AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

COORDINATED INFORMATION SHARING AND HOMELAND SECURITY TECHNOLOGY

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY AND PROCUREMENT POLICY

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

JUNE 7, 2002

Serial No. 107–182

Printed for the use of the Committee on Government Reform

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

U.S. GOVERNMENT PRINTING OFFICE

85–840 PDF WASHINGTON : 2003

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

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
BOB BARR, Georgia
DAN MILLER, Florida
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
DAVE WELDON, Florida
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
C.L. "BUTCH" OTTER, Idaho
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
JOHN SULLIVAN, Oklahoma

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
JANICE D. SCHAKOWSKY, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts

BERNARD SANDERS, Vermont (Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
JAMES C. WILSON, *Chief Counsel*
ROBERT A. BRIGGS, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON TECHNOLOGY AND PROCUREMENT POLICY

THOMAS M. DAVIS, Virginia, *Chairman*

JO ANN DAVIS, Virginia
STEPHEN HORN, California
DOUG OSE, California
EDWARD L. SCHROCK, Virginia

JIM TURNER, Texas
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii

EX OFFICIO

DAN BURTON, Indiana

HENRY A. WAXMAN, California

MELISSA WOJCIAK, *Staff Director*
VICTORIA PROCTOR, *Professional Staff Member*
TEDDY KIDD, *Clerk*
MARK STEPHENSON, *Minority Professional Staff Member*

CONTENTS

	Page
Hearing held on June 7, 2002	1
Statement of:	
Harman, Hon. Jane, a Representative in Congress from the State of California	85
Sugar, Ronald D., Ph.D., president and chief operating officer, Northrop Grumman Corp.; Leonard Pomata, president, Federal Group, webMethods, Inc.; S. Daniel Johnson, executive vice president, public services, KPMG Consulting, Inc.; and Kevin J. Fitzgerald, senior vice president, government, education & healthcare, Oracle Corp.	100
Yim, Randall, Managing Director, National Preparedness Team, General Accounting Office; Mark Forman, Associate Director, Information Technology and E-Government, Office of Management and Budget; Robert J. Jordan, Director, Information Sharing Task Force, Federal Bureau of Investigation; George H. Bohlinger III, Executive Associate Commissioner for Management, Immigration and Naturalization Service; and William F. Raub, Ph.D., Deputy Director, Office of Public Health Preparedness, Department of Health and Human Services	11
Letters, statements, etc., submitted for the record by:	
Bohlinger, George H., III, Executive Associate Commissioner for Management, Immigration and Naturalization Service, prepared statement of	51
Davis, Hon. Thomas M., a Representative in Congress from the State of Virginia:	
Briefing memo	135
Prepared statement of	4
Fitzgerald, Kevin J., senior vice president, government, education & healthcare, Oracle Corp., prepared statement of	109
Forman, Mark, Associate Director, Information Technology and E-Government, Office of Management and Budget, prepared statement of	41
Harman, Hon. Jane, a Representative in Congress from the State of California, prepared statement of	88
Horn, Hon. Stephen, a Representative in Congress from the State of California, prepared statement of	8
Johnson, S. Daniel, executive vice president, public services, KPMG Consulting, Inc., prepared statement of	115
Jordan, Robert J., Director, Information Sharing Task Force, Federal Bureau of Investigation, prepared statement of	75
Pomata, Leonard, president, Federal Group, webMethods, Inc., prepared statement of	124
Raub, William F., Ph.D., Deputy Director, Office of Public Health Preparedness, Department of Health and Human Services, prepared statement of	61
Sugar, Ronald D., Ph.D., president and chief operating officer, Northrop Grumman Corp., prepared statement of	103
Yim, Randall, Managing Director, National Preparedness Team, General Accounting Office, prepared statement of	14

COORDINATED INFORMATION SHARING AND HOMELAND SECURITY TECHNOLOGY

FRIDAY, JUNE 7, 2002

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TECHNOLOGY AND PROCUREMENT POLICY,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2154, Rayburn House Office Building, Hon. Thomas M. Davis (chairman of the subcommittee) presiding.

Present: Representatives Tom Davis of Virginia, Jo Ann Davis of Virginia, Horn and Turner.

Also present: Representative Harman.

Staff present: Melissa Wojciak, staff director; George Rogers, Uyen Dinh, and John Brosnan, counsels; Victoria Proctor, professional staff member; Teddy Kidd, clerk; Todd Greenwood and Nick Vaughan, interns; Mark Stephenson, minority professional staff member; and Jean Gosa, minority assistant clerk.

Mr. TOM DAVIS OF VIRGINIA. We have Members moving to take their seats. We're going to start with Members' statements.

Good morning. I want to welcome everybody to today's oversight hearing. After September 11th, there's been a sea change in the mission of government. The first priority of the Nation has become homeland security. To win this fight, the government must be able to detect and respond to terrorist activity. We also must be ready to manage the crisis and consequences of future attacks, to treat casualties, and to protect the functioning of critical infrastructures. Thus, defending America in the new war against terrorism will require every level of government to work together with citizens and the private sector.

More than ever our success is dependent upon collecting, analyzing and appropriately sharing information that exists in data bases, transactions and other data points. Effective use of accurate information from divergent sources is critical to our success in this fight. Indeed as the President said last night in his speech to the Nation, "Information must be fully shared so we can follow every lead to find the one that may prevent a tragedy."

The President spoke with vision about our Nation's titanic struggle against terrorism and the triumph of freedom over fear. I applaud his leadership in asking the Congress to create a Department of Homeland Security. I'll be working with our colleagues to enact legislation to meet his call. I believe the proposed Department of Homeland Security will greatly assist information sharing

by reorganizing the government along the more rational strategic lines that will more efficiently pursue homeland security. The new Department will be a customer of the FBI and the CIA and will be able to analyze, diffuse and disseminate information to Federal, State and local agencies, the private sector and citizens.

However, integration of the information systems and practices of the agencies to be consolidated into the new Department will be a prime concern, as will the new information-sharing relationships that will evolve between the Department of Homeland Security, the FBI, the CIA and other agencies.

I'm also heartened to see that the plan for the new Department of Homeland Security includes flexible acquisition policies to encourage innovation and rapid development of critical technologies. This concept is at the core of H.R. 3832, the Services Acquisition Reform Act that I recently introduced. I look forward to discussions with the administration to further redefine the legislation and move forward the new Department.

Today's hearing continues the subcommittee's oversight of the barriers to robust information sharing, both within and between agencies. In February of this year, we reviewed some of the management initiatives and technology acquisitions needed to ensure that stovepipes of knowledge and a lack of coordination between agencies would not compromise homeland security. While new funding for procurement of products and services is certainly needed if the government is going to effectively modernize, share information and win the war against terrorism, we should also continually measure the results of the government's efforts. When it comes to the war on terrorism, Americans are not asking for more spending; they are asking for more spending that works.

Unfortunately, as witnessed in the February hearing revealed, there has not been an organized, cohesive and comprehensive process within the government to evaluate private sector solutions to the problems of information sharing and homeland security. Many technology firms with expertise to address homeland security matters have indicated that they are having a hard time getting a real audience for their products.

Addressing the acquisition challenges to achieve homeland security must be a priority so that we can begin to leverage America's competitive advantage in IT innovation for the benefit of all Americans. After the February hearing we introduced legislation to facilitate private sector innovation by establishing an interagency team of subject matter experts to issue major announcements seeking unique and innovative anti-terror solutions. These experts would also screen and evaluate innovative proposals for industry and send them to the proper Federal agencies for action. This legislation would also launch a program offering monetary awards to companies with the best and most cutting-edge terror-fighting solutions. In addition, it would establish an acquisition pilot program to encourage agency professionals to creatively use streamlined authorities and waivers to buy commercial, off-the-shelf solutions with immediate impact on homeland security.

In this hearing I look forward to hearing from the agencies and leading companies represented for their insights into how programmatic changes, management initiatives and technology acquisitions can contribute to the better sharing of information and the achievement of the homeland security mission.

[The prepared statement of Hon. Thomas M. Davis follows:]

DAN BURTON, INDIANA
CHAIRMAN

BENJAMIN A. GILMAN, NEW YORK
CONSTANCE A. MORELLA, MARYLAND
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
STEPHEN HORN, CALIFORNIA
JOHN L. MICA, FLORIDA
THOMAS M. DAVIS, VIRGINIA
MARK E. SOUDER, INDIANA
STEVEN C. LATOURETTE, OHIO
BOB BARR, GEORGIA
DAN MILLER, FLORIDA
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
DAVE WELDON, FLORIDA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
C.L. "BUTCH" OTTER, IDAHO
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE
JOHN SULLIVAN, OKLAHOMA

ONE HUNDRED SEVENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051
TTY (202) 225–6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
PATSY T. MINK, HAWAII
CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
ROD R. BLAGOJEVICH, ILLINOIS
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, MAINE
JANICE D. SCHAKOWSKY, ILLINOIS
WM. LACY CLAY, III, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS

BERNARD SANDERS, VERMONT,
INDEPENDENT

SUBCOMMITTEE ON TECHNOLOGY AND PROCUREMENT POLICY

OVERSIGHT HEARING

"Meeting the Homeland Security Mission: Assessing Barriers to and Technology Solutions for Robust Information Sharing"

OPENING STATEMENT

June 7, 2002 at 10 a.m.

Room 2154 Rayburn House Office Building

Good Morning, I would like to welcome everyone to today's oversight hearing.

After 9/11/01, there has been a sea change in the mission of government. The first priority of the nation has become homeland security. To win this fight, the government must be able to detect, prevent, and respond to terrorist activity. We also must be ready to manage the crises and consequences of future attacks, to treat casualties and to protect the functioning of critical infrastructures.

Thus, defending America in the new war against terrorism will require every level of government to work together with citizens and the private sector. More than ever before, our success is dependant upon collecting, analyzing, and appropriately sharing information that exists in databases, transactions, and other data points. Effective use of accurate information from divergent sources is critical to our success in this fight.

Indeed, as the President said last night in his speech to the Nation, "Information must be fully shared, so we can follow every lead to find the one that may prevent tragedy." The President spoke with vision about our Nation's titanic struggle against terrorism and the triumph of freedom over fear. I applaud his leadership in asking Congress to create a Department of Homeland Security, and I will be working with my colleagues to enact legislation that meets his call.

I believe the proposed Department of Homeland Security will greatly assist information sharing by reorganizing the government along more rational, strategic lines

that will more efficiently pursue homeland security. The new department will be a customer of the FBI and CIA and will be able to analyze, fuse, and disseminate information to federal, state, and local agencies, the private sector, and citizens. However, integration of the information systems and practices of the agencies to be consolidated into the new Department will be of prime concern, as will the new information sharing relationships that will evolve between the Department of Homeland Security, the FBI, the CIA, and other agencies. I also am heartened to see that the plan for the new Department of Homeland Security includes flexible acquisition policies to encourage innovation and rapid development of critical technologies. This concept is at the core of H.R. 3832, The Services Acquisition Reform Act I recently introduced. I look forward to discussions with the Administration to further refine the legislation and move forward the new Department.

Today's hearing continues the Subcommittee's oversight of the barriers to robust information sharing both within and between agencies. In February of this year, we reviewed some of the management initiatives and technology acquisitions needed to ensure that stovepipes of knowledge and a lack of coordination between agencies would not compromise homeland security. While new funding for procurement of products and services is certainly needed if the government is going to effectively modernize, share information, and win the war against terrorism. We also should continually measure the results of government's efforts. When it comes to the war on terrorism, Americans are not asking for more spending; they are asking for more spending that works.

Unfortunately, as witnesses at the February hearing revealed, there has not been an organized, cohesive, and comprehensive process within the government to evaluate private sector solutions to the problems of information sharing and homeland security. Many technology firms with expertise to address homeland security matters have indicated that they are having a hard time gaining a real audience for their products. Addressing the acquisition challenges to achieving homeland security must be a priority so that we can begin to leverage America's competitive advantage in IT innovation for the benefit of all Americans.

Thus, after the February hearing, I introduced legislation to facilitate private sector innovation by establishing an interagency team of subject matter experts to issue agency announcements seeking unique and innovative anti-terror solutions. These experts would also screen and evaluate innovative proposals from industry and send them to the proper federal agencies for action. This legislation would also launch a program offering monetary awards to companies with the best, most cutting-edge terror-fighting solutions. In addition, it would establish an acquisition pilot program to encourage agency professionals to creatively use streamlined authorities and waivers to buy commercial, off-the-shelf solutions with immediate impact on homeland security.

In this hearing, I look forward to hearing from the agencies and leading companies represented for their insights into how programmatic changes, management initiatives, and technology acquisitions can contribute to the better sharing of information and the achievement of the homeland security mission.

Mr. TOM DAVIS OF VIRGINIA. I now yield to my ranking member, Mr. Turner from Texas, for his opening statement.

Mr. TURNER. Thank you, Mr. Chairman. I appreciate the good timing of the hearing that you called this morning, and I join with you in commending the President on his initiative to create a new Cabinet-level position for homeland security. As you know, there has been legislation pending in the Congress which I have supported to accomplish that, and I think that the President's initiative will be well received, and I look forward to the work that our committee will have the opportunity to do in refining that proposal.

We all know that the attacks of September 11th have created the greatest challenge our Nation has faced in its history, and the sophistication and fanaticism of al Qaeda and similar organizations no doubt represent a challenge that all of us must work together to address.

I appreciate all of our government agency witnesses here today, as well as the private sector witnesses who have come. One of the common complaints that I've heard from the private sector business folks during the last few months is that they go to the Office of Homeland Security, and they present their ideas and offer up various proposals, and yet they never hear anything, and obviously part of that problem exists because of the lack of authority in the Office of Homeland Security. The President's reorganization effort will, I think, resolve that, and we will be on our way toward utilizing the best that the private sector has to offer in the war on terrorism.

I think the American people have been quite tolerant and forgiving of the intelligence failures that led to the tragic events of September 11th, but I have no doubt that we will be all held accountable in the event of another similar event. And so it is up to us to put our shoulder to the wheel, both in the government sector, as well as to bring in the best assistance we can find from the business community to be vigilant, prepared and to address the threats that we face.

Responding to the challenge requires, I think, new thinking, thinking out of the box, new methods, new technologies. All of this can be provided if we build a good, strong working relationship with the powerful forces of the private sector in this country, and I look forward to working with the chairman to accomplish that. And, again, I thank our witnesses for being here today.

Thank you, Mr. Chairman.

Mr. TOM DAVIS OF VIRGINIA. Thank you, Mr. Turner.

Mrs. Davis, any statement?

Mr. Horn.

The gentleman from California is recognized.

Mr. HORN. Thank you, Mr. Chairman.

This is a very important hearing. My Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations has been holding a series of field hearings on how effectively the Federal Government is helping State and local agencies prepare for another terrorist attack. We started in Nashville, and we've done a few more: Phoenix, Albuquerque, Los Angeles, San Francisco. Witnesses from local agencies in each of these cities have said that intelligence sharing and their ability to commu-

nicate with other local and Federal agencies are among the very leading concerns. These are the men and women who will be on the front lines should another attack occur.

We must do everything possible to ensure that they're equipped with the best information possible so that they can effectively and efficiently protect and serve the American people, and I would like to, Mr. Chairman, put in the record a letter that Mr. Shays and myself sent to Mr. Sensenbrenner, the chairman of the Committee on the Judiciary, with the bill we put in, H.R. 3483, the Intergovernmental Law Enforcement Information Sharing Act of 2001. Mr. Burton is very supportive of this, and Mr. Shays and myself, Ms. Schakowsky, Mrs. Maloney, so forth, and if I might put that in and——

Mr. TOM DAVIS OF VIRGINIA. Without objection, it will be put in the record.

[The prepared statement of Hon. Stephen Horn follows:]

DAN BURTON, INDIANA,
CHAIRMAN

BENJAMIN A. GILMAN, NEW YORK
CONSTANCE A. MORELLA, MARYLAND
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
STEPHEN HORN, CALIFORNIA
JOHN L. MICA, FLORIDA
THOMAS M. DAVIS, VIRGINIA
MARK E. SOUDER, INDIANA
JOE SCARBOROUGH, FLORIDA
STEVEN C. LaTOURETTE, OHIO
BOB BARR, GEORGIA
DAN MILLER, FLORIDA
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
DAVE WELDON, FLORIDA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
C.L. "BUTCH" OTTER, IDAHO
EDWARD L. SCHROCK, VIRGINIA

ONE HUNDRED SEVENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225-5074
FACSIMILE (202) 225-3974
MINORITY (202) 225-5051
TTY (202) 225-6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
PATSY T. MINK, HAWAII
CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
ROD R. BLAGOJEVICH, ILLINOIS
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, MAINE
JANICE D. SCHAKOWSKY, ILLINOIS
WM. LACY CLAY, MISSOURI

BERNARD SANDERS, VERMONT,
INDEPENDENT

Opening Statement
Stephen Horn, Chairman
Subcommittee on Government Efficiency,
Financial Management and Intergovernmental Relations

Thank you Mr. Chairman.

I am especially interested in today's hearing. My Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations has been holding a series of field hearings on how effectively the Federal Government is helping State and local agencies prepare for another terrorist attack.

Thus far, we have visited Nashville, Tennessee; Phoenix, Arizona; Albuquerque, New Mexico; and Los Angeles and San Francisco, California.

Witnesses from local agencies in each of these cities have said that intelligence sharing and their ability to communicate with other local and Federal agencies are among their leading concerns.

These are the men and women who will be on the frontlines should another attack occur. We must do everything possible to ensure that they are equipped with the best information possible so they can effectively and efficiently protect and serve the American people.

DAN BURTON, INDIANA,
CHAIRMAN

BENJAMIN A. GILMAN, NEW YORK
CONSTANCE A. MORELLA, MARYLAND
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
STEPHEN HORN, CALIFORNIA
JOHN L. MICA, FLORIDA
THOMAS M. DAVIS, VIRGINIA
MARK E. SOUDER, INDIANA
STEVEN C. LATOURETTE, OHIO
BOB BARR, GEORGIA
DAN MILLER, FLORIDA
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
DAVE WELDON, FLORIDA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
C.L. "BUTCH" OTTER, IDAHO
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE

ONE HUNDRED SEVENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051
TTY (202) 225–6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
PATSY T. MINK, HAWAII
CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
ROD R. BLAGOJEVICH, ILLINOIS
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, MAINE
JANICE D. SCHAKOWSKY, ILLINOIS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS

BERNARD SANDERS, VERMONT,
INDEPENDENT

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS,
AND INTERNATIONAL RELATIONS
Christopher Shays, Connecticut
Chairman
Room B-372 Rayburn Building
Washington, D.C. 20515
Tel: 202 225-2548
Fax: 202 225-2382
E-mail: hr.nsc@mail.house.gov

March 18, 2002

The Honorable F. James Sensenbrenner, Jr.
Chairman, Committee on the Judiciary
Rayburn House Office Building, Room 2138
Washington, D.C. 20515-6216

Re:
H.R. 3483 ***The Intergovernmental Law Enforcement Information Sharing Act Of 2001***

Dear Chairman Sensenbrenner:

We respectfully request the Committee on the Judiciary conduct a hearing on HR 3483, *The Intergovernmental Law Enforcement Information Sharing Act Of 2001* at your earliest convenience.

The Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations and the Subcommittee on National Security, Veteran Affairs, and International Relations held a joint hearing last year regarding information sharing between federal, state and local officials.

The Subcommittees found there is a growing concern on the part of state and local officials across the nation who believe they are not getting access to the full range of intelligence they need to carry out their public safety duties.

State and local officials must be able to receive information regarding potential threats within their jurisdictions in a timely manner, and unnecessary barriers to information sharing among federal, state and local officials should be identified and eliminated.

The Subcommittees learned the chances of identifying potential terrorist targets and reducing the possibility of another terrorist attack would improve if certain state and local officials were given security clearances. Expanding the issuance of security clearances would be an important means of improving information sharing among federal, state and local officials and agencies.

HR 3483, *The Intergovernmental Law Enforcement Information Sharing Act Of 2001,* requires the Attorney General to ensure that all information available to the Department of Justice concerning terrorist activities and potential threats is shared with appropriate officials of state and local governments who have a need for that information, and to provide appropriate security clearances under the standards set forth in applicable statutes and executive orders.

We ask that HR 3483 be raised for a public hearing. Thank you for your consideration.

Sincerely,

Stephen Horn

Stephen Horn, Chairman
Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations

Christopher Shays

Christopher Shays, Chairman
Subcommittee on National Security, Veterans Affairs, and International Relations

Mr. HORN. Because whatever you'd like to put on language, we don't have a big ego about this, we just want to get the job done.

Mr. TOM DAVIS OF VIRGINIA. Well, thank you very much, Mr. Horn.

The subcommittee is now going to hear testimony from our first panel. We have Mr. Randall Yim, the Managing Director of the National Preparedness Team at GAO; Mr. Mark Forman, a frequent contributor to this subcommittee's work, the Associate Director of Information Technology and E-government at OMB; George Bohlinger, the Executive Associate Commissioner for Management at INS; Dr. William Raub, the Deputy Director, Office of Public Health Preparedness at HHS; and Mr. Robert Jordan, the Director of the Information Sharing Task Force at the FBI. I appreciate everyone being here.

It's the policy of this subcommittee that all witnesses be sworn, so if you would stand with me and raise your right hands.

[Witnesses sworn.]

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

Mr. Yim, why don't we start with you and move straight down the line. Your total testimony is going to be—is a part of the record, so it's in the record. What I'd like you to do is try to use 5 minutes to hit your key points. There's a light in front of you. When it turns orange, you have a minute to try to hit your 5 minutes and try to keep it moving along. Most of the Members have read the total testimony, so our questions are kind of ready, but we'd like you to hold it to 5 minutes.

Mr. Yim, thank you for being with us.

STATEMENTS OF RANDALL YIM, MANAGING DIRECTOR, NATIONAL PREPAREDNESS TEAM, GENERAL ACCOUNTING OFFICE; MARK FORMAN, ASSOCIATE DIRECTOR, INFORMATION TECHNOLOGY AND E-GOVERNMENT, OFFICE OF MANAGEMENT AND BUDGET; ROBERT J. JORDAN, DIRECTOR, INFORMATION SHARING TASK FORCE, FEDERAL BUREAU OF INVESTIGATION; GEORGE H. BOHLINGER III, EXECUTIVE ASSOCIATE COMMISSIONER FOR MANAGEMENT, IMMIGRATION AND NATURALIZATION SERVICE; AND WILLIAM F. RAUB, Ph.D., DEPUTY DIRECTOR, OFFICE OF PUBLIC HEALTH PREPAREDNESS, DEPARTMENT OF HEALTH AND HUMAN SERVICES

Mr. YIM. Thank you very much, Mr. Chairman and members of this committee. Thank you for inviting me to share information with you about the critical need for information sharing, and integration of new and existing technologies, and to an effective strategy for homeland security.

Although there are many players in this complex arena of homeland security, we all share the same goal, to make our great Nation more secure against terrorists and to prevent tragedies such as September 11th from ever occurring again. This will be a formidable task, since it will be very difficult to stop an enemy that is fluid, less structured and deliberately tries to blend into the background with our Federal, State and local governmental institutions that are more highly structured and less agile, making it all the more important that our governments adopt the innovative and

creative tools of government that are flexible and have adaptable characteristics.

We could never be 100 percent secure or 100 percent prepared, but we can be better prepared. Everyone cannot do everything, and everyone cannot and should not do the same things. Instead we must augment, foster, develop and maintain what particular governments do best, what the private sector and local communities do best and integrate these efforts through our national strategy.

