DHS addressed these weaknesses? Is there a timeline for updating the technology available to border inspectors at primary inspection points?*

A2. The Secretary of Homeland Security has made screening of the Interpol Stolen and Lost Travel Documents Database a goal for inbound air passengers. The inclusion of Interpol Data on Lost and Stolen Passports, (the Stolen and Lost Travel Documents Database or SLTD) is less reliant upon a technological solution than an agreement between Interpol and DHS to implement within agreed-upon parameters. Customs and Border Protection completed a pilot in July 2006 to assess the technical and operational issues. The expense for connectivity has been estimated at two million dollars for implementation and \$500,000 as a yearly recurring cost. Access at airport primary inspection points is expected to be introduced in 2007 with eventual implementation to all primary inspection points.

*Q3. How sophisticated is the technology of those smuggling people, weapons, and drugs into our country?*

A3. Smugglers, regardless of the item they are attempting to move, are creative and resourceful. They are adept at creating concealed compartments inside of otherwise normal appearing vehicles, shipping containers, and cargo items. They use computers and commonly available software to create or alter travel documents. They take advantage of difficult terrain and remote areas of our borders to surreptitiously enter the United States. They understand trade procedures and attempt to mask illicit activity under the guise of legitimate import of goods. CBP and ICE rely on a layered approach to border security that emphasizes effective personnel, infrastructure, technology, and resources to counter smuggling threats and ensure that

regardless of the tactics used the adversary is successfully detected and responded to as appropriate.

**Questions submitted by Representative Michael T. McCaul**

*Q1. I would like to discuss the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program for a moment. Despite what many folks believe, the US-VISIT program has not been fully implemented. The Exit portion of US-VISIT is only operation as a pilot program in nine airports and two sea-ports. As you know the exit procedures of the program are critical component to the overall effectiveness of US-VISIT. As visitors leave the country, US-VISIT Exit scans their travel documents and captures their biometrics, matching the visitors' identity, verifies departure, and confirms compliance with U.S. immigration policy.*

*The U.S. allows in approximately 200 million temporary visitors a year, with virtually no way to keep visitors from staying beyond their authorized visit. DHS estimates that at least 30 percent of the approximately 10 million illegal immigrants living in the U.S. are probably visa absconders or over-stayers. The Government Accountability Office says that figure is more likely 40 percent.*

*With such a national problem facing our country I am unable to understand why DHS has not fully rolled-out an exiting Departmental program, especially one involving bio-metrics that can help track visa overstays. Can you explain this?*

A1. Response US-VISIT is reviewing how to improve biometric exit at air and sea ports of entry and how to improve compliance. US-VISIT will continue to use the Advanced Passenger Information System (APIS) to track departures.

*Q2. I understand that fiscal year 2006 (FY06) expenditure plan for US-VISIT was never submitted to Congress—contained in that spending plans was additional FY06 monies to roll-out the Exit side of US-VISIT. The Senate, in their version of the FY07 DHS Appropriations Bill is also concerned regarding the current state of the Exit portion of US-VISIT. In fact, they directed DHS to submit a strategic plan for US-VISIT 30 days after enactment of the bill.*

*Given the importance of this program, does the Department of Homeland Security plan to submit to Congress a FY06 expenditure plan that includes a further roll-out of the Exit portion of US-VISIT?*

A2. The US-VISIT FY2006 expenditure plan was delivered to Congress on August 14 and US-VISIT is now awaiting a response. The plan includes continuing current exit pilots.

*Q3. What is DHS's vision for SBInet? Mr. Giddens, what is your and DHS's strategic plan for SBInet? What did you communicate to private industry with regard to DHS's needs for this program?*

A3. The challenges that this nation faces in having both open and secure borders is multi-faceted and complex. It encompasses not only the facilitation of legitimate trade and travel, but more importantly, the protection of our homeland from cross-border and transnational threats to our security, public safety and economy. With the mandates to have both open and secure borders also comes the recognition that attention must be paid to the processes that begin away from our borders, occur at the border, and continue to all regions of the United States. The Department's Secure Border Initiative (SBI) will create a new border security culture within the Department, integrating and unifying border security systems, and developing and coordinating programs and policies to secure the border and efficiently enforce U.S. immigration and customs laws.

SBInet is a critical component of the Department's strategic strategy in securing the Nation's borders. SBInet, when fully implemented, will enable DHS to detect, identify, classify, respond and bring to a law enforcement resolution cross-border threats. SBInet will meet the varied requirements of the U.S. border environment—southern, northern and maritime. It will integrate capabilities by utilizing a systems- and risk-based approach. SBInet will also develop and deploy a Common Operating Picture providing commonality to DHS components as well as inter-operability with external stakeholders. What has been communicated to private industry from the onset by the highest levels of the Department is that the proposed solution must be a dynamic, creative systems approach that will ensure the optimum mix of personnel.

*Q4. Mr. Giddens, your testimony seemed to be very short on specifics. Could you describe the different, specific needs of the border and how specifically technology will address these requirements?*

A4. The U.S. border can be best viewed as three basic tactical environments—urban, rural and remote. Different environments require different deployment tactics and this ultimately affects what specific technology will be used.