To fashion such a strategy, we'll need to identify those key enablers to the creation and implementation of the strategy. Clearly better information sharing and IT architectures are one of the most critical enablers, and expanding and adapting our sizable advantages in technology and research and development, using our positive asymmetries effectively against the asymmetric threats posed by terrorists will be a key enabler. We must overcome roadblocks that have been identified, such as protection of proprietary and sensitive information, including information that may adversely affect business value and financing, legal barriers such as antitrust and liability concerns, jurisdictional and turf issues such as those being highlighted in the current exploration of stovepiping in intelligence and law enforcement communities, and format and architecture mismatches to prevent sharing and interconnectivety even when people want to share.

And we will need to identify an investment strategy that maximizes the use of our finite human and fiscal capital resources so our strategy is both affordable and sustainable, and we need to begin now since our threats are now. This means we cannot, unfortunately, wait to and only design new architectures from scratch, but we must assess what we currently have; assess what others have done and what they are doing when facing problems that share characteristics with our fight against terrorism; determine how we can adapt and refine existing or analogous mechanisms; and also consider good old-fashioned low-tech and common-sense solutions and solutions that rely on the smarts of our citizens and government leaders. And finally, we have to acknowledge that any national strategy lacking measurable objectives, measurable performance indicators and accountability mechanisms will not be sustainable.

There is no doubt that there is more than one way to accomplish these goals. The GAO has focused upon the factors relevant to the decisionmaking process and some of the emerging and best practices that may be adaptable to the homeland security mission. It is important not only to do things right, but also to do the right things. This means we have to get the right information to the right people at the right times, and we also have to do the right things with that information. So we will need an integrating strategy that makes sense of the information that separates the relevant few from the general noise, that helps us to find the relevant needles in the haystack that spur us to take further action to prevent, interdict and respond to terrorists; and we have to do this in ways that are already familiar to State and local and private sector first responders so that we don't start from scratch, and consider adaptive use of programs that are already integrated into State and local and private sector response mechanisms, that com-

plement rather than become additional burdens, because we all know that we are asking these people to undertake significant homeland security tasks in addition to their other duties and responsibilities, all with finite human and fiscal resources.

Some good examples of effective use of information in new technologies exist, and more are beginning to emerge. We've illustrated some of these for you in the one-page handout that we've distributed for you today. For example, computer intrusion detection systems constantly try to monitor deviations from, "normal background," to detect potential threats.

The same know-how can be applied to airline data bases, energy supply and infrastructure monitoring systems, cargo container tracking or manifest systems, all to try to detect anomalies from a, "background that may be an indicator to spur further action."

Increasing use of digitized information, the power of digitization, integrating satellite-derived digital imagery with digitized maps of critical infrastructure and computer modeling to provide gaming simulations to guide preparedness or predict attacks or identify vulnerabilities. These models could even help us determine what types of data needs to be collected now, not only once, but consistently over time, to develop trends that would help us establish a background, and models could also be used to perhaps assign responsibilities to different jurisdictions or Federal agencies for detection and prevention.

We will need not only, thus, to rely on new technologies, such as advancements in biometrics and devices to detect biological and radioactive agents in hidden locations, such as within cargo containers, but also adaptive use of existing technologies as well as common-sense and low-tech approaches. Above all, we will need to foster and augment and stimulate creative tools of government, combinations of high and low tech in ways we might not have imagined. Who would have thought that one of our most effective weapons in Afghanistan would have been 21st-century airplanes and smart weaponry guided to their targets by the cavalry on horseback?

Mr. Chairman, this concludes my statement, and GAO is pleased to assist in whatever way we can.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

[The prepared statement of Mr. Yim follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology and Procurement Policy, Committee on Government Reform, House of Representatives

For Release on Delivery
10:00 a.m., EDT, Friday
June 7, 2002

NATIONAL PREPAREDNESS

Integrating New and Existing Technology and Information Sharing Into an Effective Homeland Security Strategy

Statement of Randall A. Yim
Managing Director, National Preparedness

GAO-02-811T

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to participate in today's hearing on homeland security. In the wake of the terrorism attacks of September 11, the Office of Homeland Security is preparing a strategy to address these threats to our nation. In addition, federal, state, and local governments, and the private sector, are taking steps to strengthen the safety and security of the American people, including actions to strengthen border and port security, airport security, and health and food security, and protect critical infrastructure. You asked that I discuss what challenges exist in facilitating these security initiatives--particularly in terms of technology and information sharing—and how addressing these challenges fits in with developing and implementing a national preparedness strategy.

In brief, there are specific data, information sharing, and technology challenges facing the country in developing and implementing a national preparedness strategy. Primarily:

- The nature of the terrorist threat makes it difficult to identify and differentiate information that can provide early indication of a terrorist threat from the mass of data available to those in positions of authority responsible for homeland security.
- We face considerable barriers—cultural, legal, and technical--in effectively collecting and sharing information.
- Many technologies key to addressing threats are not yet available, and many existing technologies have not been effectively adapted for the threats the country now faces.

The real challenge, however, is not just to find the right solutions to each of these problems but to weave solutions together in an integrated and intelligent fashion so that they are collectively more than the sum of their parts. At the national level, this will require developing a blueprint, or architectural construct, that defines both the homeland security mission and the information, technologies, and approaches necessary to perform the mission in a way that is divorced from organizational parochialism and cultural differences. Local, state, and federal agencies responsible for homeland security will need to carry out their respective roles under this construct, with a great deal of assistance from the private sector. Fortunately, there are starting

points for addressing each challenge and actions are being taken to strengthen security in a broad range of areas. But there will still be a need for mechanisms to make sure that things happen as they should.

In preparing for this testimony, we relied on prior GAO reports and testimonies on national preparedness, critical infrastructure protection, enterprise architectures, intellectual property, and information technology. We reviewed and analyzed studies on homeland security and a variety of proposals for developing a comprehensive strategy. We also analyzed government and industry reports on the use of remote sensing technologies, media reports of information sharing difficulties, governmentwide guidance on the development of architectures, as well as statements from the Office of Homeland Security on actions taken to address homeland specific challenges. In addition, we recently discussed specific barriers to sharing information on vulnerabilities and attacks with industry officials.

THE THREAT THE COUNTRY IS FACING AND HOW IT NEEDS TO BE POSITIONED TO RESPOND

Our country cannot be 100 percent secure from terrorist attack, particularly when these threats are asymmetric to our strengths, and where terrorists intend to sustain their efforts for as long as need be but view success in terms of single, isolated events causing loss of life or disruption of normal daily routines. What makes it particularly difficult to gauge and respond to this kind of threat?

- Terrorist groups are typically loosely structured, fluid and flexible units, operating in the background seeking targets of opportunity – what futurist Edith Weiner terms "hiborgs" or hybrid organizations. By contrast, our government is highly structured, less able to change rapidly.
- Terrorists groups take advantage of targets becoming complacent, or simply being unable to recognize threats that "blend" into the background of normal life. Countering this complacency and sustaining a high alert status on our part is very difficult.
- The primary job of the terrorist is to find the soft spots, or vulnerabilities, such as lax airport

security, unprotected borders, or weak controls over critical computer assets – and to attack these targets in asymmetric ways. Our job—to limit the soft spots--is much more difficult and costly. As the aftermath of the September 11 attacks has shown, providing adequate security to airports alone is a massive challenge--requiring the hiring thousands of security personnel, acquiring advanced security technology, placing undercover law enforcement officials on flights, developing new passenger boarding procedures, training pilots and flight crew on hijacking scenarios, limiting access points, deploying national guardsmen, and instituting second screening procedures. While significant steps have been taken to improve passenger security, there are concerns remaining, such as the safety of charter airlines.

- Moreover, our government agencies are still required to perform missions or provide essential public services that extend their responsibilities well beyond countering terrorists – with finite fiscal and human capital resources.

It is extremely difficult to defend against a suicide bomber or other asymmetric threats. Yet we are not helpless. Asymmetry can also be made to work to our advantage particularly if we recognize that government institutions are highly structured and less fluid, and deliberately take advantage of innovative and readily adaptable tools that enable us to better to counter terrorists and employ our positive asymmetrical advantages against such groups. Moreover, this country has tremendous resources at its disposal, leading edge technologies, a superior research and development base, and extensive expertise and experience of human capital resources. However, there are substantial challenges to leveraging these tools, including getting the right information at the right times and sharing it and getting the right technologies, and developing a construct that makes sure not only the right information goes to the right people, but that we can prevent, detect, and respond to attacks in a concerted, effective manner.

DATA CHALLENGES

What Needs To Be Done?

- Develop an understanding of the homeland security mission and who does what, for what reason, and how/where/when they do it. Based on that knowledge, decide on the types of data to be collected and reported as well as on the level of detail.
- Collect needed information from a broad range of entities—from federal, state, and local agencies, the private sector, and the research and development community – not just once, but consistently over time so that trends may be established.
- Determine the right format and standards for collecting data so that disparate agencies can aggregate and integrate data and communicate those standards to reporting entities.
- Prioritize data, boil it down to the pieces that can be used to build baselines of normal activity and mechanisms that can effectively detect deviations or anomalies that would indicate vulnerabilities or threats and how serious they may be.

Getting the right information needed for effective and sustainable homeland security will be a daunting challenge, considering the myriad of possible targets, types of attack, and variables that need to be considered in any one aspect of homeland security. Nevertheless it is important to begin deciding what needs to be collected, how it should be collected and what form it should take so that we can begin to collect data that we will need over time to detect terrorist activity before an actual attack.

The first challenge in doing this is to develop an understanding of the homeland security mission, goals, and objectives, and the key activities and players involved.[1] This includes learning specifically: (1) who does what for what reason, (2) how, where, when they do it, (3) what do they use to do it, and (4) in what form. It also includes developing a risk and threat analyses. Building this knowledge will be considerably difficult considering the number of individuals and organizations involved in national preparedness, and the asymmetrical nature of the threat, but it is essential to identify gaps in data, technology, and approaches.

[1] We plan to issue a report on the need to define the homeland security mission within the next month.

Other data-related challenges include:

- ***Deciding what types of data need to be collected for certain activities as well as the level of detail.*** This can be extremely complex for any one aspect of national preparedness. Take transportation mobility, for example, which is critical in the event of a chemical, biological, or nuclear attack. Road network information, when combined with digital elevation models and terrain analysis would help analysts identify transportation or other infrastructure open to threats and to plan mitigating strategies. The same information would also help to identify alternate routing to evacuate or avoid affected areas. Census data and current weather patterns (winds, temperature, and humidity) would allow emergency management officials to determine which areas are most at risk and plan appropriate evacuation routes under multiple scenarios. Finally, any large-scale evacuation will stress emergency facilities and other transportation network elements. As immediate post-attack work done at the World Trade Center illustrates, real-time aerial data can also assist clean-up and recovery efforts.[2]

- ***Balancing varying interests and expectations.*** For example, as we have testified in the past,[3] when it comes to protecting cyberspace, the private sector may want specific threat or vulnerability information so that immediate actions can be taken to avert an intrusion. Law enforcement agencies may want specific information on perpetrators and particular aspects of the attack, as well as the intent of the attack and the consequences of or damages due to the attack. At the same time, many computer security professionals may want the technical details that enable a user to compromise a computer system in order to determine how to detect such actions.

- ***Deciding how much is enough.*** It is important to recognize that it is not possible to build an overall, comprehensive picture of activity on a national scale or even certain confines of activity. For example, it would not be possible to develop a complete picture of the nation's

[2] Ray A. Williamson. "Information as Security: Remote Sensing, Transportation Lifelines and Homeland Security." *Space Imaging.* May/June 2002.

[3] *Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination.* GAO/T-AIMD-00-268. Washington, D.C.: July 26, 2000.

information infrastructure. Networks themselves are too big, they are growing too quickly, and they are continually being reconfigured and reengineered.

- ***Determining the right format and standards for collecting data so that disparate agencies can aggregate and integrate data sets.*** For example, Extensible Markup Language (XML) standards could be considered as one option to exchange information among disparate systems.[4] Further, guidelines and procedures need to be specified to establish effective data collection processes, and mechanisms need to be put in place to make sure that this happens—again, a difficult task given the large number of government, private, and nonprofit organizations that will be involved in data collection. Finally, mechanisms will be needed to disseminate data, making sure that it gets into the hands of the right people at the right time.

More importantly, to make sure the homeland strategy is sustainable, we eventually need to boil data down to the pieces that will allow us to build baselines of normal activity and mechanisms that will enable us to effectively detect deviations or anomalies that would indicate vulnerabilities or threats and how serious they may be. This is already done on a much smaller scale for such things as self-diagnostic systems in automobiles, aircraft, and even electric appliances that alert the owner or manufacturer after sensing slight temperature changes or other small deviations that could indicate a mechanical problem even before it occurs. Moreover, it is done for protecting computer networks.[5] But it promises to be an extremely complicated endeavor for homeland security. For starters, determining what is normal and abnormal activity relative to terrorists would be difficult because it would require developing an extensive body of knowledge—beyond just intelligence information--to build a baseline for terrorist activity when

[4] XML is a flexible, nonproprietary set of standards for annotating or "tagging" information so that it can be transmitted over a network and readily interpreted by disparate systems. For more information on its potential use for electronic government initiatives, see U.S. General Accounting Office. *Electronic Government: Challenges to Effective Adoption of the Extensible Markup Language.* GAO-02-327. Washington, D.C.: April 2002.

[5] Intrusion detection systems used to protect computer networks are built based on data on normal use of system and network activity as well as known attack patterns. Deviations are discovered based on data from analyses of network packets, captured from network backbones or local area network segments, or data sources generated by the operating system or application software.

the activity itself is elusive, fluid, and difficult to predict.

Fortunately, there are good places to start data gathering and modeling. Organizations known as Information Sharing and Analysis Centers (ISACs) are already collecting information on critical aspects of our infrastructure; government agencies at all levels have databases that may be adapted and become useful for such activities as tracking potential terrorists or detecting biological attacks; and extensive information is already being collected through the use of satellites and remote sensing technology that should be useful in building models to detect, analyze, and respond to threats.

Starting Points

- Information Sharing and Analysis Centers (ISAC) are being established to develop information on the nation's critical infrastructure, specifically information to identify vulnerabilities and prevent and respond to attacks. These include the National Coordinating Center for Telecommunications and the Financial Services Information Sharing and Analysis Center. In September 2001, we reported that six ISACs within five infrastructures had been established and that at least three more were being formed.
- Federal agencies, such as the FBI, INS, Customs, Health and Human Services, already have databases containing information critical to homeland security. State and local government also have databases that if adapted will be useful, such as those belonging to highway and transportation departments, county health departments, and school systems.
- Models and statistical techniques have already been developed by the military to analyze threats and provide "gaming" simulation of multiple threat scenarios. In addition, agencies are already collecting information that could feed into these models such as census and weather data, aerial mapping of cities and farmlands, and detailed images of shipping and transportation routes, and maps detailing critical infrastructure and their capacities, such as telecommunications and utility lines.

INFORMATION SHARING CHALLENGES

What Needs To Be Done?

- Establish effective information sharing between private sector, nonprofit, and government organizations to facilitate research and development efforts, data collection efforts, law enforcement efforts, and efforts to respond to attacks.
- Ensure security measures exist to protect sensitive information.

Events preceding and following the attacks of September 11 spotlighted one of our most serious vulnerabilities. We do not share information effectively, particularly when it comes to intelligence, law enforcement, and response activities. If we cannot do a better job of sharing information, we will not be able to effectively identify vulnerabilities, develop needed technology, and coordinate efforts to detect and respond to attacks.

Federal agencies and the Congress are still looking into the specifics of information sharing difficulties related to the September 11 attacks, but recent reports of information sharing failures within the FBI and CIA highlight some of the primary barriers we face: stovepiped organizational structures, inadequate database sharing, and simple "turf" issues. Legal and regulatory impediments may have made information sharing even more difficult.

This problem is not new. Two years ago, for example, we testified that the ILOVEYOU computer virus, which affected governments, corporations, media outlets, and other institutions worldwide, highlighted the need for greater information sharing and coordination to respond to attacks on our critical infrastructure. Because information sharing mechanisms were not able to provide timely enough warnings against the impending attack, many entities were caught off guard and forced to take their networks off-line for hours. Getting the word out within some federal agencies themselves also proved difficult. At the Department of Defense, for example, the lack of teleconferencing capability slowed the response effort because Defense components had to be called individually. The National Aeronautics and Space Administration had difficulty communicating warnings when e-mail services disappeared. Some departments that received warnings did not share that information with their bureaus.

As illustrated below, however, the problem of information sharing is much more extensive than just sharing information about an impending attack—it extends from the early stages of research and development, to collecting data, to preventing and detecting attacks, and responding to attacks. Barriers themselves extend well beyond poor mechanisms for issuing attack warnings, or communicating calls for "heightened alert." For example, in recent discussions with us,

industry officials said that their chief concern in sharing information about vulnerabilities and attacks is disclosure of proprietary data. Our past reviews have also highlighted concerns about roles and responsibilities, antitrust violations, and national security as barriers to sharing information.

In short, there are formidable challenges that need to be overcome to build a more comprehensive and effective information-sharing relationships.[6] Trust needs to be established among a broad range of stakeholders, important questions on the mechanics of information sharing and coordination need to be resolved, and roles and responsibilities need to be clarified among all levels of government.

Figure 1: Highlights of Information Sharing Barriers

Where information sharing can potentially break down	Why
Government efforts to sponsor research and development efforts to develop new homeland security technologies	• Intellectual property concerns may affect the willingness to contract with the government, including poor definitions of what technical data is needed by the government and unwillingness on the part of government officials to exercise the flexibilities available to them concerning intellectual property rights.
	• Concerns that inadvertent release of confidential business material, such as attempted or successful attacks, gaps in security, or trade secrets or proprietary information, could damage reputations, lower consumer confidence, hurt competitiveness, and decrease market shares of firms.
Government efforts to facilitate data sharing on critical infrastructures	• Concerns about potential antitrust violations may keep companies from sharing information with other industry partners.
	• Concerns that sharing information with the government could subject data to Freedom of Information Act disclosures or expose companies to potential liability may also prevent companies from sharing data with government agencies.

[6] More information about barriers to information sharing can be found in: *Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination.* GAO/T-AIMD-00-268. Washington, D.C.: July 26, 2000 and *Intellectual Property: Industry and Agency Concerns Over Intellectual Property Rights.* GAO-02-723T. Washington, D.C.: May 10, 2002.

Private sector efforts to get data from the government on potential vulnerabilities and threats.	• National security concerns may prevent agencies from sharing data with the private sector. • The process of declassifying and sanitizing data takes time—possibly too long to be of use to private sector time critical operations. • Security clearances may not be available for the "right people" who need to know.
Coordinating law enforcement and intelligence activities.	• Law enforcement and intelligence agencies operate in "distinct universes" separated by jurisdictional, organizational, and cultural boundaries. At the same time, however, roles and responsibilities at different levels of government are not always clear and distinct. • Information may be considered too sensitive to release to law enforcement colleagues because it could compromise source and collection techniques. • Certain laws and regulations as well as privacy concerns may prevent information sharing between federal agencies, state, and local law enforcement agencies. • Insufficient direction about what specific steps should be taken when security alert status is increased • Lack of access to databases and problems with interconnectivity may impede information sharing among agencies.
Issuing attack warnings and responding to attacks.	• Information sharing mechanisms and procedures for warning against attacks, especially between different levels of government, may be inadequate. • Roles and responsibilities between emergency, rescue, relief, and recovery organizations may not always be clear, especially at different levels of government.

Because information sharing was a critical problem in other crises facing the government, there are some very good models to learn from and build on. The ISACs mentioned earlier are a good example of government and private sector relationships for information sharing. The Centers for Disease Control and Prevention (CDC) also uses several information-sharing computer systems to help accomplish its mission to monitor health, detect and investigate health problems and conduct research to enhance the prevention of disease.[7] In addition, actions have already

[7] GAO reported in September 2001 that the usefulness of several of these systems is impaired both by CDC's untimely release of data and by gaps in the data collected.

been taken by the Congress and the administration to strengthen information sharing. The USA Patriot Act, for example, enhances or promotes information sharing among federal agencies and numerous terrorism task forces have been established to coordinate the investigations and improve communications among federal and local law enforcement. Also, very recently, leading financial services firms in New York formed a private database company that will compile information about criminals, terrorist, and other suspicious people, for use in screening new customers and weeding out those who may pose a risk. The company will specifically focus on helping financial companies comply with anti-money-laundering regulations, including requirements in legislative approved after the September 11 attacks. Additional private sector solutions also need to be considered such as current research efforts to link airline reservation systems.

Starting Points

- The Agora is a Seattle-based regional network of over 600 professionals representing various fields, including information systems security, law enforcement, local, state, and federal governments; engineering; information technology; academics; and other specialties. Members work to establish confidential ways for organizations to share sensitive information about common problems and best practices for dealing with security threats. They develop and share knowledge about how to protect electronic infrastructures and they prompt more research specific to electronic information systems security.
- Carnegie Mellon University's CERT Coordination Center (CERT/CC) is charged with establishing a capability to quickly and effectively coordinate communication among experts in order to limit damage, respond to incidents, build awareness of security issues across the Internet community. In this role, CERT/CC receives from and provides to system and network administrators, technology managers, and policymakers Internet security-related information and it provides guidance and coordination to major security events.

TECHNOLOGY CHALLENGES

What Needs To Be Done?

- Research and develop new technologies integral to the fight against terrorism, such as bioweapon or low level radioactive weapons detection systems and biometric devices.
- Refine emerging technologies so that they are more user friendly and less cost prohibitive.
- Adapt existing technologies to the homeland security mission.
- Connect and make interoperable databases integral to information sharing, such as those belonging to the FBI and the INS.

This is one area where we certainly have an edge over terrorists. Newly developed unmanned aerial vehicles are providing intelligence vital to military efforts in Afghanistan. Satellite networks and remote sensing technologies are facilitating assessments of threats overseas as well as military operations and guidance systems for weapon systems. However, though we have vast technological resources available on the homefront, there are substantial challenges confronting us. In particular:

- Certain technologies important to homeland security have not been developed. These include bioweapons and low level radioactive weapons detection systems and disease surveillance systems.

- Some technologies already in existence have not been effectively adapted to homeland security. Space-based satellites and sensors, for example, are being used to guide weapon systems, map cities, and study the weather and environment. But they also may be adapted to the homeland security mission. Moreover, some experts believe that making this transition may require modifications to current technology, such as the addition of video features so that we can observe ground activity as it is changing.[8]

[8] Joseph A. Engelbrecht Jr., *Global Security Will Drive Real-Time Surveillance,* Space Imaging, May/June 2002.

- There is a lack of connectivity and interoperability between databases and technologies important to the homeland security effort. Databases belonging to federal law enforcement agencies and the INS, for example, are not connected, and databases between state, local, and federal governments are not always connected. In fact, we have reported for years on federal information systems that are duplicative and not well integrated.[9] A related problem is that there are not common standards for data exchange and application programming interfaces for technologies that provide physical security. As a result, much of the equipment needed to protect buildings is not interoperable. We recently testified,[10] for example that deploying an access control system that uses a smart card containing a fingerprint biometric would require at least three pieces of equipment: the card reader device, the fingerprint scan device, and the hardware device used to house and operate the biometric software. If these devices are made by different manufacturers, they cannot function as an integrated environment without costly additional software to connect the disparate components.

- Some existing technologies important to homeland security are not user-friendly. We recently testified[11] that some biometric technologies are inconvenient to use. Retina scanning, for example, feels physically intrusive to some users because it requires close proximity with the retinal reading device. Moreover, fingerprinting feels socially intrusive to some users because of its association with the processing of criminals. There is also an assortment of health concerns among a segment of the population regarding certain security technologies. For instance, there is evidence that pacemakers and hearing aids can be adversely affected by some detection technologies.

- The capabilities of security technologies can be overestimated, potentially luring security officials into a false sense of security and relaxed vigilance. During our recent review of

---

[9] U.S. General Accounting Office. *Information Technology: Enterprise Architecture Use across the Federal Government Can Be Improved.* GAO-02-6. Washington, D.C.: February 2002.

[10] U.S. General Accounting Office. *National Preparedness: Technologies to Secure Federal Buildings.* GAO-02-687T. Washington, D.C.: April 25, 2002.

[11] U.S. General Accounting Office. *National Preparedness: Technologies to Secure Federal Buildings.* GAO-02-687T. Washington, D.C.: April 25, 2002.

federal building security technologies, we found instances in which the performance of biometric technologies were overestimated.[12]

Because of our nation's substantial investment in technology and research and development, there are numerous good starting points for developing and harnessing technology needed for the homeland security mission. Significant advances, for example, have already been made in technologies needed to protect building, airports, and other facilities. We also have a good technological foundation, including space-based satellites, imagery and remote sensing systems, to begin developing systems for effectively monitoring and gauging terrorist activities.

Additionally, the administration is promoting a host of new initiatives to acquire the technologies needed for homeland security. For example, projects already underway include:

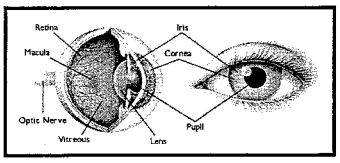
- Taking stock of what technologies are already available and what gaps exist.
- Assessing what changes are needed to federal databases to facilitate information sharing.
- Efforts to develop protocols to permit the access of databases and information owned by federal agencies as well as state and local authorities.
- Developing an optimized entry-exit system for border security.
- Assessing biometric technology options.

[12] U.S. General Accounting Office. *National Preparedness: Technologies to Secure Federal Buildings.* GAO-02-687T. Washington, D.C.: April 25, 2002.

Starting Points

Continue to develop and refine emerging technology

- Some of the emerging biometric devices, such as iris scans and facial recognition systems, theoretically represent a very effective security approach because biometric characteristics are distinct to each individual and, unlike identification cards and pin numbers or passwords, they cannot be easily lost, stolen, or guessed. Until recently, in addition to being very expensive, the performance of most biometric technologies had unreliable accuracy. However, prices have significantly decreased and, after years of research, the technology has recently improved considerably.



Iris scan technology is based on the unique visible characteristics of the eye's iris, the colored ring that surrounds the pupil. A high-resolution digital image of the iris is taken to collect data. The system then defines the boundaries of the iris, establishes a coordinate system over the iris, and defines the zones for analysis within the coordinate system. The visible characteristics within the zone are then converted into a 512-byte template.

Adapt potentially useful existing technology

- Combining geospatial digital information tools, including remote sensing and satellite imagery technology, can assist efforts to model threat prevention and response scenarios and build baselines of normal activities and detect deviations from the norm. The same information can also be used to respond to a successful attack and assist in crime scene investigation. This technology is already being used to plan and execute military operations and analyze threats overseas, as well as to map cities, study the environment and weather, monitor transportation and shipping routes, monitor compliance with laws, regulations and treaties, and model differing scenarios to assist in planning and prevention.

Satellite photo with geospatial digitized overlay.

Make good use of low tech alternatives

- New ionization radiation technologies that the United States Postal Service (USPS) is implementing may be a promising way to sanitize mail contaminated by anthrax, but there are proven low tech solutions that should still be considered, such as manual mail handling procedures to pre-sort non-anonymous mail to reduce the volume that would require higher tech irradiation techniques.

- New high tech explosive detection systems can be used to detect bulk or trace explosives concealed in, on, or under vehicles, containers, packages, and persons. However, dogs are also an effective and time-proven tool for detecting concealed explosives. The dogs currently used by DOD, for example, can detect nine different types of explosive materials. And since dogs have the advantage of being mobile and able to follow a scent to its source, they have the significant advantage over mechanical explosive detection systems in any application that involves a search.

Security dogs may be more cost effective and easier to deploy than new high tech explosive detection systems

MECHANISMS NEEDED TO EFFECTIVELY RESPOND TO CHALLENGES

What Needs To Be Done?

- Apply risk management principles to identify assets that need to be protected to maintain continuity of operations, as well as threats, vulnerabilities, risks, priorities and countermeasures.
- Use this understanding to develop a blueprint, or architectural construct, that defines the information, technologies, and approaches necessary to perform the homeland mission.
- Assign responsibilities among the stakeholders so that everyone is not doing the same thing, but instead all are doing something slightly different that together forms a more effective shield.
- Establish analytical and warning capabilities.
- Create performance goals and metrics, and feedback and accountability mechanisms, so that efficacy of investments and efforts may be measured and programs continually improved.

The overriding challenge for homeland security, of course, is how to prevent, detect, and respond to attacks. Technology and information are critical enablers, but they are not the sole answer. There are significant issues involving people and approaches that also need to be dealt with. For example, people—the majority of whom will never witness a terrorist event--will be required to be able to sense relevant minute changes from normal activity that could alert them to the possibility of a threat. They will also be required to work together to implement policies, processes, and procedures that serve as countermeasures to identified risks. To do so effectively, they will need information about what additional concrete things they must do when new threat information becomes available. In addition, because there are thousands of individuals and organizations involved in detecting, preventing, and responding to attacks and numerous projects being initiated, measures need to be taken to prevent redundancy and inefficiency in homeland security efforts.

To be truly effective, however, the homeland security strategy needs to go beyond promoting redundancy and efficiency to finding innovative approaches to homeland security activities—ones that fully optimize skills, capabilities, and available resources. The asymmetrical threat we face demands that act in accordance with the Marines' operation motto: "Improvise, Adapt, Overcome." In fact, expeditionary forces within the military provide a good example of how we can find new approaches by capitalizing on technology, skills and capabilities, and flexibility. These are forces that are designed, trained, and organized in a very different fashion than conventional forces, which previously relied on highly structured and standardized approaches to warfighting and require considerable infrastructure in their deployments. In the Navy and the Marine Corps, for instance, expeditionary forces have the ability to go rapidly and easily to places where there is no infrastructure to operate on their arrival because they carry their infrastructure on their back and in the holds of ships. The forces are trained to be self-reliant, self-sustaining, highly adaptable, and adept in the most austere environments. Because they are uniquely positioned and organized to accomplish a wide range of missions, including long-range strike operations and early forcible entry to facilitate or enable the arrival of follow-on forces, they have been used in a wide range of missions for decades.

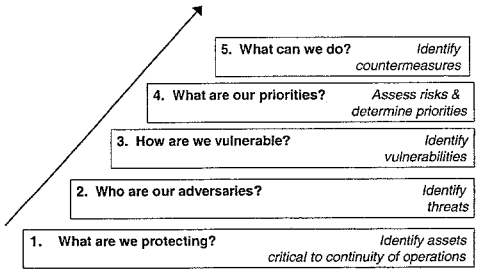
Starting Points

There are some very good starting points for addressing all of these challenges as well as the need to integrate solutions to information sharing and technology problems. These include applying risk management principles to identifying security priorities and implementing appropriate solutions; developing an architecture for homeland security; developing analytical and warning capabilities; and establishing goals and performance measures and accountability mechanisms.

Risk Management Principles

Risk management principles should be applied to analyze and identify assets that need to be protected to maintain continuity of critical operations, as well as threats, vulnerabilities, risks, priorities, and countermeasures. It may seem ideal to employ extreme security measures that cover every risk imaginable. But the reality is that this cannot be done, either because doing so could disrupt operations and adversely affect the safety of citizens or the economics of our businesses, or merely be impractical from a resources standpoint. Our previous reports for homeland security and information systems security, [13] have shown that risk management principles can provide a sound foundation identifying security priorities and implementing appropriate solutions. These principles, which have been followed by members of the intelligence and defense community for many years, can be reduced to five basic steps that help to determine responses to five essential questions:

[13] U.S. General Accounting Office, *Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts,* GAO-02-208T, October 31, 2001 and Information Security Management: Learning From Leading Organizations, GAO/AIMD-98-68, May 1998.



The first step in risk management is to identify assets that must be protected to maintain continuity of critical operations and the impact of their potential loss. The second step is to identify and characterize the threat to these assets. Is the threat, for example, that unauthorized individuals can gain access to the building to commit some crime, or more menacing, that a terrorist will introduce a chemical/biological agent or even a nuclear device into the building. Step three involves identifying and characterizing vulnerabilities that would allow identified threats to be realized. In other words, what weaknesses can allow a security breach? In the fourth step, risk must be assessed and priorities determined for protecting assets. Risk assessment examines the potential for the loss or damage to an asset. Risk levels are established by assessing the impact of the loss or damage, threats to the asset, and vulnerabilities. The final step is to identify countermeasures to reduce or eliminate risks. In doing so, the advantages and benefits of these countermeasures must also be weighed against their disadvantages and costs.

In prior reports, we have recommended that the federal government conduct multidisciplinary and analytically sound threat and risk assessments to define and prioritize requirements and properly focus programs and investments in combating terrorism.[14] Without the benefits that

[14] U.S. General Accounting Office. *Combating Terrorism: Selected Challenges and Related Recommendations.* GAO-01-822. Washington, D.C.: September 20, 2001. Also see, *Homeland Security: Key Elements of a Risk Management Approach.* GAO-02-150T. October 12, 2001. *Combating Terrorism: Threat and Risk Assessments Can Help Prioritize and Target Program Investments.* GAO/NSIAD-98-74. Apr. 9, 1998 and *Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attack* GAO/NSIAD-99-163, Sept. 7, 1999.

these assessments provide, many agencies have been relying on worst case chemical, biological, radiological, or nuclear scenarios to generate countermeasures or establish their programs. By using these worst case scenarios, the federal government is focusing on vulnerabilities (which are unlimited) rather than credible threats (which are limited).

Homeland Security Architecture

The federal government should develop a blueprint, or architecture, that defines both the homeland security mission and the information, technologies, and approaches necessary to perform the mission in a way that is divorced from organizational parochialism and cultural differences. This would need to be based on the outcome of a risk assessment along with a good understanding the roles and responsibilities of individuals involved in the homeland security mission. The Office of Homeland Security has acknowledged that an architecture is an important next step because it can help identify shortcomings and opportunities in current homeland security related operations and systems, such as duplicative, inconsistent or missing information. Of course, while the federal government can develop the construct for homeland security, it will be up to state and local governments to carry it out, with a great deal of assistance from the private sector.

Specifically, the architecture should describe homeland security operations in both (1) logical terms, such as interrelated processes and activities, information needs and flows, and work locations and users, and (2) technical terms, such as hardware, software, data, communications, and security attributes and performance standards. It should provide these perspectives both for the current or "as is" environment and for the target or "to be" environment as well as a transition plan for moving from the "as is" to the "to be" environment. A particularly critical function of an architecture for homeland security would be to establish protocols and standards for data collection to ensure that data being collected is usable and interoperable--and to tell people what they need to collect and monitor.

Many organizations have successfully developed enterprise architectures, though on a much smaller scale, and have found that doing so promotes better planning and decisionmaking;

prevents the building of redundant systems; facilitates the management of extensive, complex environments; improves communication and information sharing; focuses on strategic use of emerging technologies; and achieves economies of scale by providing mechanisms for sharing services. Our experience with federal agencies has shown that managed properly, architectures can clarify and help optimize interdependencies and interrelationships among related enterprise operations and the underlying technology infrastructure and applications that support them.

There are readily available frameworks that could be used in developing an architecture for homeland security. These include DOD's C4ISR Architecture Framework, the Department of Treasury's Enterprise Architecture Framework, and the Federal Enterprise Architecture Framework, published by the Federal Chief Information Officers (CIO) Council. In addition, the CIO Council, Office of Management and Budget, and GAO have collaborated in producing guidance on the content, development, maintenance, and implementation of architectures.[15]

Analytical and Warning Capabilities

Analytical and warning capabilities should be developed to detect precursors to terrorist attacks so that advanced warnings can be issued and protective measures implemented. Since the 1990s, the national security community and the Congress have identified the need to establish analytical and warning capabilities to protect against strategic computer attacks against the nation's critical computer-dependent infrastructures. Such capabilities involve (1) gathering and analyzing information for the purpose of detecting and reporting hostile or otherwise potentially damaging actions or intentions and (2) implementing a process for warning policymakers and allowing them time to determine the magnitude of the related risks. In April 2001, we reported on the National Infrastructure Protection Center's progress in developing such mechanisms for computer-based attacks and impediments, which include a lack of a generally accepted methodology for strategic analysis of cyber threats to infrastructures, inadequate data on

[15] Chief Information Officer Council. *A Practical Guide to Federal Enterprise Architecture.* Version 1.0. Washington, D.C.: February 2001.

infrastructure vulnerabilities, and a lack of needed staff and expertise.[16] Similar approaches should be developed for other homeland security priorities.

Goals and Performance Measures and Accountability Mechanisms

Goals and performance measures and accountability mechanisms should be established not only to guide the nation's preparedness efforts to but assess how well they are really working. The Congress has long recognized the need to objectively assess the results of federal programs. For the nation's preparedness programs, however, outcomes of where the nation should be in terms of domestic preparedness have yet to be defined. Given the recent and proposed increases in preparedness funding as well as the need for real and meaningful improvements in preparedness, establishing clear goals and performance measures are critical to ensuring both a successful and fiscally responsible effort. As we testified earlier this year,[17] without measurable objectives, policymakers would be deprived of the information they need to make rational resource allocations, and program managers would be prevented from measuring progress. In our testimony, we highlighted the recommendation of one expert with the Office of Homeland Security that the government should develop a new statistical index of preparedness, incorporating a range of different variables, such as quantitative measures for special equipment, training programs, and medicines, as well as professional subjective assessments of the quality of local response capabilities, infrastructure, plans, readiness, and performance in exercises. The index could go well beyond current rudimentary milestones of program implementation to capture indicators of how well a particular city or region could actually respond to a serious terrorist event.

In conclusion, developing a comprehensive and sustainable homeland security strategy is a formidable, even unprecedented task. Because of the nature of the threat, the scope of the things

[16] U.S. General Accounting Office. *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities.* GAO-01-323. Washington, D.C.: April 25, 2001.

[17] U.S. General Accounting Office. *Combating Terrorism: Critical Components of a National Strategy to Enhance State and Local Preparedness.* GAO-02-548T. Washington, D.C.: March 25, 2002.

that need to be done are seemingly endless. There are significant challenges on a variety of fronts, particularly in making sure that the right information gets to the right people at the right time and in making good use of technology. Moreover, any solution must be national in nature, not just a federal strategy, since over 80 percent of nation's infrastructure is privately owned, and state and local government are the front line defenders and responders in the fight against terrorism. While there are no quick fixes or "silver bullet" single solutions, there are good starting points for addressing specific areas of challenges as well as for weaving solutions together to develop an integrated framework for preventing, detecting, and responding to attacks.

Even with these mechanisms in place, however, there will still be a need for strong leadership on the part of the federal government and the Congress not just to provide the resources, expertise, and training needed carry out the strategy, but to work through concerns and barriers, develop trust relationships, make sure things are working as they should, and most importantly, sustain national attention to the problem.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions that you or members of the subcommittee may have.

CONTACT AND ACKNOWLEDGEMENT

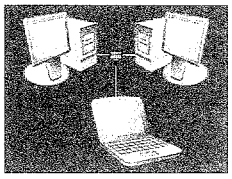
For further information, please contact Randall A.Yim at (202) 512-6787. Individuals making key contributions to this testimony include Cristina Chaplain and Dave Powner.

(976301)

Building Tools to Assess and Detect Terrorist Threats

Getting information to the right people at the right time is critical, but we also need an intelligent strategy to integrate the information. One way is to build baselines of normal activity and mechanisms that will enable us to effectively detect deviations or anomalies that would indicate threats and how serious they may be.

First step: Use Existing Technology



Intrusion detections systems are already being used to protect critical computer networks. These systems are built based on data on normal use of system and network activity as well as known attack patterns. Deviations are discovered based on data from analyses of network packets, captured from network backbones or local area network segments, or data sources generated by the operating system or application software.

Next step: Apply the Same Know-How to Protect Other Infrastructures

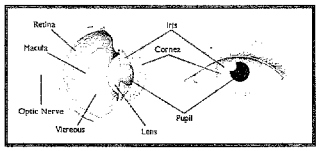
For example, security information systems can be built to assess threats to air travel. Data could be drawn from government watch lists and airline reservations systems. Deviations could be identified by matching names from reservation systems to government watch lists or by detecting unusual patterns in travel or reservations.

The Challenge Ahead

Building systems to predict and detect deviations on larger scale, for example, to protect major cities. This will be an extremely complex and difficult endeavor. For starters, determining what is normal and abnormal activity relative to terrorist activity would be difficult because it would require developing an extensive body of knowledge—beyond just intelligence information—to build a baseline to make terrorist activity standout when the activity itself is elusive, fluid, and difficult to predict.

Technologies that can be used in this regard include geospatial digital information tools, including remote sensing and satellite imagery technology.

Satellite photo with geospatial digitized overlay



Iris scan technology is based on the unique characteristics of the eye's iris, the colored ring that surrounds the pupil.

Developing other new technologies needed to detect and protect people, buildings, and critical infrastructures from attack. This includes

- Bioweapons and low level radioactive weapons detection systems
- Disease surveillance systems
- Biometric devices, such as iris scans, facial recognition systems and speaker verification systems.

Mr. DAVIS OF VIRGINIA. Mr. Forman, thanks for being here.

Mr. FORMAN. Good morning, Mr. Chairman, Congressman Turner and members of the subcommittee. I thank you for your leadership in holding hearings on information sharing and knowledge management issues for Federal agencies in the wake of the terrorism attacks. The President's announcement last night demonstrates that the administration considers homeland security to be a top priority. The enterprise architecture and e-government initiatives I'll discuss today will assist in accomplishing this mission.

As you know, many Federal agencies are engaged in homeland security efforts that will require sharing information. Associated with that are many IT projects that are overlapping or redundant, when we need them to be integrated and unified. For example, there are eight law enforcement case management systems among our largest IT investments. To ensure investments improve operational performance across agencies, the President proposed in the fiscal year 2003 budget request the creation of an information integration program office known in the budget as the Homeland Security Information Technology and Evaluation Program within the Department of Commerce's Critical Infrastructure Assurance Office.

I'll discuss five key barriers that need to be addressed for finding, tracking and responding to terrorist threats. Creating the Information Integration Program Office is critical to overcoming these barriers.

The first impediment concerns agency culture. Agency cultures reflect long-standing roles and responsibilities. Homeland security activities affect roles and responsibilities that cut across jurisdictions of Federal, State and local government organizations. Barriers associated with insular agency cultures will be overcome by providing a sustained level, high level of leadership and commitment, establishing an interagency government structure and giving priority to cross-agency work.

Second, citizens must trust the security and privacy of the government. Achieving a secure homeland must be accomplished in a manner that builds trust, preserves liberty and strengthens our economy. Agencies are currently building strong controls into both e-government and homeland security systems. OMB will monitor agency security and privacy performance, as I've noted in previous statements before this subcommittee.

Third, a major obstacle is a lack of funding for initiatives that cross agency boundaries. Funding is provided in a manner that matches long-standing departmental silos. We are seeing this issue as we've tried to obtain funding for cross-agency e-government initiatives and the Information Integration Program Office. We have recommended approaches such as greater Appropriations Committee attention to cross-agency issues.

A fourth difficulty is stakeholder resistance. The Federal Government is not structured for undertaking cross-agency initiatives. These initiatives threaten traditional concepts of accountability and responsibility. Stakeholder resistance will be minimized by timing performance evaluations to cross-agency success and having members of the President's Management Council work collectively on

initiatives. The Information Integration Program Office will also assist in this regard.

Fifth and finally, the lack of a Federal enterprise architecture hampers efforts to communicate across business lines. Agencies generally buy systems that address internal needs, and rarely are those systems able to interoperate or communicate with people in other agencies. A common integrated business and technology architecture will help to organize these systems and the information they contain in order to retrieve, analyze and act upon information.

The Federal Government requires business processes that allow for a comprehensive approach to prepare for, mitigate and respond to terrorist activities. It's critical to have the Information Integration Program Office design interagency business and information architectures that will support this interagency access to information.

OMB and the Office of Homeland Security are currently defining a baseline of homeland security-related activities that serve as components in the Federal business reference model. The baseline lists those problems, constraints and gaps within the government's information and data base and recommends actions to address those gaps; additionally will identify modular and reusable IT capabilities and ways to configure it to support key homeland functions and the lines of business.

As noted in the President's budget, e-government projects have significant impact on homeland security efforts, and today I'd like to discuss three of those projects.

Project SAFECOM will identify and implement solutions that enable interoperability for public safety communication across all levels of government. Additionally, the administration's Geospatial One-Stop will build a distributed infrastructure that enables use of seamless, standardized geographic and geospatial data. Third, the administration's disaster management e-government initiative will be the authoritative one-stop shop for end-to-end information and services related to Federal disaster management activities.

Improving our interoperability with State and local partners is a key piece of the President's management agenda for e-government and for homeland security.

In conclusion, the administration is focused on identifying, locating and establishing mechanisms to share across government the information required to protect the Nation's border and to prepare for, mitigate and respond to terrorist activities. The President's budget noted that we need to focus these efforts on two measures of success: First, accelerating response time, and second, improving decisionmaking quality.

I appreciate the opportunity to brief you today on how we are integrating the work and results of homeland security enterprise architecture and e-government initiatives.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

[The prepared statement of Mr. Forman follows:]

STATEMENT OF
MARK A. FORMAN
ASSOCIATE DIRECTOR FOR INFORMATION
TECHNOLOGY AND ELECTRONIC GOVERNMENT
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON TECHNOLOGY AND PROCUREMENT POLICY
U.S. HOUSE OF REPRESENTATIVES

June 7, 2002

Good morning Mr. Chairman and members of the Subcommittee. Thank you for inviting me here today to discuss information sharing and knowledge management issues for Federal agencies in the wake of the terrorism attacks on America. I will discuss these issues in the context of developing the Federal government's enterprise architecture, the Administration's electronic government initiatives, and the President's Management Agenda.

Office of Homeland Security: Information Integration Program Office

As you know, both the number of Federal agencies and the number of Federal programs dealing with homeland security issues are vast and varied. To leverage our resources and coordinate activities, the President proposed in the FY03 budget request the creation of an Information Integration Program Office (IIPO) within the Department of Commerce. The office will enable implementation of programs and projects focused on the integration of information essential to combating terrorism nationwide. The most important function of this office will be to design and help implement an interagency information architecture that will support efforts to find, track, and respond to terrorist threats within the United States and around the world, in a way that improves both the time of response and the quality of decisions. Together with the lead federal agencies, and guided strategically by the Office of Homeland Security, the IIPO will produce roadmaps (migration strategies) that will be used by the agencies to move to the desired state. This target architecture will be integrated with OMB's Federal enterprise architecture effort.

The Office of Homeland Security and the Information Integration Program Office will also define near-term pilot projects and proof of concept initiatives that can immediately address short-term OHS requirements. These short–term efforts can offer immediate results while putting in place the foundations for continuous improvement.