In an urban environment, the criminal has the tactical advantage because an illegal entrant can be across the border and into the community infrastructure in a matter of minutes, sometimes seconds. If accessible to entry, urban areas require an inordinate number of enforcement personnel to effectively confront the illegal activity. The goal of technology used for border security in an urban environment is to create a perception of such impenetrability that potential illegal entrants and smugglers are deterred from attempting an entry, thereby reducing an excessive investment in personnel resources.

In a rural area, the time it takes for an illegal entrant to mix into the community infrastructure is greater, thereby giving enforcement personnel the tactical advantage of time to respond, and the enforcement response may be measured. The technology used in the rural area will be able to detect the entry in time to respond, resolve, and bring the situation to an appropriate law enforcement resolution.

In remote environments, the time from entry to infrastructure is greater still and may occur in hours or even days. In many remote areas, it may take two to three days to reach the nearest road. In such situations, CBP makes every effort to apprehend illegal entrants at a location as close to the point of entry as practical. Messaging targeted toward deterrence is an essential component to attaining border safety in a remote environment.

The technology that will be used in all of the environments along the border will vary depending on the location, terrain, climate, topography, etc. CBP will utilize assorted tested and proven technologies that may include ground surveillance radars combined with unattended ground sensors and sensor assets attached to aerial vehicles. These technologies will complement other components and infrastructures to ensure the proper mix of systems are deployed along the border.

**Question submitted by Representative Lincoln Davis**

*Q1. Since its inception, DHS has benefited from a strong working relationship with the Department of Energy national labs, which have helped DHS identify, develop, and examine cutting edge homeland and border security technologies. How will the proposed reorganization of DHS S&T Directorate affect the way DHS works with the labs?*

A1. The S&T Directorate recognizes the value of the national laboratories and will continue to utilize the expertise of the national laboratories. The S&T Directorate plans to leverage prior investments in the R&D capability of the national laboratories by the Department of Energy, the Department of Defense and many other agencies and to continue this farsighted tradition through focused investments for the future. The recent alignment of the S&T Directorate includes establishing a Director of Research position reporting to the Under Secretary, who will oversee the Office of National Laboratories, which has responsibility for coordination and utilization of the national laboratories to support the homeland security mission. This includes both harvesting current national laboratory science and technology and supporting investments that are needed to develop and maintain critical homeland security capabilities for the future. Both of these missions are essential.

## ANSWERS TO POST-HEARING QUESTIONS

*Responses by Peter R. Worch, Independent Consultant, Member of the U.S. Air Force Science Advisory Board*

**Question submitted by Representative Jo Bonner**

*Q1. I wish we could match good ideas with funding—but we have to search out great ideas, establish the cost of the projects, and have them implemented. As we go through this process, a lot has been said about Unmanned Aerial Vehicles (UAVs) along the border. Some reports suggest the use of UAVs in one of the most costly means of monitoring border security—please explain some of the uphill battles of this costly project.*

*A1.* The purchase and operation of unmanned aerial vehicles for border surveillance (or any other application) is costly. I don't know the exact numbers because the cost analyses I have seen have tended to use flawed assumptions.

In the border security tasks, the initial "trip-wire" detections would best be accomplished by buried (or covert) unattended ground sensors. A somewhat larger area may be covered by the pole mounted sensors (terrain, foliage, and urban structures permitting). Clearly, ground or pole-mounted sensors are low in cost. But both are inflexible—they can only cover that designated area around their location. In forested areas, for example, these sensors would have to be very closely spaced (100's of feet). Moreover, for the pole-mounted sensors, a determined intruder would certainly figure out a way to avoid detection by the pole-mounted sensors because he/she can easily see the areas such a sensor could see or not see. Various cover, concealment, and camouflage means (as well as careful timing) could avoid detection.

The value of the UAV is that it can

- rapidly deploy to a newly-identified area of suspected or real penetrations
- provide persistent surveillance at that site, and
- provide relentless tracking of the intruder, no matter where he/she chose to travel. (The use of Predator in Iraq has time and again demonstrated this strength.)

In my mind, the UAVs would not patrol the entire border, but would be selectively used in situations in which fixed (including aerostat-carried) sensors simply could not provide the service. Thus, a limited number would be procured and strategically based to do tasks that other sensor concepts could not do, and to augment other elements of border security.

Thus, I see it as a matter of cost-effectiveness, not just cost.

As for the "uphill battles," I see three issues to be addressed in establishing an effective UAV surveillance force:

- **Human-System Integration (HSI)**—situational awareness, controls and displays, health management, and emergency procedures all require improved HSI to be safe and effective in intercepting intruders
- **Detect, See and Avoid techniques** that are highly automated, vision-based systems are needed for UAV operations (and would benefit civil and military aircraft) in civil airspace
- **Careful, but limited, basing and an appropriate concept of operations** to provide for reasonable flyout times, supportability, and system cost effectiveness.

These issues are not insurmountable, nor are the solutions in themselves costly. Joint efforts with the military to address the first two issues would be appropriate.