Addressing Potential Barriers to Information Sharing

It is essential for agencies to transition to business processes that support the exchange of information in real time. In many cases, this will require substantial reengineering of business applications. Last summer, the Administration's E-government Taskforce identified five barriers to information sharing and cross agency initiatives. Although these barriers were identified for E-government, they are also relevant to homeland security. Information sharing is

a massive change management initiative and needs to be approached and managed as such. These same barriers must be successfully mitigated to advance homeland security goals. Overcoming these obstacles will lead to increased and improved information sharing both within and outside the Federal government.

1. Agency culture

There must be a clear articulation of the roles, responsibilities, and jurisdictions of the Federal agencies and State and local government organizations involved in homeland security activities. All levels of government must work together to share critical data related to intelligence gathering and analysis, crisis management and consequence management activities. In addition, the roles and responsibilities of the private sector also must be defined.

Barriers associated with insular agency cultures will be overcome by: 1) providing a sustained high level of leadership and commitment; 2) establishing an interagency governance structure; 3) giving priority to cross-agency work; and 4) engaging interagency user/stakeholder groups in mapping process and information use to identify opportunities to reduce cycle time and improve quality.

2. Public Trust

A successful E-government strategy must deploy risk-based and cost-effective controls to ensure the security of the Federal government's operations and assets. Security is integral to both the E-Government and Homeland Security initiatives. Additionally, all E-government and homeland security initiatives, where applicable, must comply with security requirements in law, OMB policy, and technical guidelines developed by the National Institute of Standards and Technology. These initiatives must also ensure privacy for personal information that is shared with the Federal government. Achieving a secure homeland must be accomplished in a manner that builds trust, preserves liberty, and strengthens our economy. The Administration's e-Authentication project addresses security and privacy concerns by enabling mutual trust to support widespread use of electronic interactions between the public and government and across government by providing common avenues to establish "identity". It will provide a secure, easy to use and consistent method of proving identity to the Federal government that is an appropriate match to the level of risk and business needs of each e-gov initiative. In addition, project teams will address privacy concerns regarding the sharing of personal information. E-Government depends on confidence by citizens that the government is handling their personal information with care. Agencies are working on building strong privacy protections into both E-government and Homeland security initiatives and OMB is focusing on government wide privacy protections by all agencies.

3. Resources

A major obstacle to success is the method of funding federal initiatives that cross agency boundaries. What is needed for homeland security as well as E-government success is the ability to fund government-wide initiatives by appropriating across agencies - not under the purview of any single agency. Just like the information 'stovepipes' that must be overcome, funding is provided in a 'stovepipe' manner. Appropriation committees are constrained in funding desired cross-agency initiatives or projects, because of difficulties with the current processes that do not

easily permit this type of funding. Working with Congress, we have begun to undertake steps to address this issue, e.g. through proposed funding through the FY02 supplemental and FY03 budget process for the establishment of the Homeland Security Information Integration Program Office. We look forward to continuing to work with you on this issue.

This same issue arose with respect to funding for the Administration's E-government initiatives. E-Government initiatives are targeted at improving the quality of services to citizens, business, governments and government employees, as well as the effectiveness and efficiency of the Federal government. E-Government initiatives will identify resources, which should be moved to programs with the greatest return and citizen impact. Performance measures will then be created and used to monitor implementation.

It is clear that information sharing must be addressed both vertically (sharing with State, local governments and other organizations) and horizontally (across the Federal government). The President's Budget proposes $722 million for improvements to information –sharing within the Federal government and between the Federal government and other State and local governments. Technology investments will improve the performance of agencies in preparing for, detecting and responding to threats to homeland security. The Office of Homeland Security is charged with facilitating the development of an appropriate physical infrastructure and policies to ensure that threats are conveyed vertically to State and local officials in a timely manner. This will enable all agencies with homeland security responsibilities to access threat information throughout the government.

4. Stakeholder Resistance

The Federal government is not structured for undertaking cross-agency initiatives. Existing budget processes, operational practices, and agency cultures perpetuate bureaucratic divisions of labor. In addition, fear of reorganization creates resistance to integrating work and sharing use of systems across agencies. Legal and policy requirements may create additional barriers to achieve homeland security and E-government mission and therefore increase stakeholder resistance.

Cross agency initiatives threaten traditional incentives associated with accountability and responsibility. Stakeholder resistance will be minimized by tying performance evaluations to cross-agency success, and having President's Management Council members work collectively on initiatives. In addition, the OHS Information Integration Program Office will work to overcome stakeholder resistance to information sharing initiatives.

5. Lack of a Federal Architecture

Timely access to accurate and complete information is absolutely essential to prepare for, mitigate, and respond to terrorist activities. The information systems used by organizations and individuals involved in homeland security efforts must collect, maintain, provide access to, share, and protect the data and information across organizational boundaries. A common, integrated business and technology architecture will help to organize these systems and the information that they contain. Agencies generally buy systems that address internal needs, and rarely are the systems able to interoperate or communicate with those in other agencies. Consequently, agencies cannot easily share information.

In order to retrieve, analyze and act upon information in a timely manner, the Federal government requires building architectures that allow for a comprehensive approach to:

1) prepare for, mitigate, and respond to terrorist activities;
2) understand the business functions, processes, and activities necessary to effectively integrate key security functions and technologies to protect our Nation's borders and combat terrorism; and
3) identify workforce needs such as the competencies, capabilities, and accurate and complete information required to adequately perform their work.

The National Strategy currently being developed by the Office of Homeland Security will articulate the vision and objectives that must be addressed collaboratively by Federal, State, local, and private sector entities.

Improving Horizontal and Vertical Information Sharing

OMB created a Federal enterprise architecture program management office to develop the Federal government's first enterprise architecture. This office will play a critical role in addressing the operational, organizational and institutional, as well as technological requirements to meet the government's homeland security goals.

The foundation piece of the Federal Enterprise architecture is the business reference model. A business reference model is a function-driven framework that describes the lines of business and internal functions performed by the Federal government regardless of the Federal agencies that perform them. The first iteration of this model, which addresses the entire Federal government, has been developed and vetted with the agencies. In conjunction with the Office of Homeland Security, we are currently defining a baseline of homeland security related activities that serve as components in the business reference model. The baseline: 1) identifies the specific business functions, processes, and activities that support homeland security related mission, program, and business lines; 2) defines and locates the data and information necessary to support homeland security activities; 3) assesses problems, constraints, and gaps within the government's data and information base; and 4) recommends actions to address them. These efforts will be completed within the next 90- to 120-days and will support the Office of Homeland Security.

In addition, the Government to Government (G2G) initiatives contained in the President's Management Agenda under E-government, will enable sharing and integration of Federal, state and local data to facilitate better performance of key government operations, such as disaster response. The G2G initiatives also improve grant management capabilities, as required by the Federal Financial Assistance Improvement Act (P.L. 106-107). These initiatives strongly support "vertical" (i.e. intergovernmental) integration necessary to meet homeland security goals.

As noted in the President's budget, E-Government projects in the G2G portfolio have significant impact on our homeland security efforts. I would like to discuss three of the Administration's E-government projects – Project SAFECOM, the Geospatial One-Stop and Disaster Assistance and Crisis Response.

Project SAFECOM – Wireless Interoperability

Project SAFECOM is a key initiative that addresses the need for interoperable communications among Federal, State and local public safety officials. Establishing on-scene communications for first responders in a timely manner is crucial to saving lives and reducing property damage. We have all heard accounts of first responders that lacked the ability to communicate at a critical time. As a nation, we devote significant resources towards our wireless infrastructure – and yet there remain gaps in our ability to communicate. Project SAFECOM will identify and implement solutions that enable interoperability for public safety communications across levels of government.

The Project SAFECOM team is working closely with the Office of Homeland Security and the Federal enterprise architecture program management office to define a concept of operations and an architectural framework for the wireless public safety solution. The team is assessing horizontal information sharing processes and data requirements in support of Federal to Federal interoperability. Next, the team will develop vertical voice, data, and telecommunication protocols to enable Federal to State interoperability. Project SAFECOM will deliver initial deployment of new capabilities by next summer.

In addition, HSPD-3 articulated the need for a Homeland Security Advisory System, which also directed the Attorney General to develop a means of communicating and conveying threat advisories horizontally and vertically. HSPD-4, now in draft form, will ensure that classified and sensitive-but-unclassified homeland security-related information can be communicated to federal, state, local and private sector officials who need it.

To that end, we are working on a system of ensuring that States have secure communications suites (SVTS systems, STE's, secure faxes) so that they can communicate through secure means to each other and their federal counterparts. Also working on a "homeland security portal system" that will allow federal, state, local and private sector officials the ability to communicate through a VPN system and to access disparate databases (watch lists, LEO, RISS.NET) on one screen through the application of middleware technology."

The Geospatial Data One-Stop

Geospatial data is the backbone for homeland security and government management initiatives across all levels of government. It is the information that identifies the geographic location and characteristics of natural or constructed features on the Earth. This information may be derived from remote sensing, mapping, charting, surveying, the Global Positioning System, environmental monitoring, or statistical data. It is critical that geospatial data assets are: 1) created; 2) well maintained; 3) readily available to those who need them; and 4) interoperable.

Examples of the application of geospatial data for homeland security include physical infrastructure locations, graphical depiction of building infrastructure and detail, and real time tracking of cargo delivery.

Federal, State and local governments also have business needs for geospatial data beyond homeland security. In fact, local governments have been building geospatial data sets for many years. Geospatial systems have never been coordinated, making interoperability difficult and

expensive. Therefore our goal at the Federal level should not be to buy redundant and separate datasets. Instead we should use our federal dollars to invest and leverage state and local assets and expertise. With today's technologies and by aligning with State and local governments, we can get better returns for our investment.

In its first phase, the Geospatial One-Stop will establish national standards for the most commonly used data sets. Phase two will build a distributed infrastructure that enables the discovery and use of seamless, standardized geospatial data. Ultimately, the goal of the Geospatial One-Stop is to harmonize, align, and focus intergovernmental investments in geospatial data.

Disaster Management

This initiative will be the authoritative one-stop shop for end- to-end information and services related to Federal disaster management activities. These activities cover the spectrum of Preparedness, Response, Recovery and Mitigation, and apply to all of the signatory organizations of the Federal Response Plan. Functions within each of these activities include transportation, communications, resource support, firefighting, public works and engineering, information and planning, mass care, health and medical services, urban search and rescue, hazardous materials, food and energy.

Information Sharing Success Rests on Collaboration

The G2G initiatives and the homeland security initiatives will fail without strong coordination between Federal, State and especially local governments. Timely, accurate information, easily accessible and capable of being shared across federal, state, and local jurisdictions is fundamental to the decision making capability of those tasked with the homeland security mission. Therefore, improving interoperability with our State and local partners is a key piece of the President's Management Agenda under E-government and homeland security, and requires the involvement of the private sector.

Currently, discussions are underway with the National Association of State Chief Information Officers (NASCIO) to coordinate their work with the Federal enterprise architecture effort. This should lead to the identification of business processes identified in the Federal enterprise architecture that are common to multiple levels of government, and that can be coordinated – such as border protection and emergency preparedness, mitigation, and response. This will assist in identifying key homeland security processes and systems that can be targeted for joint attention.

Technology Acquisition to Address Barriers and Assist Information Sharing

As defined in the Clinger Cohen Act, technology purchases must be based on business process and organizational improvement. The Administration's efforts to establish the Federal enterprise architecture will help to define the requirements, capabilities, computing and communications platforms, and supporting products and standards necessary to share information across Federal agencies, and with State and local government organizations. The key issue in technology

acquisition continues to be identification of valid requirements. The Federal enterprise architecture will include a set of "business reference models" and "component-based architectures" that will be shared across government organizations and with private industry to help them better understand and address the information management requirements to meet homeland security goals.

As mentioned earlier in the testimony, the business reference models are a function-driven framework that describe the lines of business and internal functions performed by the Federal government independent of the Federal agencies that perform them. They will help to shed light on the Federal government's expectations and needs in the areas of homeland security performance and outcomes, business activities, application-capabilities, data and information management, and technical computing requirements. The reference models can be incorporated into acquisition and procurement packages to ensure that government solicitations and industry options will effectively and efficiently meet Federal information management and technology requirements, including information sharing. Additionally, the component-based architectures will identify modular and reusable IT capabilities and configurations to: 1) support border protection; 2) prepare for, mitigate, and respond to terrorism; 3) gather and analyze intelligence information; 4) manage crises; and 5) support first responders. The components will be built in accordance with applicable business reference models. The overarching intent is to expedite access to important information processing capabilities, reduce unnecessary redundancy, and promote government wide interoperability and information sharing.

Linkage of the business reference models and the component architectures will occur through the annual budget process. The business reference model will serve as the business layer of the Federal enterprise architecture and will provide a foundation on which the applications, data, and technology layers of the Federal enterprise architecture are developed. Agency capital asset plans or business cases, submitted as part of the agency's budget, will be mapped against this framework to identify opportunities for cross-agency collaboration and potential system redundancies. OMB's A-11 guidance is currently being modified to ensure that cross agency IT buys are made in conjunction with this best practice approach.

Steps to Overcome Information Stovepipes

New agency information technology investments must specify standards that enable information exchange and resource sharing, while retaining flexibility in the choice of suppliers and in the design of work processes. They must also address security needs. As you know, the President has given a high priority to the security of government assets including government information systems and the protection of our nation's critical information assets from cyber threats and physical attacks. We believe that protecting the information and information systems that the Federal government depends upon requires agencies to identify and resolve current security weaknesses and risks, as well as protect against future vulnerabilities and threats. OMB will continue to monitor and measure agency security performance through their annual security reports and the budget process.

The Administration's ongoing effort to establish the Federal enterprise architecture is helping to identify, locate, and establish mechanisms to share across government the information required to protect the Nation's borders and to prepare for, mitigate, and respond to terrorist activities. Over time, every agency has developed its own set of business processes and supporting IT

systems. These "stovepiped" systems were built with the intention of supporting a specific business unit or function and never contemplated data exchanges with other systems in the organization. E-Government and homeland security requires us to exchange data across organizations at the federal level as well as with our partners in State and local governments, and the citizen. To overcome these rigid systems, we are using enterprise architecture best practices. This will enable us to develop simpler, more efficient business processes. Best practices combined with information technologies allow us to quickly develop and implement simple and more efficient business processes including processes for homeland security initiatives.

Conclusion

I appreciate the opportunity to brief you today on the Administration's homeland security efforts, enterprise architecture work, E-government initiatives, and most importantly how we are integrating the work and results of each of these programs. I look forward to updating you on future progress. Our mutual success is dependent on swift and supportive action by Congress to assist us in addressing the barriers we have identified. As you know, the matter of homeland security is not a political issue it is an American issue. The Administration will continue to work collaboratively across Federal agencies and with State and local governments to strengthen information sharing in support of homeland security efforts.

Mr. TOM DAVIS OF VIRGINIA. Mr. Bohlinger.

Mr. BOHLINGER. Morning, Mr. Chairman and members of the committee. I appreciate the opportunity to participate in your continuing review of information sharing and knowledge management between and among Federal agencies in the war against terrorism.

Since September 11th, we at the Immigration and Naturalization Service have seen the unprecedented sharing of data and knowledge among Federal agencies. Under the direction and leadership of the Attorney General, all components of the Department of Justice have stepped up efforts to coordinate information and improve data sharing in the common effort to prevent terrorism and disrupt its sources.

The INS is clearly one of the core agencies that requires enhanced information-sharing capabilities. Just as we need to tap into additional external sources of data to support our enforcement and intelligence functions, so can the data we collect be crucial to other law enforcement and intelligence communities. Consequently, we are deeply involved in efforts to overcome the barriers to the appropriate and secure exchange of data and, just as importantly, the conversion of data to useful information that supports clear operational objectives.

The INS has worked on important data-sharing initiatives in both the pre- and post-September 11th periods. As early as 1985, INS was sharing vital information with the U.S. Customs Service. Other data-sharing programs have been under way for some time with the Department of State, the U.S. Marshals Service, the FBI and the Social Security Administration. INS also assists State and local law enforcement through its Law Enforcement Support Center.

We also verify immigration status for State and local benefit-granting agencies, some employers and some State driver's license bureaus. However, in all of these data-sharing initiatives, we have to be sensitive to established regulatory, statutory and policy constraints in the routine and customary use of information by other agencies. While making information available to other entities, security, privacy considerations and appropriate user access are primary considerations.

The management principle guiding INS's approach to development of information systems is to build a sound strategic foundation. INS has established important mechanisms to address this principle internally. Our initial contribution to a governmentwide effort is to assure that our own information environment is sound and interoperable. Our formal enterprise architecture and technical architectures are nearing completion. Additionally, our information technology investment management process ensures that IT investments are spent wisely and coordinated among INS components. In doing so, we are mindful of the relationships that we must support with our technical enhancements while integrating our business objectives and developing technical solutions.

The development and prioritization of clear and integrated Federal law enforcement in intelligence mission requirements is an undertaking that must be completed quickly. Only when these are clearly articulated can industry assist us meaningfully in applying the best technical solutions.

Some of the most compelling progress that I have seen in recent months has been the formalization of the planning and management processes that must occur if the wide array of Federal, State, local and private entities are to achieve the level of information sharing that we all desire. This will ensure that we first define what our operational objectives should be, identify the data and data sources needed to support those objectives, and then apply the appropriate technological solutions to deliver that information. This leads to the crucial task of examining the barriers that may inhibit or otherwise thwart full partnership between public and private sectors in coming together in the war against terrorism.

Barriers come in two forms, human and technological, and they manifest themselves three ways, through cultural, organizational or resource approaches. Like many of my colleagues, I have met with representatives from the private sector who have proffered technologically based products and solutions to any number of counterterrorism-driven prevention, detection and mitigation scenarios. Their sincerity and commitment are of the highest order. Unfortunately, in many instances, they perceive the Federal Government as an unresponsive bureaucracy. Some have suggested that the Federal procurement process may be to blame. However, I believe it would be a mistake to look at the procurement process as the sole culprit. If clear requirements can be formulated, many procurement alternatives are available that can fulfill our needs while ensuring broad participation by industry.

Without well-defined requirements, even the best solutions stand little chance of effective and timely application. Encouraging the private sector to participate in problem solution through the request for information as well as other processes prior to the initiation of a formal procurement makes good sense. This will preserve a fair and open procurement process enabling the government to make best use of America's technological superiority and the creative problem-solving resources in the private sector.

In summary, we in the Federal Government must establish and employ standards for information sharing between and amongst ourselves and further fully define our mission requirements or needs. Then we can take advantage of the wealth of existing technology solutions that currently exist within Federal agencies and corporations. This will enable us to develop solutions that better balance our openness to new ideas with applications that directly address our needs.

Thank you, Mr. Chairman, for this opportunity, and I appreciate the opportunity to appear with you—before you and the committee.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

[The prepared statement of Mr. Bohlinger follows:]

U.S. Department of Justice
Immigration and Naturalization Service

STATEMENT OF

GEORGE H. BOHLINGER, III
EXECUTIVE ASSOCIATE COMMISSIONER FOR MANAGEMENT
U.S. IMMIGRATION & NATURALIZATION SERVICE

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON TECHNOLOGY AND PROCUREMENT POLICY

REGARDING
REVIEW OF COORDINATED INFORMATION SHARING
AND KNOWLEDGE MANAGEMENT ISSUES
FOR KEY FEDERAL AGENCIES
IN THE WAKE OF TERRORISM ATTACKS ON AMERICA

FRIDAY, JUNE 7, 2002

2154 RAYBURN HOUSE OFFICE BUILDING

10:00 A.M.

GOOD MORNING MR. CHAIRMAN AND MEMBERS OF THE COMMITTEE.

I appreciate the opportunity to participate in your continuing review of "coordinated information sharing and knowledge management" between and among Federal agencies in the war against terrorism. I am particularly interested in addressing the Committee's desire to examine barriers that may hinder coordinated sharing and management, both within the Federal community, and between the Federal community and the private sector.

Since September 11, we at the Immigration and Naturalization Service (INS) have seen the unprecedented sharing of data and knowledge among federal agencies. Under the direction and leadership of the Attorney General, all components of the Department of Justice have stepped up efforts to coordinate information and improve data sharing in the common effort to prevent terrorism and disrupt its sources.

Congress signaled its support for these efforts by enacting the Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173) on May 14, 2002. As you know, this legislation requires the INS to fully integrate all of its databases and data systems that process or contain information on aliens. This integrated system will become part of the interoperable electronic data system, called Chimera. This system, when completed, will provide current and immediate access to information in law enforcement and intelligence databases relevant to determine whether to issue a visa and to determine the admissibility of an alien.

The INS is clearly one of the core agencies that requires enhanced information sharing capabilities. We need to tap into additional external sources of data to support our enforcement and intelligence functions, and we recognize that the data we collect can be crucial to the law enforcement and intelligence communities to combat the threat of terrorism.

Consequently, we are deeply involved in efforts to overcome the barriers to the appropriate and secure exchange of data and, just as important, the conversion of that data to useful information that supports clear operational objectives.

Mr. Chairman, before addressing the impediments to progress, let me begin by describing some important things we are already accomplishing in addressing these barriers.

As you know, the Office of Homeland Security, in conjunction with the Office of Management and Budget, is overseeing initiatives that promote information sharing between Federal agencies horizontally, and then from those agencies to State and local governments. We are working directly with State governments to improve the information available to support enforcement efforts. We are working internationally to develop better ways of sharing information that will support international enforcement and intelligence operations.

From my perspective, I cannot over-emphasize the commitment of the INS and other participants to work together in order to achieve a more supportive and comprehensive information environment.

Prior to September 11, the INS shared data in many ways with other agencies in support of law enforcement efforts. Since then we have redoubled our efforts to contribute data and information that have supported counter-terrorism intelligence, investigative, and enforcement operations.

One of the most important initiatives that we have worked on is the Foreign Terrorist Tracking Task Force (FTTTF), which the President directed the Department of Justice to establish on October 30, 2001. The mission of the FTTTF is to keep foreign terrorists and their supporters out of the United States by providing critical and timely information to border control and interior enforcement agencies and officials. To do so requires electronic access to large sets of data, including the most sensitive material from law enforcement and intelligence sources. The INS works hand-in-hand with the FTTTF to discern patterns and probabilities of terrorist activities and to ensure that data is properly shared.

For many years, the INS has taken steps to enhance the exchange of information through greater cooperation among the law enforcement community. As early as 1985, the INS was sharing vital information with the U.S. Customs Service through the Interagency Border Inspection System (IBIS), the primary automated screening tool currently used by Customs and the INS to which many Federal agencies contribute lookout information. Since that time, we

have put in place a number of other initiatives to exchange information with other entities, which are in various stages of implementation.

For example, the INS and the Department of State recently expanded our ongoing datashare efforts. INS inspectors at ports-of-entry now have access to biometric data on all visa applicants, including digitized photographs, and are able to compare the photograph of the individual standing before them with the photograph of the individual who actually applied for the visa abroad.

Another example involves the sharing of fingerprint data. Prior to September 11, the INS had worked with the U.S. Marshals Service to incorporate fingerprint data of their wanted persons into the INS fingerprint identification system known as IDENT. After September 11, the INS worked with the Federal Bureau of Investigation (FBI) to incorporate fingerprint data from their Integrated Automated Fingerprint Information System (IAFIS) "wants and warrants" file into IDENT as well. IAFIS contains fingerprints for persons wanted by Federal, State, and local law enforcement agencies. This effort has been extremely successful and has already resulted in the identification and apprehension of over 1,600 individuals wanted for felony crimes.

One of the primary ways the INS assists State and local law enforcement is through the INS Law Enforcement Support Center (LESC). The primary mission of the LESC is to support other law enforcement agencies by helping them determine if a person they have contact with, or have in custody, is an illegal, criminal, or fugitive alien. The LESC provides a 24/7 link between Federal, State, and local officers and the databases maintained by the INS.

We also maintain a data sharing project with the Social Security Administration (SSA) through their participation in the INS Systematic Alien Verification for Entitlements (SAVE) program. Using the SAVE program, SSA has access to the Alien Status Verification Index, which provides alien status information. SSA uses this information to determine if a Social Security Number should be issued to a noncitizen applicant.

We also verify immigration status for State and local benefit granting agencies, some employers, and some State driver's license bureaus. For example, the INS has an ongoing data

sharing initiative with the California Department of Motor Vehicles to enhance the integrity of their driver's license issuance process by providing information to verify that applicants are lawfully present at the time they apply for a license or State identification card.

We have intensified our efforts to share critical information with other law enforcement entities following the tragic events of September 11. We are coordinating with law enforcement officials at all levels -- Federal, State, and local – which are working together, coordinating information and sharing knowledge resources in the joint effort to avert and disrupt terrorist activity.

However, in all of these data sharing initiatives, we have to be sensitive to all established regulatory, statutory, and policy constraints in the routine and customary use of information by other agencies. When making information available to other entities, security, privacy considerations and appropriate user access are primary considerations. The INS has created a standing review body to ensure these issues are addressed with each data sharing request.

The Federal Government maintains a number of databases that provide real-time information to foreign diplomatic outposts, border points- of-entry, and interior domestic law enforcement. We work closely with these agencies to prevent terrorists from entering the United States, to detect and apprehend those already in the country, and to gather intelligence on terrorist plans and activities or conspiracies.

Examples of systems that share data include:

- The Department of State TIPOFF System--designed to detect known or suspected terrorists who are not U.S. citizens as they apply for visas overseas or as they attempt to pass through U.S., Canadian, and Australian border entry points.
- The FBI's National Crime Information Center--the nation's principal law enforcement automated information sharing tool. It provides on-the-street access to information to over 650,000 Federal, State, and local law enforcement officers.
- The Interagency Border Inspection System (IBIS)--the primary automated screening tool used by both the INS and U.S. Customs Service at ports-of-entry. The inclusion

of terrorist data in this integrated database helps preclude the entry of known and suspected terrorists into the U.S., warn inspectors of a potential security threat, and alert intelligence and law enforcement agencies that a suspected terrorist is attempting to enter the U.S. at a specific location and time.

Mr. Chairman, having addressed what we have been doing to deal with the immediate challenges in response to guidance from Congress and the Administration, let me turn to the activities that address emergent issues on the horizon.

The management principle guiding the INS' approach to development of information systems is to build on a sound strategic foundation. The INS has established important mechanisms to address these principles internally. One of these mechanisms is our formal enterprise architecture and technical architectures, which are nearing completion. Additionally, an Information Technology Investment Management (ITIM) process has been in place for over three years. ITIM is the standardized process by which investment dollars are approved for information technology (IT) projects. This process ensures that IT investments are spent wisely and coordinated among INS components. In doing so, we are mindful of the relationships that we must support with our technical enhancements while integrating our business objectives and developing technical solutions.

ITIM and our formal enterprise and technical architectures will support the development of mission objectives. The development and prioritization of clear and integrated Federal law enforcement and intelligence missions is an undertaking that must be completed quickly. Only when these are clearly articulated can industry assist us meaningfully in applying the best technical solutions.

Some of the most compelling progress that I have seen in recent months has been formalization of the planning and management processes, as exemplified by the Attorney General's directive of April 11, 2002, to coordinate information relating to terrorism, that must occur if the wide array of Federal, State, local and private entities are to achieve the level of information sharing that we all desire. Structures are being developed that will bring discipline

to the development and application of technology that will ensure we first define what our operational objectives should be, identify the data and the data sources needed to support those objectives, and then apply the appropriate technology solutions to deliver that information.

As I stated previously, I am particularly interested in examining and understanding what barriers may exist that inhibit, or otherwise thwart, full partnership between the public and private sectors in coming together in the war against terrorism. Like many of my colleagues, I have met with a myriad of representatives from the private sector who have proffered technologically-based products and solutions to any number of counter-terrorism driven prevention, detection, and mitigation scenarios. Their sincerity and commitment are of the highest order. Unfortunately, in many instances, they perceive the Federal Government as an unresponsive bureaucracy.

Some have suggested that the Federal procurement process may be to blame. However, I believe it would be a mistake to look at the procurement process as the culprit. If clear requirements can be formulated, many procurement alternatives are available that can fulfill our needs, while ensuring broad participation by industry.

One example of identifying our requirements is in the implementation of the Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173). The INS is in the process of identifying information needs from Federal law enforcement and the intelligence community to improve national security. We continue to value private sector input through the Request for Information process prior to initiation of a formal procurement process, while preserving a fully fair and open procurement process.

There are a number of information technology professional associations that provide venues for exchange of issues, discussions of requirements and development of ideas. The INS is fully engaged in these opportunities. We have been steadfast in articulating our position to industry, and our willingness to engage in active and meaningful partnerships, not only during procurements, but also post award.

In summary, we in the Federal Government must establish and employ standards for information sharing between and among ourselves and further, fully define the mission requirements or needs. Then we can take advantage of the wealth of existing technology solutions that are already out there, but which may be imbedded within individual agencies and corporations. This will enable us to knit solutions together in a meaningful way to better balance our openness to new ideas with focus on applications, which directly address our needs.

Thank you Mr. Chairman for this opportunity to share my views with you and the Committee.

# # #

Mr. TOM DAVIS OF VIRGINIA. Dr. Raub.

Mr. RAUB. Morning, Mr. Chairman, Mr. Turner, members of the committee. I appreciate the opportunity to represent the Department——

Mr. TOM DAVIS OF VIRGINIA. Push your button there.

Mr. RAUB. I appreciate the opportunity to represent the Department of Health and Human Services and describe our activities related to the theme of the hearing this morning.

With your permission, Mr. Chairman, I'll submit my prepared statement for the record and make only a few comments now. First has to do with the item on our perception of barriers to achieving homeland security.

With respect to bioterrorism and other aspects of public health emergencies, we believe we face formidable problems, but that none of them are intrinsically insurmountable. We don't believe that we can anticipate every threat scenario, but we do believe that with a strong, sustained and closely coordinated effort among public health, medical, scientific and technological communities, we can develop the basic capabilities we need to respond effectively.

On pages 3 and 4 of my prepared statement, I summarize five fundamental functions that a local community must be able to do if it is able to respond effectively to bioterrorism or some other public health emergency. All five of those functions currently are doable with current knowledge and current technology. Doing any one of them is hard. Doing all five is very hard. Doing all five in every community in the country is daunting. But that's, in fact, what we're attempting to do.

We have a vigorous effort under way and our State and our local partners are responding enthusiastically to this. The President and the Congress for this fiscal year have provided more than $1 billion for this purpose, and we have moved very quickly to mobilize it. Moreover, the President is requesting more than $1.5 billion for the similar purpose in fiscal year 2003. We have in place cooperative agreements with every State and other eligible entities. We are well along with them in their work plans for use of these funds. These plans focus on particular targets, things we call critical benchmarks and critical capacities, and the watchwords for all of this are speed, flexibility and accountability; speed in getting the money out, flexibility in giving the State and others considerable discretion in how they address the benchmarks we've set out, but also accountability, because at the end of the day, unless we have measurable milestones and objective evidence of enhanced preparedness, we will not have met the charge of the President and the Congress.

My second area of comment has to do with information technology and its applications in that in every one of those five fundamental functions and many other aspects of public health, information technology is absolutely central to public health preparedness. I'm talking about electronic communications, computer-manipulable data bases and about statistical and analytical software. The information technology community has presented us with a wealth of tools and, in fact, is way ahead of our ability to apply them right now.

In some States in this Nation, the public health capabilities are already linked by high-speed Internet connections with substantial computer systems supporting them. In other public health departments in our Nation, there are no computers. There are no Internet connections. There are rotary telephones, and case reports arrive by postcard. We have a substantial effort in front of us to reduce the variance in this.

Our immediate challenge is to choose judicially amongst the information technology options available to us as a community with respect to the effectiveness for our immediate and longer-term purposes, the efficiency and the economy with which we can deploy them, and, most of all, achieving the interoperability. Unless these systems link at every level from the fundamental connections to the operating systems, to the applications programs, we will fail in achieving the kind of true public health system we must achieve.

Our Centers for Disease Control and Prevention has promulgated a set of information technology standards. It's been adopted by our other agencies and is being used in our efforts with not only State and local health departments, but also hospitals throughout the United States.

As this effort evolves with our State and local partners, we look forward to our and their collaborations with the information technology industry as we can catch up and make more effective use of what's available and as they proceed to offer us a still richer array of capabilities for us.

Thank you, Mr. Chairman.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

[The prepared statement of Mr. Raub follows:]

Testimony
Before the Committee on Government Reform
Subcommittee on Technology and Procurement Policy
United States House of Representatives

Coordinated Information Sharing and Knowledge Management Issues for Key Federal Agencies in the Wake of the Terrorism Attacks on America - The Role of HHS's Office of Public Health Preparedness

Statement of
William F. Raub, Ph.D.
Deputy Director,
Office of Public Health Preparedness
Department of Health and Human Services

For Release on Delivery
Expected 10:00AM
Friday, June 7, 2002

Good morning, Mr. Chairman and members of the Subcommittee. I am William F. Raub, Deputy Director of the Office of Public Health Preparedness, Department of Health and Human Services (HHS). I welcome this opportunity to apprise the Subcommittee about HHS activities related to coordinated information sharing and knowledge management in the wake of the terrorism attacks on America. I will begin by describing the mission of the HHS Office of Public Health Preparedness and then address each of the topics posed in your letter of May 23 to Secretary Thompson.

THE OFFICE OF PUBLIC HEALTH PREPAREDNESS

In the wake of the terrorist attacks in September and October, 2001, Secretary Thompson acted to strengthen HHS anti-terrorism programs by creating the Office of Public Health Preparedness (OPHP) within the Office of the Secretary. Up to that time, HHS had conducted its anti-terrorism efforts through a highly decentralized organizational structure. The mission of OPHP is to introduce and sustain a "One-Department" approach to developing preparedness and response capabilities related to bioterrorism and other public health emergencies. The HHS program currently focuses on a) enhancement of state and local preparedness by strengthening the relevant capabilities of health departments and hospitals across the nation; b) development and maintenance of critical federal government response assets (such as the National Pharmaceutical Stockpile and the National Disaster Medical System); c) research and development toward new vaccines, diagnostics, and drugs related to the pathogenic organisms mostly likely to be used in a terrorist attack on the U. S. homeland; d) protection of the food supply from accidental or deliberate contamination with potentially life-threatening agents; and

e) liaison with key organizations outside HHS (such as the White House Office of Homeland Security and the academic and industrial communities). Led by OPHP, the HHS program features the coordinated activities of the Centers of Disease Control and Prevention, the Office of Emergency Preparedness, the Health Resources and Services Administration, the National Institutes of Health, and the Food and Drug Administration.

TOPICS FOR WHICH THE SUBCOMMITTEE REQUESTED COMMENTS

The Chairman's letter of May 23 to Secretary Thompson listed four topics to be addressed during this hearing. The remainder of this statement comprises HHS' comments on those topics.

1. your agency's assessment of the barriers, if any, that exist to achieving the Homeland Security Initiative of the President

Insofar a national preparedness for bioterrorism and other public health emergencies is concerned, HHS recognizes that it faces formidable challenges – many of them manifesting extraordinary complexity and in some cases viewed heretofore as intractable. Nevertheless, HHS does not believe that it faces any intrinsically insurmountable barriers in helping to achieve the Homeland Security Initiative of the President. In saying this, we do not presume that we can anticipate every bioterrorism scenario – especially scenarios conceived or executed by those who have no compunction against killing innocent people while committing a suicidal act. On the contrary, we presume that we will be tested by challenges not precisely foreseen or perhaps not even foreseeable. But we approach our task with confidence that a strong, sustained, and closely coordinated effort by the American public health, medical, scientific, and technological

communities can and will provide our nation with the basic capabilities it needs to respond to the myriad threats posed by terrorists intent upon using biological agents to inflict mass casualties and societal instability.

As an example of the challenges HHS faces, consider those capabilities that would be most in need if a bioterrorism event were to occur tomorrow:

> The local public health department should have the capability to receive and evaluate urgent disease reports electronically on an around-the-clock basis and, as necessary, invoke the aid of the state health department and, through it, the disease surveillance and epidemiological capabilities of the Centers for Disease Control and Prevention (CDC), including the resources of the HHS-led Laboratory Response Network.
>
> The local health department also should have the capability to receive and manage material from the National Pharmaceutical Stockpile if local supplies of pharmaceuticals and other medical materiel are likely to be exhausted and to carry out mass administration of drugs or vaccines should such intervention be necessary to treat the victims or to stem the advance of a terrorist-induced epidemic of communicable disease.
>
> At the same time, hospitals and other elements of the health care system should have well-rehearsed protocols for infection control – including the use of isolation rooms and other methods to prevent the spread of contagious disease and be able on short notice to

expand capacity (people, facilities, and equipment) to deal with the surge in demand for health care that the mass casualties following a terrorism event could engender.

Further, if patient care demands threaten to overwhelm local resources, the local health care system should be prepared to call upon and accommodate the resources of the HHS-led National Disaster Medical System and other assets designated for mobilization under the Federal Response Plan.

And, through it all, community leaders should be able to ensure that the public receives accurate and up-to-date information regarding the nature of the crisis, the efforts underway to address it and its consequences, and the actions that citizens should take to ensure their own health and safety.

All of these capabilities are attainable, but heretofore the requisite efforts have exceeded the resources available. Thus, as indicated by a survey conducted within the last year by the Department of Justice in collaboration with the CDC and as confirmed by recent HHS reviews of state-developed workplans to enhance public health and hospital preparedness, few local public health systems now possess any of these capabilities in full; and most local public health departments need to make substantial improvements in every area.

HHS is working aggressively to help states and local governments effect the necessary improvements; and our state and local partners are responding enthusiastically. The

appropriations act for Fiscal Year 2002 includes just over $1 billion to enhance the preparedness of health departments and hospitals; and the President's budget request for Fiscal Year 2003 includes just over $1.5 billion to continue and expand this initiative. Further, both the current appropriations bill and the President's request for next year include substantial resources for the continued development and maintenance of complementary federal government assets – principally the infectious disease surveillance and epidemiological response capabilities at the CDC in Atlanta, the National Pharmaceutical Stockpile, and the National Disaster Medical System. While much work remains to be done before preparedness approaches the level we seek, considerable progress has occurred since last year, and the prospects seem bright for continued rapid improvement.

2. its assessment of government efforts to improve intra- and inter-agency information sharing

One of the major tasks for the HHS Office of Public Health Preparedness (OPHP) is to improve sharing of information among HHS agencies. HHS believes that its internal communications about anti-terrorism activities are strong but looks to the OPHP to improve them. New procedures associated with the establishment of terrorism-related spending priorities across the Department and the allocation of funds within the Public Health and Social Services Emergency Fund are serving this objective.

With respect to inter-agency activities, HHS coordinates its anti-terrorism activities closely and productively with the Office of Homeland Security (OHS). Secretary Thompson and other senior staff are in frequent contact with OHS Director Ridge regarding multi-Department

activities as well as specific HHS initiatives. For example, earlier this year, HHS briefed OHS about the impending HHS action to award more than $1 billion via cooperative agreements to all 50 States, 4 selected major municipalities (the District of Columbia, Los Angeles County, Chicago, and New York City), and the 5 U.S. territories to foster state and local preparedness for bioterrorism, other outbreaks of infectious disease, and other public health threats and emergencies. In addition, HHS Deputy Secretary Claude Allen participates routinely as a member of the Office of Homeland Security's Deputies Committee, which is the primary senior-level mechanism for inter-Departmental communication and coordination; and several other HHS senior staff participate in more specialized inter-Departmental groups, called Policy Coordinating Committees, that support the work of the Deputies Committee.

3. <u>its review of government's capabilities, limitations, and gaps in information technology to fight terrorism</u>

Information technology is central to HHS anti-terrorism activities. Our efforts to enhance infectious disease surveillance and other aspects of public health preparedness at local, state, and national levels depend heavily upon making judicious use of the Internet and other forms of electronic communication, computer-manipulable data bases, and statistical and other analytical software.

The centerpiece of HHS information technology applications related to public health preparedness is the Health Alert Network (HAN). As its name suggests, HAN is being developed with a view to enabling rapid electronic notifications about urgent health matters to

local public health departments and other key entities and individuals throughout the public health system. Under emergency circumstances, such as would be the case in the wake of a bioterrorism incident, the capability for public health officials to communicate instantaneously with one another and with others who need the latest accurate health information could be the difference between prompt mitigation of an epidemic and a public health catastrophe. Moreover, as the Network expands to meet our goal of covering local health departments that collectively serve at least 90% of the U.S. population, HAN is expected to furnish an electronic medium for many routine health communications and for educational activities. In particular, HAN could facilitate health education and training by enabling access to collections of specialized material such as diagnostic protocols and archives of micrographs of pathogenic organisms and by facilitating webcast teleconferencing and distance learning.

Complementing HAN are HHS efforts, led by the Center for Disease Control and Prevention, to develop and promulgate information technology standards for the public health community. The evolving standards cover hardware, operating systems, and applications. The primary objective is to help public health departments and others make effective and economical use of state-of-the-art information technology while achieving the high degree of interoperability that is essential if information is to flow readily within the public health system and between it and its collaborators such as community leaders, law enforcement agencies, public safety agencies, and the news media. In general, the emerging needs of the public health community for information technology are met readily by products and services routinely available; and the progressive improvements in these products and services are likely to outstrip the demands of the public

health community, at least for the next several years. The issue at present is not the limitations of current information technology but rather the ability of the public health community to choose wisely from among the wealth of choices that information science and technology offer it.

4. its comments, if any, on proposals to assist in the assessment of homeland security technology proposals

The private sector seems able and eager to help advance the HHS priorities. In the vaccine development area, representatives of the pharmaceutical industry have stressed that, to the extent that the federal government can prescribe its vaccine requirements and assure up front that the requisite funds will be available, the industry will meet the challenge. Thanks to the President's leadership and Congressional appropriations for Fiscal Year 2002, this currently is the case for the HHS effort to develop and acquire a sufficient quantity of a new smallpox vaccine to protect the entire U.S. population. HHS is hopeful for a similar scenario to be realized for a new anthrax vaccine, if the advanced development work during Fiscal Year 2002 is successful and if the President's request for $250 million for anthrax vaccine acquisition in Fiscal Year 2003 is approved by the Congress.

The private sector also is active in other pertinent areas. Development of new or improved multi-spectrum antibiotics is a high priority for the pharmaceutical industry. Many companies, large and small, are attempting to develop rapid diagnostic tests and devices for microbes likely to be used by terrorists. Still other companies, large and small, are pursuing new information

technologies and systems that may prove valuable for infectious disease surveillance and hospital response to mass casualty events.

HHS-funded research, primarily through the National Institutes of Health, is generating new knowledge that will enable the academic and industrial communities to develop new or improved anti-bioterrorism capabilities. Foremost among these research efforts is the rapidly expanding array of studies in microbial genomics. By sequencing the genomes of the various species and strains of the microbes most likely to be used by terrorists, and by performing computer-based comparative analysis of these genomes and their protein products, scientists hope to achieve fresh leads for the development of new or improved diagnostic devices, drugs, and vaccines. Moreover, such research (often included under headings such as comparative genomics, proteomics, and bioinformatics) also may yield new insights into the genetic basis for why different species of microbes (or even different strains of the same species) differ from one another, often substantially, in either their virulence or their susceptibility to antibiotics. In addition to spurring advanced development and commercialization of new diagnostic, therapeutic, and prophylactic products, this research also could enable more informed preventative and therapeutic strategies using existing products.

The food industry has engaged actively in strengthening security measures at food processing facilities, restaurants, and retail establishments through establishment of the Alliance for Food Security. In January of this year, the Food and Drug Administration published food security guidance for the domestic and imported food industries. The guidance provides a checklist of

potential preventive measures that these firms can take to reduce the risk that food under their control will be subject to tampering, criminal, or terrorist action.

For the purpose of identifying opportunities for public private partnerships, Secretary Thompson established the *Council on Private Sector Initiatives to Improve the Security, Safety, and Quality of Health Care*. The Council has four objectives:

- Provide the private sector with a single HHS point of contact for innovative ideas that cut across agencies and departments;
- Coordinate requests from individuals and firms seeking HHS review of their ideas;
- Ensure that HHS responds systematically and consistently to these requests; and
- Report to the Secretary on the Council's activities and actions resulting from them.

In keeping with its charge, the Council meets regularly to triage requests from individuals and firms seeking review of their ideas or products and to forward information to the appropriate agencies and offices.

HHS recognizes that much remains to be done to ensure that our nation is adequately prepared for bioterrorism, other outbreaks of infectious disease, and other public health threats and emergencies. HHS believes that its fundamental anti-terrorism strategy is sound and notes that it is already yielding solid incremental enhancements in local, state, and national capabilities to ensure homeland security.

That concludes my written statement. I would be happy to answer any questions from the Subcommittee.

Mr. TOM DAVIS OF VIRGINIA. Mr. Jordan.

Mr. JORDAN. Good morning, Mr. Chairman and members of the subcommittee. My name is Bob Jordan, and I serve as the head of the FBI's Information Sharing Task Force. I welcome this opportunity to meet with you today about the status of the FBI's information-sharing initiatives within the Bureau and with other government agencies for homeland defense purposes.

The FBI is an organization in change. Not only are we structurally different, but in very fundamental ways Director Mueller has revamped our approaches to counterterrorism and prevention. Since September 11th, we have seen massive shifts in our resource deployments. Our missions and priorities are being redefined to better reflect the post September 11th realities. As an agency we are committed to devoting whatever resources are necessary to meet our prevention mission and continue to sustain a dramatically enhanced worldwide counterterrorism effort. A substantial component of this approach is information sharing not only at the Federal level, but also within the entire law enforcement and intelligence communities. Over the last several years, much has improved, but this seemingly simple issue is actually a complex myriad of technology, legal policy and cultural issues.

Since the tragic events of September 11th, this single issue critical to public safety is receiving the sustained high-level attention necessary to ensure that everything that can be done is being done. In that regard, I'm happy to say that the spirit of collaboration and willingness to exchange data has never been stronger or more pronounced than it is today. Many of the legal and policy impediments that kept us from more fully exchanging information in the past have been or are now being changed.

The Patriot Act has greatly improved our ability to exchange data within the Intelligence Community and across law enforcement. In addition, the Attorney General's recent directive to increase coordination and sharing of information between DOJ, FBI, INS, Marshals Service and the Foreign Terrorist Tracking Task Force on terrorist matters and to establish secure means of working with State and local officials are major milestones in improving our information-sharing and collaboration efforts.

Equally important, the difficult technology challenges we all face are on top of everyone's list. This is especially so at the FBI. Under Director Mueller's leadership, the FBI on every front is hard at work carrying out the Attorney General's information-sharing directive.

Within the FBI, Director Mueller has taken on the challenge of improving information sharing and has directed FBI executive management to develop every means necessary to share as much information as possible with other agencies, as well as State and local law enforcement. Years of experience have demonstrated that joint terrorism task forces, JTTFs, have proven to be one of the most effective methods of unifying Federal, State and local law enforcement efforts to prevent and investigate terrorist activity. There are currently 47 JTTFs. We are working expeditiously to establish JTTFs in each of our 56 field offices. As recently as 1996, there were only 11 of these task forces.

The creation of JTTFs this year is resulting in an expanded level of interaction and cooperation between the FBI and our Federal, State and local counterparts. Among the full-time participants in JTTFs are INS, Marshals Service, Secret Service, the FAA, Customs, ATF, State Department, Postal Inspection, IRS, Department of Defense and U.S. Park Police. State and local agencies are heavily represented. Information is also being shared with the Transportation Security Administration and the U.S. Coast Guard.

The FBI has a long tradition of exchanging unclassified information with Federal, State and local law enforcement agencies on warrants, fingerprints, forensic information and watch lists. The last few years have seen dramatic increases in the exchange of specific case-related information, due in large part to the proliferation of JTTFs. Now we are improving our sharing of classified information again through such mechanisms as the JTTFs.

Director Mueller has undertaken several initiatives that directly enhance the FBI's information-sharing capacities. All of these efforts are designed around the recognition that post-September 11th, the FBI has adopted both a new focus and priorities that recognize that a substantial investment is being made in prevention. A few examples include Director Mueller has named Lewis Kay, who is currently chief of the High Point, North Carolina, Police, to be the FBI's Assistant Director for Law Enforcement Coordination. Our Office of Intelligence is now part of the FBI's organizational structure. The FBI has undertaken major recruiting and hiring initiatives to bring into the FBI private sector IT experts who can greatly assist our sizable IT projects. We have a new Records Management Division that has been established, and the FBI is detailing personnel to other agencies and vice versa to ensure that information is shared and understood within our agencies. These efforts are particularly critical to programs like our National Infrastructure Protection Center, the Counterterrorism Center at CIA and others.

Information security is a significant issue in these initiatives. We must balance our desire to share information as freely as possible with the need for the security of information.

I'm going to go to the last part of my comments here. The FBI's future ability to deter and prevent crimes requires the use of current and relevant IT. We have several critical initiatives under way to upgrade the FBI's IT infrastructure and investigative applications. Funding for these programs is essential to provide our investigators and analysts with IT resources and tools.

That concludes my prepared remarks, Mr. Chairman. I'll be happy to answer any questions.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

[The prepared statement of Mr. Jordan follows:]

Statement for the Record of
Robert J. Jordan
Federal Bureau of Investigation
on **Information Sharing Initiatives** Before the
United States House of Representatives Subcommittee on
Technology and Procurement Policy
Washington, D.C.
June 7, 2002

Good morning, Mr. Chairman and Members of the Subcommittee. My name is Bob Jordan and I serve as the head of the FBI's Information Sharing Task Force. I welcome this opportunity to meet with you today about the status of the FBI's information sharing initiatives within the Bureau and with other government agencies for homeland defense purposes.

The FBI is an organization in change. Not only are we structurally different but, in very fundamental ways, Director Mueller has revamped our approaches to counterterrorism and prevention. Since 9/11, we have seen massive shifts in our resource deployments. Our missions and priorities are being redefined to better reflect the post-9/11 realities. As an agency, we are committed to devoting whatever resources are necessary to meet our prevention mission and continue to sustain a dramatically enhanced worldwide counterterrorism effort. A substantial component of this approach is information sharing, not only at the federal level but also within the entire law enforcement and intelligence communities. Over the last several years, much has improved but this seemingly simple issue is actually a

complex myriad of technology, legal, policy and cultural issues. Since the tragic events of 9/11, this single issue, which is critical to public safety, is receiving the sustained, high-level attention necessary to ensure everything that can be done on every facet of the issue is being done.

In that regard, I am happy to say that the spirit of collaboration and willingness to exchange data has never been stronger or more pronounced than it is today. Many of the legal and policy impediments that kept us from more fully exchanging information in the past have been or are now being changed. The USA Patriot Act (Pub. L. 107-56) has greatly improved our ability to exchange data with the intelligence community and across law enforcement. In addition, the Attorney General's recent directive to increase the coordination and sharing of information between the DOJ, the FBI, the INS, the USMS, and the Foreign Terrorist Tracking Task Force (FTTTF) on terrorist matters and to establish secure means of working with state and local officials are major milestones in improving our information sharing and collaboration efforts. Equally important, the difficult technology challenges we all face are on the top of everyone's priority list. This is especially so at the FBI. Under Director Mueller's leadership, the FBI, on every front, is hard at work carrying out the Attorney General's information-sharing directive.

Joint Terrorism Task Forces

Within the FBI, Director Mueller has personally taken on the challenge of improving information sharing and has directed FBI executive management to develop every means necessary to share as much information as possible with other agencies as well as with state and local law enforcement. Years of experience have demonstrated that Joint Terrorism Task Forces, JTTFs, have proven to be one of the most effective methods of unifying federal, state and local law enforcement efforts to prevent and investigate terrorist activity by ensuring that all levels of law enforcement are fully benefitting from the information possessed by each.

There are currently 47 JTTFs. We are working expeditiously to establish JTTFs in each of the FBI's 56 field offices. In 1996, there were only 11 of these task forces. The creation of 21 new JTTFs this year is resulting in an expanded level of interaction and cooperation between FBI Special Agents and their Federal, state and local counterparts, as well as an enhanced flow of information between the participating law enforcement agencies.

Among the full-time federal participants on JTTFs are the INS, the Marshal's Service, the Secret Service, the FAA, the Customs Service, the ATF, the State Department, the Postal Inspection Service, the IRS, Department of Defense and the

U.S. Park Police. State and local agencies are heavily represented. Information is also being shared with the Transportation Security Administration and the U.S. Coast Guard.

In addition to the JTTFs, the Regional Terrorism Task Force (RTTF) initiative serves as a viable means of accomplishing the benefits associated with information sharing without establishing a full-time JTTF. FBI Special Agents assigned to counterterrorism matters meet with their Federal, state and local counterparts in designated alternating locations on a semi-annual basis for common training, discussion of investigations, and to share and discuss intelligence. The design of this non-traditional terrorism task force provides the necessary mechanism and structure to direct counterterrorism resources toward localized terrorism problems within the United States. There are currently six RTTFs: the Inland Northwest, the South Central, the Southeastern, the Northeast Border, the Deep South and the Southwest RTTFs.

The FBI has a long tradition of exchanging unclassified information with Federal, State and local law enforcement agencies on wants and warrants, fingerprint identification, forensic information and watch lists. The last few years have seen dramatic increases in the exchange of specific case-related information due, in large part, to the proliferation

of task forces. Now, we are improving our sharing of classified information again through such mechanisms as the JTTFs.

FBI Initiatives

We have recently developed an FBI-wide and DOJ-wide capability to electronically share case information. Our Integrated Intelligence Information Application (IIIA) database is another example of major improvements in information sharing. It uses information derived from many different sources including the Department of State and INS. IIIA provides analytical support for Counterintelligence and Counterterrorism programs. It is a real-time collection system that houses over 33 million records. In the aftermath of 9/11 and PENTTBOM, IIIA has been asked to provide electronic search support to units within the FBI as well as to the critical FTTTF. To satisfy these requests, multiple programs have been written to standardize incoming data arriving in differing formats and to package the responses to accommodate the requesters' needs.

Director Mueller has undertaken several other initiatives that either directly or indirectly enhance the FBI's information sharing capacity. All of these efforts are designed around the recognition that post-9/11, the FBI has

adopted both a new focus and priorities that recognize the substantial investment being made in prevention. A few examples include:

Director Mueller has named Louis Quijas, currently Chief of Police of High Point, North Carolina, to be FBI Assistant Director for Law Enforcement Coordination. Chief Quijas has as his single mission fully exploiting state and local law enforcement support through enhanced information sharing and ensuring that state and local law enforcement have a strong voice within the FBI as we work on terrorism, prevention and major investigations.

An Office of Intelligence is now part of the FBI's organizational structure. This office has as part of its mission not only to ensure the vigorous and fluid flow of information within the FBI but also to ensure that intelligence goes elsewhere within the law enforcement and intelligence communities in every instance when it is appropriate to do so.

The FBI has undertaken a major recruiting and hiring initiative to bring into the FBI private sector IT experts who can greatly assist in designing and managing the sizable IT projects recently funded by Congress. These projects, such as Trilogy, are vital to any robust information sharing program.

A Records Management Division has been established, headed by an outside records expert, to put in place the "information management" policies and mechanisms critical to effective sharing programs.

The FBI is detailing personnel to other agencies, and vice versa, to ensure that information both is both shared and understood within both agencies. These efforts are critical to programs like the National Infrastructure Protection Center (NIPC), the Counterterrorism Center at CIA, and others.

Information Security

One equity we must balance with our desire to share information as freely as possible is the need for the security of information. As recently detailed in Judge William Webster's report, we must keep in mind that we are keepers of information that is highly classified and controlled by "need to know" principles. Access to highly confidential information will be in accordance with the FBI's broad, new security policies. Access control mechanisms, such as identification and authentication will provide accountability for those individuals having a need to know restricted information. In addition, audits of this access will be routinely conducted. The lives of agents, informants

and innocent victims often rest upon the safe keeping of their information. The need for information security must be balanced by the driving need of the criminal investigator to be able to follow any and all avenues in an investigation.

The Webster Commission report accurately points out that the FBI's information technology (IT) recapitalization effort, Trilogy, includes funding for only the foundational elements of Information Assurance (IA). At rollout, Trilogy will provide more security than the FBI's current IT backbone. The goal, however, is to develop the IA Program to be on par with other world-class information systems security efforts. Significant coordination has taken place between the Trilogy Program and personnel assigned to the IA Program to ensure that the Trilogy security architecture will support the utilization of the future IA technologies we plan to employ. So, while Trilogy and related applications will give the FBI a vastly increased capability to use, analyze, exploit and share information collected in investigations, it will be designed and deployed in a manner that addresses the shortcomings apparent in the Hanssen matter.

Challenges

Today, information sharing is technologically feasible. Advances in information technology have made it possible to link the information systems of agencies that are operating

with different hardware and software. The improvements in information sharing that are at the heart of these initiatives, however, require that agencies participating in integration initiatives come together and agree upon a governance structure to manage decision-making in an integrated environment. Federal, State and Local law enforcement must address the considerable challenge of developing a formalized organizational framework within which participating agencies will share responsibility for making and executing overarching decisions on such issues as budgeting, hardware and software purchases, and the development of policies, procedures, and protocols that effect the operational integrity of the information sharing system. Our systems were originally designed to comply with a complex set of regulations restricting what can and cannot be shared amongst Federal, State and local agencies. We are committed to redesigning our systems and making whatever changes are necessary to ensure the effective and efficient exchange of information within the law enforcement community.

At the same time, we still need to further improve our ability to share information between our own applications and our own multitude of databases. Our Data Warehousing project will provide us with the capability to finally combine information from all our applications into a coherent whole and provide advanced data mining, analytical and

visualization tools. We are also working with the Office of Homeland Security on improving horizontal information sharing, developing common data standards, and improving collaboration capabilities.

The FBI's future ability to deter and prevent crimes requires the use of current and relevant IT. We have several critical initiatives underway to upgrade the FBI IT infrastructure and investigative applications such as the Trilogy Program; Data Warehousing & Data Mining; our Collaboration Initiative; and our Information Assurance initiative. Funding these programs is essential to provide our investigators and analysts with improved IT resources and tools to support criminal and national security investigations, enabling improved and more expeditious data sharing and active collaboration.

That concludes my prepared remarks, Mr. Chairman. I will be happy to respond to any questions you may have.

Mr. TOM DAVIS OF VIRGINIA. The subcommittee is pleased to have Representative Jane Harman from California sit in with us today, and I would ask unanimous consent to allow her to give a statement and participate in a hearing.

Hearing no objection, the gentlelady from California is recognized.

STATEMENT OF HON. JANE HARMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Ms. HARMAN. Thank you, Mr. Chairman, and Mr. Turner and members of the subcommittee. I'm delighted to be here, and I want to commend you on your perfect timing. So far as I can tell, this is the first hearing on a critical piece of the homeland security subject to be held following the President's dramatic, bold and courageous announcement of last night. Good work.

Mr. TOM DAVIS OF VIRGINIA. Thank you. We saw it coming.

Ms. HARMAN. I also want to say about you, Mr. Chairman, that we go way back. You know, the Smith-Amherst Axis is pretty powerful, but also we represent communities that have some of the fastest growing tech communities on the planet. In my case, my district in southern California has a very large aerospace base. I know yours does, too, but I think mine is bigger. No competition here. It's diversified, and a lot of the aerospace companies—in fact, we're going to hear from one later—have large IT businesses.

I would like to, if you don't mind, welcome one of my constituents who will testify on your second panel, Ron Sugar, who is the president and chief executive officer of a tiny little firm called Northrop Grumman, and that is an example of the diversification that I'm talking about.

I just wanted to make a few points. First, I am late and I apologize, because I was one of 10 Members of the House and Senate who was at the White House meeting with the President and Governor Ridge today to talk about next steps in the turf and other battles related to unfolding this new Department of Homeland Security. I thought it was a very constructive meeting, and I think that this topic that you are exploring today is absolutely central to an effective homeland security effort, and the effort to put more functions into one department is related, does have a relationship to the need to improve information sharing.

It's not that it's a magic answer. It's not that all the information sharing we need will happen inside the borders of the Department of Homeland Security. Obviously other departments are represented here, and they need to share, too. But it is that this is a critical piece of the reason why we need to do this Department of Homeland Security.

Let me just touch on three issues, and I'll just summarize my testimony. First is procurement. As I mentioned, I represent a huge IT base in the South Bay of Los Angeles. Lots of the firms there, both aerospace and nonaerospace, have developed critical technologies that we need for a successful homeland security effort, and they don't really know how to access the Federal Government, how to learn about what's needed, and how to conform whatever products they make and services they render to what's needed. And we have tried hard to find places in the Federal Government that

should be the right places to access, like the Technical Support Working Group, TSWG, at DOD, and that effort, for example, has a very capable leader, John Reingrubber, who came to Los Angeles to meet with members of these firms. But his group has been overwhelmed by requests, and there's no possible way that one place in the Defense Department can handle all of the needs.

I want to commend you for H.R. 4629, of which I am a cosponsor, and I know that legislation would create a body responsible for receiving and routing technology proposals to the right government agencies. I think that's a good start. I think we need that regardless of the need to create the Department of Homeland Security. But as you know, none of this is easy. The new organization would have many bureaucratic challenges, need to recruit staff and so forth. Nonetheless, I think it is an important thing that we consider your legislation, and I strongly support it.

The second issue is data integration. I think, again, both the government and private witnesses understand this. Example: The Intelligence Community needs to be able to access information in any agency and to search multiple data bases for common themes. Looking backward in hindsight is always better. Wouldn't it have been great if we could punch in "flight training" and "Moussaoui," just two random ideas, and have multiple hits in FBI reports, the CIA watch list, FAA rosters?

When you talk about connecting the dots, you talk about data integration, and we need work on our data integration processes, and in that regard I think this new analytical capability that the President is proposing for the Office of Homeland Security is a terrific idea. Even this morning the press was asking about, well, what about the CIA and the FBI and all of the other agencies? Isn't this duplication? Or shouldn't they be pulled into all of this? And my answer is, yes and no. Yes, it's duplication. Another set of eyes, an analytical capability focused on homeland security to make sure that we do connect the dots and that our threat condition warnings are as accurate and informational as possible is a great idea. The no is that, no, we don't need to move the FBI and the CIA someplace else. They have important functions which they should still continue to perform. But at any rate, data integration is a big deal.

Final comment is on public-private partnerships, and, again, Mr. Chairman, I want to commend you and Mr. Turner and the others for all of the work that you do. It was true sometime back that we had and could afford separate industrial bases, a defense industrial base and a commercial industrial base. We invested huge amounts of money in government R&D. A lot of the most critical technologies that we employ across the board now, like GPS, were invented by the government, and with all affection for Al Gore, the Internet was invented by the government. But nonetheless, it is now true that we can no longer afford separate industrial bases. We need one industrial base with both commercial and government application, and most of that base does presently reside and should reside in the private sector, and that is why it is so critically important that we leverage private sector technologies for government uses.

In many cases the government can serve as an information clearinghouse, sharing best practices and reports. The Cyber Security

Information Act, H.R. 2435, is a good example of this. But it is also true that the government has to find better mechanisms to leverage technologies. The future of homeland security will depend on whether we do this well, and I have no doubt that our second panel will talk about how best to do that.

I just want to commend you one more time, and it's the last time I'm planning to flatter you this week, no matter what, for your enormous leadership and your partnership on a bipartisan basis with those of us in this House who have focused on this issue for a long time. I think that this is the future, and I'm very happy that you let me participate in your hearing. Thank you.

Mr. TOM DAVIS OF VIRGINIA. Well, thank you, and you keep talking that way, you can come to any of our hearings.

[The prepared statement of Hon. Jane Harmon follows:]

Testimony of the Honorable Jane Harman
"Meeting the Homeland Security Mission:
Assessing Barriers to and Technology Solutions for Robust Information Sharing"
June 7, 2002

Thank you, Chairman Davis, Congressman Turner, and Members of the Subcommittee for the opportunity to join you today at this hearing on homeland security structure and practice.

The President's announcement yesterday on a proposed Department of Homeland Security should remove some of the organizational barriers that have prevented a coordinated and efficient approach to homeland security. I fully support consolidating appropriate homeland security functions into one Department with the focus and authority to improve our capability to prevent and respond to terrorist attacks.

My remarks today focus on three issues: federal technology procurement, data integration, and a public-private partnership for homeland security. All three are less efficient and effective than possible for the same two reasons: culture and technology.

Procurement. The technologies needed for effective national homeland security largely reside in the private sector. The federal government needs to improve its information technology, detection and screening equipment, medical treatments for biological and chemical weapons, software for situational awareness at the first responder level, and many others.

These technologies are increasingly developed in the private sector. I am proud to represent many of them; Southern California is the aerospace capital of the world, and a leader in IT. I've heard from these companies first hand their frustration; they produce cutting-edge technologies necessary for effective counterterrorism, and can't find an entré to the Executive Branch. I understand that the Office and Homeland Security and countless federal agencies are also deluged with unsolicited proposals that they are unable to appropriately handle.

Last Fall, the Department of Defense issued a broad agency announcements for counterterrorism technologies. The response overwhelmed the Technical Support Working Group (TSWG), the interagency group between Defense and State charged with administering the funding allotted. The TSWG is filled with a talented, hard-working, and knowledgeable staff, and its head, John Reingruber, deserves high praise. But this group is not set up to handle this volume of responses.

H.R. 4629, of which I am a co-sponsor, would create a body responsible for receiving and routing technology proposals to the right government agency. This organization would greatly simplify the process for technology companies, which focus on innovation, not understanding complex government bureaucracies. I fully support this goal.

However, this new organization would have many bureaucratic challenges. It would need to recruit staff with the technical expertise to understand and preliminarily assess proposals, but still keep track of the complex web of government procurement, grant, and research activities. The

organization will also operate as a conduit without holding the procurement funds at its disposal, thus robbing it of the most powerful leverage in government.

Perhaps the proposed Department of Homeland Security will assume some of these responsibilities, but these difficulties must be addressed if the best technologies are to be implemented in the war against terrorism.

Data Integration. A second technical need for federal homeland security is the ability to access and efficiently process mountains of data, regardless of where they reside in the bureaucracy. Each intelligence agency collects and analyzes its own intelligence, which may take the form of electronic files, written documents, pictures, voice recordings, imagery, or others.

The intelligence community needs to be able to access information in any agency, and to search multiple databases for common themes. A search on flight training and Moussaoui, for example, should result in "hits" in FBI reports, CIA watch lists, and FAA rosters. Such capability exists openly, and free of charge, on the Internet today. The same must be true of those charged with protecting out homeland.

The technical challenge of sharing these formats of data have, to date, exceeded the capabilities of the intelligence agencies. But the technical challenge is less difficult to overcome than the cultural barrier.

The intelligence agencies, including the CIA, NSA, and FBI, hold their intelligence close. They do their work in secret, as publicity undermines their ability to infiltrate organizations and collect tips. But holding information within one agency prevents the community from putting together all the facts that might indicate a terrorist plot. Holding information within the federal bureaucracy also robs the women and men on the front lines—our nation's first responders—of the valuable clues they need to prevent attacks.

Public-Private Partnership. Finally, the U.S. government, at the federal, state, and local level, must work more closely with private entities to ensure homeland security. The government is responsible for providing security for citizens, but the private sector shares the responsibility to protect against attack or disruption. And it controls many of the assets needed to do so.

The private sector owns and operates 90% of the critical infrastructure across the country, including vital computer networks. We have yet to establish who is exactly responsible for what in protecting these systems from attack, but clearly it is in the public interest to ensure these assets are secure.

In many cases, the federal government can serve as an information clearinghouse, sharing best practices and reports on expected attacks to enhance prevention. The Cyber Security Information Act, H.R. 2435, is a good example of this service.

At other times, the government can influence companies' actions through regulation, tax incentives, and specific mandates. But legislation is a blunt instrument, and Congress will not be able to move at the speed necessary to keep up the digital demands of homeland security.

Instead, public and private sector experts must join together in making homeland security decisions and setting policy. Government agencies must update their business practices and reduce bureaucracy to be accessible to companies. And information typically shared internally on threats and proposed responses must increasingly be shared with companies.

I thank this Subcommittee for its work in these three issues, and look forward to working with you in moving legislation and improving the business practices of government to work with the private sector.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much, Ms. Harman. Let me just say your leadership on a number of these issues has been very, very important to our coalition in the House, and I'll continue to value your advice, expertise and leadership as we move through this. So thank you very much for being here.

I'm going to start the questioning with Mrs. Davis. We'll do 5 minutes around the first time. Then we'll move to Mr. Turner and back and forth.

Mrs. JO ANN DAVIS OF VIRGINIA. Thank you, Mr. Chairman, and thank you, gentlemen, for being here to testify this morning.

Sort of in conjunction with what my colleague from California said, I believe she stated that she has a lot of private IT companies that don't know how to access what the Federal Government needs, and in that regard are your agencies or your departments, are they inundated with private sector security technology proposals, No. 1? And two, do you believe you have the staff qualified to sort out what would be useful and what would not be useful? And do you have the procedures in place to accomplish your goals? Any of you? Do you want to start, Mr. Yim?

Mr. YIM. Yes. I think one of the concerns that the GAO has is how will the variety of technical solutions be evaluated. I think a lot of agencies would be deluged with proposals, and do we have effective mechanisms to assess the viability efficacies of that? The GAO has undertaken a pilot project working with the National Academy of Sciences to evaluate, for example, emerging biometric techniques. So even though we may not have the expertise in-house, although we have substantial expertise in-house, we wish to augment that with the significant scientific base provided by the National Academy, and that is one model I think that we could pursue.

Mr. TOM DAVIS OF VIRGINIA. Anyone else?

Mr. FORMAN. I'd like to speak a little bit about the framework that was laid out in the Clinger-Cohen Act. I really don't think the problem at this point is with the procurement work force in terms of staffing requirements. I think the problem, as was indicated, is in the requirements definition.

You know, the issue of how we bring technology in the government has been going on for several decades and is—just as the Congresswoman stated, a shift from the government being at the leading edge of technology to being significantly behind commercial industry technology led to several rounds of legislation. Most of that legislation said we're trying to choose technology through the procurement process, but we don't have the requirements well enough defined to make any use of the technology. So we tend to buy it as commercial best practices, and we hear terms like "governmentizing the technology." If we risked that with some of this leading-edge technology, we're not going to get the benefit out of it. We're going to expend too much out of it.

So the issue is if we've got 50 proposals for different aspects of security technology, can the government today become the systems integrator? Do we want it to become a systems integrator? Right now we don't have the talent, and we don't have the technical skills. I know this has been a subject of another hearing in another very fine piece of legislation from this subcommittee. We have to

focus on clearly understanding our requirements, and we also, I think, have to focus on getting good teamwork in industry.

You know, when a company goes out to buy security technology, it's not quite the same as they announce that they've been hit by some cybervandals, and then people start showing up. They generally look for a security architecture, a comprehensive solution approach. That's what we are trying to do in the Federal Government as well, and I think that may be tough to understand for a lot of industry, that the government works not by being our own integrator oftentimes. So when they come to—many companies that have just pieces of the technology puzzle come to talk to us, they expect us to know how to integrate it together and to buy the pieces. That's very difficult right now for the Federal Government.

Mr. BOHLINGER. I'd like to assure you that the three of us did not get together before we were making these comments, but—and not to sound like just reiterating——

Mrs. JO ANN DAVIS OF VIRGINIA. It's OK.

Mr. BOHLINGER. The issue is requirements. There's no question about it. We are significantly engaged in meeting with people from the private sector and have been going to their forums, talking with them individually, meeting with the senior people from these corporations, and there are many wonderful ideas out there, but can you imagine ideas just being thrown over the transom, all of which are good? How do you sort them out?

And what I said in my testimony I think I'd like to emphasize again is that we need to be able to tell the people in the private sector exactly what our needs are and allow them to——

Mrs. JO ANN DAVIS OF VIRGINIA. Let me interrupt you there, because my time is about running out. Where do you get what your needs are? Who gives them to you? All three of you have said requirements. Where do you get them from?

Mr. FORMAN. I—especially in this area of security, there are two areas. One is in the Government Information Security Reform Act requirements that were laid out. The baseline set of best practices identified by the National Institute for Standards and Technology gave us the ability to do a gap analysis. It's a very comprehensive gap analysis. That's led to a listing, a plan of actions and milestones, that in some agencies are 2 or 3 inches thick, and those are the requirements. So we're first year into the process, several months into the process. We now—the requirements are there, and we can make sense and go buy the technology.

Mr. BOHLINGER. If I might just continue for a second on the requirements issue, I think it's both on a macro and a micro scale. On the macro scale, it's something that has also been discussed here in talking about enterprise architectures. Federal agencies must have robust and thoroughly vetted enterprise architectures, and this is exactly how we are doing our business. On the micro area of requirements, it's as you go out with specific requests, and that might be a particular system having to do with something that just is local, it may be a nationwide system, but being able to clearly lay out in the request for information—and I'm a great proponent of that, of allowing corporations that come in and suggesting solutions to well-defined requirements, then allow you to go out with RFPs that people can apply their best technology to.

Mrs. JO ANN DAVIS OF VIRGINIA. Mr. Chairman, can they all have the time to answer?

Mr. TOM DAVIS OF VIRGINIA. Go ahead.

Mr. RAUB. I can just comment briefly. With respect to Health and Human Services, we won't claim perfection in our interface with the private sector, but we believe we're doing well and are getting better.

Secretary Thompson is taking two major structural steps that have helped us along. One is the creation of the office I represent, the Office of Public Health Preparedness, last November. He's given us a focal point within the Secretary's office for all $3 billion worth of it related to bioterrorism across our 11 agencies in the Department. And representatives of the technology community have not been bashful in seeking us out, nor have we in our interactions with them, either for activities of our own office or steering them to the Centers for Disease Control and Prevention, the National Institutes of Health, the drug administration or other elements of our Department.

Even before that, last summer the Secretary created his Council on Private Sector Initiatives. The idea was to bring together a team of representatives from every agency in the Department that would meet on a regular basis and be a one-stop shop for members of the community to bring ideas that might have some pertinence to programs of Health and Human Services. This is not limited to terrorism. It's much more broadly including the hospital sector. At a most recent meeting of that team, no fewer than nine company representatives were present describing their activities, how they might relate to Health and Human Services, and seeking some requirements and general guidance of how best to relate to the Department.

Mrs. JO ANN DAVIS OF VIRGINIA. Thank you.

Mr. Jordan.

Mr. JORDAN. As I mentioned in my direct testimony, the FBI has begun to hire outside IT experts who are helping us sift through the various suggestions made to us, and we are well along in that process. And we have an established process for interfacing with the private sector.

Ms. JO ANN DAVIS OF VIRGINIA. Thank you, Mr. Chairman.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

Mr. Turner.

Mr. TURNER. Thank you, Mr. Chairman.

Mr. Forman, talk to us a little bit about how far along we are in developing the enter prise architecture that is necessary for homeland security and how the new Homeland Security Department or office will function with regard to the work that, apparently, currently you are responsible for.

Mr. FORMAN. I can't at this point discuss any of the issues related to the President's announcement last night. It is just too early in the process. But as you point out, there are many issues that need to be addressed. So let me go through what issues you raise.

We are taking a two-tiered approach with respect to homeland security that there very clearly has to be progress made in homeland security lines of business, is the way we refer to them. A line of business could be disaster management preparedness. Within

that, people have to make architecture decisions. They have got to look at which agencies, which organizations within those agencies have what roles and responsibilities, and what performance results or outcomes those organizations are supposed to achieve. Within that, there is an awful lot of overlap, so we have to have some clear way to identify those. We call those business functions.

And so you could have, for example, within disaster management, emergency planning, and you would find out that there are many bureaus involved in that planning. You would also find out that there is a core business process, a way of doing disaster planning that cuts across those department—departments, and is probably replicated multiple times. They probably have redundant information systems. And the unfortunate thing about this is, when you pull in the focus of this, the citizen voice, the customer, if you will, which tends to be State and local emergency management officials, they have told us consistently, it is too confusing to deal with all these different activities, these different processes run by these different entities of the Federal Government.

So identifying that, consolidate it, that's what I call simplified business process. To interoperate with State and local government requires pulling people together and identifying, depicting, laying out the way we are going to work together, and we call that process design or process integration.

So, indeed, you have these in the multiple: homeland security functions. Steve Cooper, who is doing terrific work as essentially the CIO for the Office of Homeland Security, has laid out a concept as referred to as Foundation Projects; and, within those types of projects are essentially these kind of more detailed architecture projects. At a high level, we are making sure that all the different departments and agencies that play in that line of business are working together with him.

The actual work that needs to be done has to be done under some cross-agency organization. We have laid that out as the Information Integration Program Office, and we have requested accelerating that fund—that funding into the supplemental, and then that would be managed under the CIAO, the Critical Infrastructure Assurance Office.

So, at the high level, my office is making sure we are moving forward on the architecture, those business components that we have measures of effectiveness.

At the next tier down this Information Integration Program Office, working with the Office of Homeland Security, making sure that people are coming together to actually lay that out and go through the thought work, which can then define requirements. That work is due to be completed at the end of this fiscal year, so the end of September.

Mr. TURNER. It has been suggested by the GAO that we can't wait for this architecture to be developed, we have got to move faster. How do you respond to that?

Mr. FORMAN. We are moving faster, and the tradeoff I have is between roughly 2,900 major and significant IT projects in the budget. At the same time, we do not have 2,900 solutions architects. We don't have 2,900 world-class program managers.

So the trick is to allow enough good things to move forward without tying up resources that we need to focus. We are focusing our efforts on the strategic priorities that were in the budget: the war on terrorism, homeland security, revitalizing the economy. So we are not trying to boil the ocean, per se, but focus our resources.

Mr. TURNER. Do you have any comments on that from the GAO's perspective?

Mr. YIM. Well, I think that is actually the right strategy, but we also need to look and see what we currently have, what capabilities are currently already integrated into State and locals and the private sector which would be feeding the information up into the integrating strategy that would be included in the Office of Homeland Security and the national strategy. There is existing architecture that already is there that could be adapted, and one of the reasons why we may want to look at that is not only because it is familiar to State and local governments, and this would not be viewed as an additional burden upon them, but much of the information being collected there is being collected for other purposes, which, frankly, would help assure the reliability and validity of some of that data, rather than specialized data calls related to the Office of Homeland Security or any Federal agency asking for specific information.

For example, if highway information was being collected for highway improvement or Federal funding of highway projects, for example, but that was also relevant to evacuation proposals or the ability to bring law enforcement or first responders into an area of concern quickly, we would hate to see a specialized data call that, frankly, could be skewed or perhaps being done on too quick of a basis. We would like to have the ability to draw from existing data sets that were generated for other purposes. So the key would be integrating those data sets, being able to define some set of format or to focus on middleware that could integrate diverging formats so that there could be some central model in which these disparate data pieces could be sent and something made of the information in a timely manner.

Mr. FORMAN. I concur 100 percent with that.

Mr. TURNER. Do we have the staffing and expertise to accomplish this?

Mr. FORMAN. We do. We have to supplement it with the wonders of the IT industry. There is no question about it. Part of the emerging technologies, especially in the middleware arena in what's referred to as objectory architectures, where things—you hear terms like plug and play—now give you the ability to quickly leverage that data base or that work flow that was built for a different purpose, but fits this new mission. That's new technology. That's come out over the last 9 months to 12 months. And so we have to operate with the contractors helping us in this arena, consultants helping us who have already thought through this. We are not the first industry to grapple with this issue.

Mr. TURNER. Thank you, Mr. Chairman.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

Let me ask a general question. First I will start with Mr. Bohlinger.

I understand that the development of requirements is a key challenge, but are those requirements not the result of agency and government interaction? Would that process not be enhanced by a single portal type of process that we envision in our legislation? What I'm trying to say is, I am not sure you even know all your requirements sometimes until you have gone out to the private sector and seen what they have available and some of the issues they are tackling. There is an awareness gap sometimes between what government is doing and working on and what the private sector is out there doing.

Mr. BOHLINGER. I certainly concur with that, and as I said the request for information process and also more informal process working with the various private sector associations. Heaven knows, we don't know what the universe is out there, and it's a continuing education process, an education process for us in the Federal Government, and an education process for those in the private sector, on not only how you access the Federal Government, but how you assist. There are ways to assist that make a great deal of sense in helping refine requirements, in helping us understand, on the Federal side, the best way to apply technologies.

So I certainly do agree with you that these avenues have to be explored just because of the volume and complexity of the data.

Mr. TOM DAVIS OF VIRGINIA. OK. Dr. Raub, let me ask you; you refer to Secretary Thompson's Council on Private Sector Initiatives to improve the security, safety, and quality of health care. The Council was established in part to provide the private sector with a single point of contact for innovative ideas that cut across HHS's agencies and departments. Now, H.R. 4629, which I've introduced, would, among other things, establish a similar mechanism in the Office of Federal Procurement Policy, would apply to all agencies for innovative homeland security solutions. What do you think about extending the concept you use at HHS government-wide?

Mr. RAUB. Well, the concept has proved quite efficacious for HHS, and, in principle, I see no reason why it couldn't work on a broader basis across other agencies. Were that to be established, we would certainly work cooperatively and hard to ensure its success.

Mr. TOM DAVIS OF VIRGINIA. OK. Some allege that there was a communications breakdown between the CDC and the FBI and others when the anthrax letters came to Capitol Hill, New York and Philadelphia. Do you have any thoughts on that?

Mr. RAUB. Yes, sir, I do. I think both agencies have worked hard at that communication issue, and we believe will continue to improve. Some of the issues are the fundamental differences in our missions and our cultures that I think both agencies are doing better to recognize and understand one another. For example, when a matter involves a potential crime scene or a subject under surveillance from the FBI's perspective, which we appreciate significantly, a close hold of that kind of information and a very deliberate process is critical to be able to bring an ultimate successful prosecution. At the same time, the public health community needs to ensure that it has the information early enough to be able to mount various kinds of protective initiatives in the community.

So I think in general our view is the more time we spend interacting with one another, understanding the missions, the restraints, the better those communication systems can be.

Mr. TOM DAVIS OF VIRGINIA. Thank you.

Mr. Jordan, let me ask you a couple questions. FBI Agent Rowley testified yesterday at the Senate hearing that field agents have less access to information than the press because there are too many layers within the organization that clog information sharing. Do you have any comments on the reorganization efforts that have been announced by the FBI and how they might contribute to better information sharing?

Mr. JORDAN. Well, the reorganization efforts plan that the Director has submitted focus on having the FBI recognize that terrorism is our No. 1 mission, and that we are going to put more resources on terrorism, not just the investigation, but the prevention of it. And as we respond to that challenge, we are going to have new information needs and challenges to share our information outside the FBI with other intelligence and law enforcement agencies as well as make sure that information gets out to our field, which Special Agent Rowley is a representative.

So we recognize the need to—we need to share our information outside, but internally first, and we are making efforts in that regard.

Mr. TOM DAVIS OF VIRGINIA. Well, one of the reasons we called the hearing today was to determine the progress that Federal agencies involved in the homeland security were making in assessing the respective knowledge needs and information-sharing requirements.

There has been a lot of Monday-morning quarterbacking on this. Where are we in the process, in your opinion, over at the FBI?

Mr. JORDAN. We have made great strides. Our—outside of the Intelligence Community, our single largest group of partners in the prevention of terrorism are 650,000 State and local police officers who are the largest single available force to help us in a war against terrorism. We have met with them through their major city chiefs, through the ,IACP, International Association of Chiefs of Police, their representatives. We have attended their recent information-sharing summit. Director Mueller was the keynote speaker.

As I mentioned in my direct testimony, the directors brought in a high-profile chief to basically ensure that we recognize that State and local law enforcement are our partners in this effort, and that we get them the information they need, and that they share with us the—exactly what it is that they need. There are some obstacles, and, for example, some of the information that would be valuable to them is classified. It's probably not feasible to get Secret or Top Secret security clearances for 650,000 police officers. Maybe there is something in the middle that we can do, maybe some middle—or maybe there is a way to create a classification level below Secret where we can take information and change some of its attributes so that it could be disseminated at a below Secret level.

I mean, these are all the things we are working on. We are working on them with State and local law enforcement, and our Joint Terrorism Task Forces are probably one of the best and most successful and, historically, best efforts in this regard.

Mr. TOM DAVIS OF VIRGINIA. Some of the Secret stuff always gets in the hands of the press. So, you know, you want to get it in the hands of the agents as well.

Mr. JORDAN. Yeah.

Mr. TOM DAVIS OF VIRGINIA. All right. Thanks.

Let me ask Mr. Forman. Your statement stresses the important role that standards play in ensuring that the different systems can work together in furthering the homeland security mission. Where does the responsibility rest for developing and enforcing these standards?

Mr. FORMAN. There are two types of standards. One is at the technology level, and that resides with the Secretary of Commerce, and largely standards being defined at the National Institute for Standards and Technology. The other is a common component or standard of functionality, if you will. That's what we have undertaken via the CIO Council, and with the Federal Enterprise Architecture Program Office work that my office is overseeing. So I have kind of taken on that responsibility in my role at OMB on those functional standards. But we are doing it and the enforcement of it via the CIO Council's architecture committee. And, in that manner, as you know, probably the fastest way to get a standard is to get everybody who has to buy the technology to agree that this is what they are going to buy, this type of functional capability, and therefore ensuring not just the agreement on the standard, but the enforcement of that standard.

Mr. TOM DAVIS OF VIRGINIA. Thank you. I'm just going to make a final comment, and then I think Ms. Davis has a couple more questions.

Do you have a couple more questions for this panel? I think Jo Ann wants to get a question cleared up.

You know, we have gone through some of these security briefings on the House floor, and I get more out of CNN and Fox News than I do from our security briefings. And, of course, they are so nervous that somebody is going to leak something I assume they have the same kind of problems in the FBI and other agencies with getting word down to members on the street, to employees on the street who could use information, but are just so afraid that the classification, whether it's Secret or Top Secret or classified doesn't fit. And we have got to find a way to cut through this and get the information to the people on the street appropriately.

That has been one of the problems; as we look back and try to Monday-morning-quarterback this we get so hung up on all these classification systems that the word is not getting out in an appropriate fashion to the people who could benefit from it. The press has no problem getting ahold of a lot of this stuff and so we are basically victims of our own overregulation and inability to classify. And it's something we have got to continue to wrestle with. And also in our conversations with the private sector, some of this stuff I think we are overly protective of. That's just an observation, stepping back.

But I see a lot of progress being made, and I appreciate everybody taking the time to share with us and answer our questions today.

Ms. Davis.

Ms. JO ANN DAVIS OF VIRGINIA. Thank you, Mr. Chairman. And I don't mean to beat a dead horse, but I'm sort of just a straight-talking person, and I've got to say, I didn't understand your answers. The best I could understand is that the resources aren't the problem; the problem is the requirements and defining the requirements. But aren't you all supposed to define the requirements?

Mr. FORMAN. Well, we have new major IT investments in this year's budget, roughly $30 billion, and so the requirements have to come, we know best practices, from the people who are actually doing the work. When we bring in modern tools and techniques for essentially e-business in the private sector, that has tremendous applicability in virtually all the homeland security areas.

Ms. JO ANN DAVIS OF VIRGINIA. So are you supposed to, sir, define the requirements?

Mr. FORMAN. No. It's got to be at the level of the people actually who will use it in doing the work, married together with the CIOs or people within the CIO organization who are responsible for identifying.

Ms. JO ANN DAVIS OF VIRGINIA. How long does it take to do that and then to get the—I mean, by the time you do all that and get the technology in place, isn't it outdated?

Mr. FORMAN. No. Unfortunately, we tend to hide behind that in resisting change in many of the Federal agencies. It shouldn't take more than a couple weeks or a month to do this.

Ms. JO ANN DAVIS OF VIRGINIA. So, then, the problem more is in the culture and not requirements?

Mr. FORMAN. And resistance to change.

Ms. JO ANN DAVIS OF VIRGINIA. Which is the culture.

Mr. FORMAN. I tend to focus on, both dealing with the industry and with the agencies, these two simple measures of outcome that I mentioned before. How do we increase their response time, cycle time, the decisionmaking time? How do we improve the quality of the decisions that you are responsible for?

And I give the same test to the industry folks that come in, and I found from industry, some of the folks will come back to us with a very low-cost, very modern solution just because of the technologies that are out there. And when I look at low cost, I mean 40-, 50-, $60,000 for a program that had been budgeted for $30 million. To me, that's the pay off of bringing these modern technologies in; but what it means is people in the line of business do their work differently. If they don't sign up to doing their work that way, then we won't get that acceleration in decisionmaking, we won't get the results. What we will get is a 50-, $60,000 effort that turns into a $30 million effort and doesn't give us the results.

This is a chronic problem. It's been around for about 10 years now in government. It's part of change management, and, at the end of the day, a big part of the puzzle that we are using here is the management scorecard. We are literally tracking whether the agencies are adopting these modern business approaches and scoring them on that on a quarterly basis.

Ms. JO ANN DAVIS OF VIRGINIA. Well, maybe I just did things a little different in the private sector, but when I had people that worked for me, if they didn't do the changes the way I wanted them, they weren't there anymore.

Thank you, Mr. Chairman.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

Anything anyone on the panel want to add additionally?

Well, thank you all very much for your testimony today and in your answering our questions. If you want to supplement anything over the next couple of weeks, feel free to. I'll put it in the record.

I'm going to declare about a 2-minute recess as we switch panels. We have an outstanding panel coming up: Dr. Sugar of Northrop Grumman, who has already been introduced by Ms. Harman; Mr. Johnson, KPMG; Mr. Fitzgerald from Oracle, I see in the audience; and Mr. Pomata from webMethods. We will just take a couple minutes to exchange, and we will be back in 2 minutes. Thank you.

[Recess.]

Mr. TOM DAVIS OF VIRGINIA. I think we can resume the hearing. If everyone could just remain standing here, I want to swear our next distinguished panel in.

[Witnesses sworn.]

Mr. TOM DAVIS OF VIRGINIA. Let me just explain. This isn't the major investigative committee in Congress; so, by our rules, we swear every witness in. We are not trying to catch you on everything, but those are just the rules we operate under.

And so let me start with Dr. Sugar and work our way down. Try to keep it to 5 minutes. Again, we have the lights on there, and we will give some time for questions and then submit. And thank you for being with us today, Dr. Sugar.

STATEMENTS OF RONALD D. SUGAR, Ph.D., PRESIDENT AND CHIEF OPERATING OFFICER, NORTHROP GRUMMAN CORP.; LEONARD POMATA, PRESIDENT, FEDERAL GROUP, WEBMETHODS, INC.; S. DANIEL JOHNSON, EXECUTIVE VICE PRESIDENT, PUBLIC SERVICES, KPMG CONSULTING, INC.; AND KEVIN J. FITZGERALD, SENIOR VICE PRESIDENT, GOVERNMENT, EDUCATION & HEALTHCARE, ORACLE CORP.

Mr. SUGAR. Can you hear me?

Thank you, Mr. Chairman, Ms. Davis, Mr. Turner. It's always a pleasure to meet with you. My name is Ron Sugar, president and chief operating officer of Northrop Grumman, Incorporated, one of our Nation's major defense industrial firms. Northrop Grumman has a dedicated work force of over 100,000 engineers, scientists, and other professionals applying advanced technology in support of our military services and other governmental agencies. It's a great privilege to appear before you today and to talk about some of my observations on the important issue of providing technology solutions to the serious homeland security challenges facing our Nation today.

As a senior executive of a major defense firm, I cannot advise you on national policy or how to organize the government to approach this daunting task of homeland security. I can, however, provide a perspective on how those of us in the world of technology can help address this major challenge, and I can suggest certain steps the government can take to create a favorable environment where the innovative thinking, the manufacturing skills, and the procedural discipline of the defense industry could be applied to this pressing national need.

One should not underestimate the power of American industry, working with government, to provide good solutions to major challenges. We do rise to the occasion. The record of the past speaks for itself. The Manhattan Project of World War II, the development of strategic weapons and ICBMs during the cold war, and the placing of a man on the moon in the 1960's demonstrate what can be accomplished in a relatively short period of time when efforts are focused, resources are provided, and there is a national will to do it. As with these past examples, of course, urgency must now prevail.

I would like to identify for you three concerns that I believe may be inhibiting our ability to bring the power of American technological capability into this effort, and I will call them the three Rs, for lack of a better term: requirements, resources, and release from unreasonable liabilities. Requirements, resources, and release from unreasonable liabilities. Addressing these three Rs will greatly improve the requirement for industry to innovate and create effective technology solutions for this problem.

Now, let me briefly address what I mean by these three items. First, requirements. Despite the passage of 9 months, there are still very few specific requirements that have been identified by the many numerous agencies at all levels of government on what they need to meet the challenges that they face. We typically in industry provide technological solutions in response to governmental requests for proposals or requests for information, and their companion statements of requirements or specifications. Because there is great uncertainty among many agencies about their exact roles and missions in homeland security, there have been to date very few RFPs as a result of September 11th, and I would strongly second the testimony of Mr. Bohlinger from the INS on this matter. Requirements are very, very important here.

Second, resources. Now, certainly much money has been appropriated to date for this effort. With the original emergency funding, the current supplemental under consideration, and the fiscal 2003 proposal, there has been over $100 billion identified for homeland security, but the large percentage of these funds is for response and recovery. Very little to date has translated into requests for specific technology solutions. Neither Northrop Grumman Corp., nor any other major corporation that I know of at the moment, is yet able to determine from a business standpoint the additional business or revenue potential of this important emerging homeland security market. We know something is there, but we are not quite sure what it is and how we are going to address it.

And, finally, there is the third R: release from unreasonable liability, or indemnification. Many companies, including our own, now have technologies available to assist all levels of government in detecting and preventing future terrorist attacks. Paradoxically, our tort system has the capability of shifting the economic loss due to a terrorist criminal act onto those providing the tools to detect and prevent such acts.

Despite our best efforts, no technical system is infallible. The unintended consequence of even a single failure in a well-intended system or device that we might provide could result in a significant legal exposure that could financially ruin a company. Prudent com-

panies may find themselves unwilling to provide their critical technologies to the government and its agencies that need them because of the great financial risk involved. At Northrop Grumman, for example, we find ourselves face to face with this very issue now in our efforts to provide the Postal Service with a biological detection system to counter the anthrax threat. Clearly, containing liability exposure for those in industry who are trying to do good is a major policy issue that must be addressed by both Congress and the executive branch.

Now, if we can successfully deal with these three Rs, we can do a lot of good things. We have, for example, at Northrop Grumman sophisticated airborne surveillance platforms, such as the Global Hawk, that can be adapted for use in improving border and coastline security. We have Fire Scout, a smaller unmanned helicopter that can provide point surveillance around ports or other vulnerable national assets such as nuclear power stations. We have modern command, control, communications systems that can be adapted for domestic use by State and local organizations. We have increasingly effective systems for detecting and tracking chemical and biological agents. We have sophisticated information technology systems capable of managing and integrating large amounts of data, making it rapidly available. This can assist security officials, immigration officers, Customs agents, and the Border Patrol in greatly complicating any terrorist efforts to launch coordinated and deadly attacks against American facilities and citizens. We can do a lot right now.

Now, from a classical business perspective, however, homeland security would be viewed as an emerging market. But to be vibrant and viable, any market needs customers with clearly defined needs who have funds they are willing to spend to secure goods and services. Presently, with a handful of exceptions, the homeland security market is still somewhat clouded.

Mr. Chairman, your legislation, H.R. 4629, aimed at promoting innovative solutions for homeland security is a very appropriate first step. Its recommendation establishing an office to rapidly review technology proposals while providing procurement point of entry will be most helpful. I would urge you to move this legislation forward as quickly as possible. Combined with the President's announcement last evening about an establishing a Department of Homeland Security, this should provide increased momentum to allow us to bring the full power of our industry to bear.

Finally, let me be frank. I am concerned about the rate of progress we are making in protecting the Nation. This is a serious issue. Many good ideas are flowing from both the government and from industry. What we need now are the firm, specific requirements, immediately available funding resources, and protection from the risks of unreasonable liability. Give us these and we in industry will provide our Nation the tools to do this job.

Mr. Chairman, I applaud the efforts of the committee. I wish you well in your important endeavors, and thank you very much for having me here today.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

[The prepared statement of Mr. Sugar follows:]

Testimony of Dr. Ronald D. Sugar
President and Chief Operating Officer
Northrop Grumman Corporation

Before the Sub-Committee on Procurement and Technology Policy
Of the
House Committee on Government Reform

June 7, 2002

My name is Ron Sugar, President and Chief Operating Officer of Northrop Grumman Corporation, one of our nation's major defense industrial firms. Northrop Grumman has a dedicated work force of over 100,000 engineers, scientists, and other professionals applying advanced technology in support of our military services and other governmental agencies. It is a great privilege to appear before this committee and offer some observations on the important issue of providing technology solutions to the serious homeland security challenges facing our nation today.

As a senior executive of a major defense firm, I cannot advise you on national policy or on organizing the government for homeland security. I can, however, provide a perspective on how those of us in the world of technology can help address this major challenge. And I can suggest certain steps the government can take to create a favorable environment where the innovative thinking, manufacturing skills, and procedural discipline of the defense industry can be applied to this pressing national need.

One should not underestimate the power of American industry, working with government, to provide good solutions to major challenges. The record of the past speaks for itself. The Manhattan Project of World War II, the development of strategic weapons during the Cold War, and the placing of a man on the moon in the 1960s, demonstrate what can be accomplished, in relatively short time frames, when efforts are focused and resources are provided. As with these past examples, urgency must now prevail.

I would like to identify for you three concerns that I believe may be inhibiting our ability to bring the power of American technological capability into this effort. I'll call them the three "R"s:

(1) Requirements,
(2) Resources, and,
(3) Release from unreasonable liabilities

Addressing these three "R"s will greatly improve the environment for industry to innovate and create effective technology solutions.

Let me briefly address these three items. First -- **requirements**: Despite the passage of nine months, there are still very few specific requirements that have been identified by the numerous agencies, at all levels of government, on what they need to meet the challenges they face. We typically provide technological systems in response to governmental requests for proposals, RFPs, and their companion statements of requirements. Because there is great uncertainty among many agencies about their exact roles and

missions in homeland security, there have been very few RFPs as a result of September 11th.

Second – **resources**: Certainly much money has been appropriated to date for this effort. With the original emergency funding, the current supplemental under consideration, and the fiscal 2003 proposal, there has been over $100 billion identified for homeland security. But the large percentage of these funds is for response and recovery; very little to date has translated into requests for specific technology solutions. Neither Northrop Grumman, nor any other major corporation I know of, is yet able to determine the additional business potential of the emerging homeland security market.

Finally, there is the third "R" -- **release from unreasonable liability**. Many companies, including our own, now have technologies available to assist all levels of government in detecting and preventing future terrorist attacks. Paradoxically, our tort system has the capability of shifting the economic loss due to a terrorist's criminal act, on to those providing the tools to detect and prevent such attacks. Despite our best efforts, no technical system is infallible. The unintended consequence of even a single failure in a well-intended system or device we might provide could result in significant legal exposure that could financially ruin a company. Prudent companies may find themselves unwilling to provide their critical technologies to the government agencies that need them because of the great financial risk involved. At Northrop Grumman, for example, we find ourselves face-to-face with this very issue in our efforts to provide the Postal Service with a biological detection system to counter such threats as the post-911 anthrax attack. Clearly, containing liability exposure for those in industry, trying to do good, is a major policy issue that must be addressed by both the Congress and the Executive Branch.

If we can successfully deal with these "3 R's," we can do a lot of good things. We have in Northrop Grumman, for example, sophisticated airborne surveillance platforms, such as *Global Hawk*, that can be adapted for use in improving border and coastline security. We have *Fire Scout*, a smaller unmanned helicopter, that can provide point surveillance around ports or other vulnerable national assets such as nuclear power stations. We have modern command, control, and communications systems that can be adapted for domestic use by state and local organizations. We have increasingly effective systems for detecting and tracking chemical and biological agents. We have sophisticated information technology systems capable of managing and integrating large amounts of data and making it rapidly available. This can assist security officials, immigration officers, customs agents, and the border patrol in greatly complicating any terrorist efforts to launch coordinated and deadly attacks against American facilities and American citizens. We can do a lot **right now**.

From a classical business perspective, homeland security is an emerging market. But to be vibrant and viable, any market needs "customers," with clearly defined needs, who have funds they are willing to spend to secure goods and services. Presently, with a handful of exceptions, the homeland security market is still somewhat clouded.

Mr. Chairman, your legislation, HR 4629, aimed at promoting "Innovative Solutions for Homeland Security," is a very appropriate first step. Its recommendation establishing an office to rapidly review technology proposals while providing a procurement "point of entry" would be most helpful. I would urge you to move this legislation forward as quickly as possible. Combined with the President's announcement last evening about establishing a Department of Homeland Security, this should provide increased momentum to allow us to bring the full power of our industry to bear.

Finally, let me be frank: I am concerned about the rate of the progress we are making in protecting the nation. Many good ideas are flowing from both the government and the private sector. What we need now are the firm, specific requirements, immediately available funding resources, and protection from the risks of unreasonable liability. Give us these, and we will provide our Nation the tools to do the job.

Mr. Chairman, I applaud the efforts of this committee. I wish you well in your important endeavors, and I thank you for having me here today.

Mr. TOM DAVIS OF VIRGINIA. Mr. Fitzgerald.

Mr. FITZGERALD. Mr. Chairman, Ranking Member Turner, Congressman Davis, my name is Kevin Fitzgerald. I am the senior vice president of Oracle Corp., and on behalf of Oracle, I would like to thank you for inviting me to share experiences and perspective on information sharing and homeland security technology.

Mr. Chairman, since September 11th, we have been engaged in a battle on two fronts. First, we have been fighting to protect the lives of Americans from the threat of terrorism, and at the same time we have been struggling to protect the single most important asset needed to promote and preserve liberty and prosperity: the U.S. economy. If the investments made today to improve our homeland security prove ineffective, we will have missed a seminal opportunity to shape our future for the better, an opportunity that we are unlikely to see again.

If we step back and look at the goal of strengthening homeland security, the over whelming obstacle will be the effective partnering of the organizations, public and private, involved in the process. There are national, State, and local organizations geared toward law enforcement and intelligence, first responders, health care, Border Patrol, transportation, agriculture, and countless others. It is difficult to know where to start, and spending our Nation's tax dollars effectively will be challenging.

In order to protect the United States, we need an integrated national strategy and information infrastructure; yet implementing a national strategy with countless independent organizations will be like building a plane with at least 50 totally independent contractors. One builds the wings, another builds a navigation system, and yet another builds the fuselage and so on. Even if each organization excels at his or her given task, it will still work in a vacuum without any guidance on how and whether these separate parts work together in an effective whole, the combined concoction could never fly.

Imagine building our homeland security information systems airplane—like this airplane, not having any way to ensure they fit into a broader national strategy. The result will be a waste.

Fortunately, the President took a step in the right direction yesterday with his proposal to create a Department of Homeland Security, which would provide for a clearinghouse for terrorism intelligence. This is a significant and positive development, and I hope Congress will act on the President's proposal before you adjourn later this year.

For this new Department to succeed, Congress will have to target a significant amount of investments toward information technology. No doubt information is one of the most powerful weapons that we have in the fight against terrorism. The fact is that we have an extraordinary amount of information, but we lack sufficient capability to establish relationships between various information sources. Even today we see there are lots of facts we had about the individual terrorists responsible for the attacks on September 11th. Since we were unable to bring these facts together, intelligence agencies and law enforcement were not able to see the whole picture.

It would not be possible, prudent, or politically expedient to try and build a single national system for homeland security informa-

tion; we can, however, make it possible for the relevant organizations to build their systems in such a way that, although they are different, they can work in concert to support a national homeland security strategy, or, in more practical terms, a Department of Homeland Security.

Accomplishing this requires a commitment to standards. If Congress provides homeland security resources to 50 States, absent any kind of systematic direction, it will be used in at least 50 different ways, and certainly far more if these resources flow to localities. The system that would be built under this scenario may have local needs, but they will almost certainly not talk to one another unless there is an effort on a national level to require a few standards for information sharing and security. For information systems, those standards fall into three categories: data, integration, and security.

Data standards provide guidelines for how data is collected and stored, making data possible—sharing possible. For example, in law enforcement, the Department of Justice has defined a standard called the National Incident-Based Reporting System, or NIBRS. This standard defines guidelines for collecting and reporting information related to criminal incidents. So if my system is NIBRS-compliant, and your system is NIBRS-compliant, then we can compare data with one another because we both use and understand the codes that represent that type of criminal incident. Data standards like NIBRS are critically important for ensuring that once we establish connectivity between systems, we will know how to compare and interpret the results.

Integration standards define how a system exposes its data to other systems. For example, Web Services standards like WSDL, UDDI, and SOAP, define how a system wraps its data and publishes it to other systems. So a system can use these standards to say, in effect, I know all about pilot licenses in the State of Florida. If you give me a Social Security number, I will check your credentials and then give you XML in the following format that includes that person's license information. This approach means that I don't care what a system does or how it was built, I only care that it can accept and answer my question.

Perhaps the most important form of information standard is geared toward security. The most significant barrier to information sharing will not be technical issues, but concerns raised by organizations about exposing their data to potentially insecure systems. There are well-established standards in existence, and they have matured around the world, and they are now accepted globally. In the United States their use is managed by NIAP, the National Information Assurance Partnership. This is a collaboration between the National Security Agency and the National Institute of Standards and Technology.

Consistent government enforcement of security standards has been a source of frustration for Oracle. Despite its importance to national security, what we too often see is that the requirements for independent security evaluations are waived in procurement. This summer, a National Information Assurance Acquisition policy called NSTISSP No. 11 is scheduled to go into effect for systems that contain information relating to national security and requires

these systems to use products that have undergone an independent security evaluation. After September 11th, it is fair to say more and more Federal systems have a direct link to national security. Thus, policies like this one need to be strengthened and enforced through the procurement policy.

What can the Federal Government do to better ensure the use of these standards? First, national agencies need to take responsibility for defining more data standards as the Justice Department has done in the defining of NIBRS. Second, we urge Congress not to try and create integration standards. Industry and the Internet are defining and refining these standards faster than the government possibly could. Exploit what they develop. Third, Congress should encourage relevant agencies to enforce NSTISSP No. 11. These standards and processes are already in place.

We all know there will be an accounting for how Congress has targeted Federal spending on homeland security, and, with the President's announcement yesterday, this new Department, should Congress create it, will likely be held accountable as well for the administrative success of homeland security. If the result is 1,000 little systems with no improved national capacity to deal with the threat of terrorism, the American people will recognize this failure of planning and protection. Let's work together to make sure that doesn't happen. Congress, in its role as policy leader, can include appropriate standards to guide Federal, State, and local organizations down a common path of information sharing. The information technology industry can devise the systems to make sure these policies can work to accomplish our national goals.

Thank you again, Mr. Chairman, for the opportunity to be heard today. I look forward to answering any questions you have.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

[The prepared statement of Mr. Fitzgerald follows:]

Statement Of

Kevin Fitzgerald
Senior Vice President
Oracle Corporation

Before the
Subcommittee on Technology and Procurement Policy
Committee on Government Reform
United States House of Representatives

7 June 2002

Mr. Chairman, Ranking Member Turner, and distinguished members of the Subcommittee, my name is Kevin Fitzgerald, and I am Senior Vice President of Oracle Corporation. On behalf of Oracle, I would like to thank you for inviting me to share our experiences and perspective on information sharing and homeland security technology. Given recent news stories, this is a particularly well-timed hearing today.

I will summarize my statement, but I ask that my entire statement, along with several supporting documents relating to Oracle initiatives on homeland security, and the security of information technology be made a part of the record.

Mr. Chairman, since September 11th, we have been engaged in a battle on two fronts. First, we have been fighting to protect the lives of Americans from the threat of terrorism. And, at the same time, we have been struggling to protect the single most important asset needed to promote and preserve liberty and prosperity – the US economy. If the investments made today to improve our homeland security are wasted, we will have missed a profound opportunity to shape our future for the better – an opportunity that we are unlikely to see again soon.

If we step back and look at the goal of strengthening our homeland security, it can be overwhelming to think of all of the various organizations – public and private -- involved in the process. There are national, state and local organizations geared toward law enforcement and intelligence, first responders, healthcare, border control, transportation, agriculture, and countless others. It's difficult to know where to start. Also, spending national dollars effectively is very difficult. The dilemma is a spending scheme that will do nothing to strengthen our *national* homeland security.

In order to protect the United States, we need an integrated, national strategy and infrastructure. Yet implementing a national strategy with countless independent organizations would be like building a plane with at least 50 totally independent contractors. One builds the wings, another builds a navigation system, and yet another builds a fuselage and so on. Even if each organization excels at his or her given task, if they work in a vacuum without any guidance on how or whether these separate parts work together in an effective whole, the combined concoction could never fly.

Imagine building our homeland security like that airplane, and did not have some way to ensure each part fit in a broader national strategy. The result would be a waste.

Congress is expected to target much of the post-9/11 investments toward information technology. No doubt, information is one of, if not the most powerful weapon that we have in the fight against terrorism. The fact is we have extraordinary amounts of information, but we lack sufficient capability to establish relationships between various information sources. Even today, we see that there are lots of "facts" that we had about the individual terrorists responsible for the attacks on September 11th. Since we were unable to bring these facts together, intelligence agencies and law enforcement were not able to see the whole picture.

It would not be possible, prudent or politically expedient to try to build a single, national system of homeland security information. We can, however, make it possible for various, relevant organizations to build their systems in such a way that, although they are different, they can work in concert to support a national strategy for homeland security. Accomplishing this requires a commitment to standards.

If Congress provides homeland security resources to 50 states, absent any kind of systemic direction, it will be used in at least 50 different ways, and certainly far more if these resources flow to localities. The systems that would be built under this scenario may or may not function, but they will almost certainly not talk to one another unless there is an effort on the national level to require a few standards for information sharing and security.

For information systems, those standards fall into three categories: Data, Integration, and Security.

Data standards provide guidelines for how data is collected and stored, making data sharing possible. For example, in Law Enforcement, the Department of Justice has defined a data standard called the National Incident Based Reporting System or NIBRS. This standard defines guidelines for collecting and reporting information related to a criminal incident. So, if my system is NIBRS compliant and your system is NIBRS compliant, then we can compare data with one another because we both use and understand codes that represent a type of criminal incident, such as code 240, which represents a "Motor Vehicle Theft."

Data standards like NIBRS are critically important for ensuring that once we establish connectivity between systems, we will know how to compare and interpret the results.

Integration standards define how a system exposes its data to other systems. For example, Web Services standards like WSDL, UDDI, and SOAP define how a system wraps up its data and publishes it to other systems. So a system can use these standards to say (in effect), "I know all about pilot licenses in the state of Florida. If you give me a social security number, I will check your credentials and then give you XML in the following format that includes that person's license information." This approach means that I don't care what a system does or how it was built. I only care that it can accept and answer my question.

Perhaps the most important form of information standard is geared toward security. The most significant barrier to information sharing will not be technical issues, but concerns raised by organizations about exposing their data to potentially insecure systems. There are well-established standards in existence, and they have matured around the world and are now accepted globally. In the United States, their use is managed by NIAP, the National Information Assurance Partnership. This is a collaboration between the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST).

Consistent government enforcement of security standards has been a source of frustration for Oracle. Despite its importance to national security, what we too often see is that requirements for independent security evaluations are waived in procurement after procurement. This summer, a National Information Assurance Acquisition policy (NSTISSP #11) is scheduled to go into effect for systems that contain information related to national security, and requires these systems to use products that have undergone an independent security evaluation. After September 11th, it is fair to say that more and more federal systems have a direct link to national security. Thus, policies like this one need to be strengthened and enforced through procurement policy.

What can the federal government do to better ensure the use of these standards? First, national agencies need to take responsibility for defining more data standards, as the Justice Department has done in defining NIBRS. Second, we urge Congress not try to create integration standards. Industry and the Internet are defining and refining these standards faster than the government possibly could. Exploit what they develop. Third, Congress should encourage relevant agencies to enforce NSTISSP #11. The standards and process for this are already in place.

No doubt, when the dust settles, an accounting will be made of how Congress has targeted federal spending on homeland security. If the result is a thousand little systems, but no improved national capacity to deal with the threat of terrorism, the American people will recognize this failure of planning and protection. Let's work together to make sure that doesn't happen. Congress, as policy leaders, can define appropriate policies to guide federal, state and local organizations down a common path of better information sharing. The information technology industry can devise the systems to make sure these policies can work, despite government differences, to accomplish our national goals.

Thank you again, Mr. Chairman, for the opportunity to be here today. I look forward to answering any questions the Subcommittee may have.

Mr. TOM DAVIS OF VIRGINIA. Mr. Johnson.

Mr. JOHNSON. Mr. Chairman and members of the subcommittee, thank you for this opportunity to share KPMG Consulting's views on the topic of homeland security. My name is Dan Johnson, and I lead our public services business unit, which is comprised of over 3,000——

Mr. TOM DAVIS OF VIRGINIA. Mr. Johnson, you don't need to keep it a secret; you need to turn on your microphone.

Mr. JOHNSON. Got it now?

Mr. TOM DAVIS OF VIRGINIA. Got it.

Mr. JOHNSON. Sorry. I'll start over again.

Mr. Chairman and members of the subcommittee, thank you for this opportunity to share KPMG Consulting's views on the topic of homeland security. My name is Dan Johnson, and I lead our public services business unit, which is comprised of over 3,000 professionals serving Federal, State, and local government clients.

KPMG Consulting supports large-scale information technology modernization programs at many of the Federal agencies that are critical to our homeland security efforts, including the Immigration and Naturalization Service, the Customs Service, the Department of State, the Internal Revenue Service, the Federal Aviation Administration, Coast Guard, and the military departments, as well as many public safety agencies in key States such as Pennsylvania, New York, Texas, California, South Carolina, and the District of Columbia. Most recently we have been engaged to help stand up the Transportation Security Agency in defining its mission activities in business processes as well as supporting development of an entry/exit system at Immigration and Naturalization Service which would document the arrival and departure of aliens at U.S. ports of entry.

Mr. Chairman, we feel that our 40 years of experience in serving government entities such as these and the knowledge of their organizations, systems, processes, and protocols that experience brings uniquely qualifies KPMG Consulting to discuss change management issues and technology acquisition measures as they relate to homeland security. In the aftermath of September 11th, when KPMG Consulting mobilized to provide recovery assistance to our New York Port Authority and New York Department of Finance clients at the World Trade Center, as well as our DOD Office of the Comptroller clients at the Pentagon, the requirements for a higher level of cooperation and collaboration between Federal, State, and local governments, as well as the private sector, has reached a new level of urgency. We would like to address several areas which will impact and challenge attaining that higher level of integration.

The first is leveraging existing capabilities. We must get a firm grasp of the information available today, the technologies that are being employed, and match that data and those technologies to identifiable programs. An example we are most familiar with is the Pennsylvania Criminal Justice Network, commonly referred to as JNET. Following the crash of United Airlines Flight 93 in Western Pennsylvania, a JNET terminal was set up for the FBI. Running the Flight 93 passenger list through JNET and searching multiple Commonwealth justice system data bases simultaneously, the FBI was able to identify one of the suspected terrorists on board, and

confirmed that another suspected terrorist was, in fact, already incarcerated.

The JNET story is a microcosm of the challenges that homeland security faces. Initiated in 1998, it overcame the stovepipe territorial issues of sharing sensitive information across 17 different State agencies, 2 cities, and 20 counties, now totaling over 5,000 users this year. It did so with an architecture which lent itself to gradual and interactive development showing incremental benefit and promoting comfort among its stakeholders as it evolved. It did so through strong executive sponsorship and a centralized independent budget for it alone. It did so through protecting the integrity of the individual stakeholder data bases by implementing rigid access controls, and it did so by establishing a government structure in which all the key stakeholders were represented.

The second area, as agencies look across their investments with an eye toward addressing homeland security missions, they must first determine what information is needed before looking for new technology solutions. They must match this with their understanding of what their problems are, what technologies exist today to address those problems, and how can they best leverage those technology solutions and improve upon them. Then, and only then, can agencies take the next step of determining what else needs to be done, what other technologies must be acquired.

Last, Mr. Chairman, we commend you for introducing H.R. 4629, which would establish a program to encourage and support carrying out innovative proposals to enhance homeland security. Its provisions for the streamlined acquisition of innovative solutions certainly is needed.

In our experience, application of IT investment and portfolio management disciplines is essential to the success of a technology program of the magnitude of homeland security. A set of standard criteria should be established to streamline and focus the screening of these technology proposals and to normalize the evaluation of their potential. Using this type of approach, each proposal is viewed as a component of an overall homeland security technology portfolio. The portfolio would be continuously monitored and adjusted as new proposals were presented and technologies were tested and implemented, and would ensure that all components of homeland security are considered against an integrated framework.

Mr. Chairman, again, thank you for holding this important hearing today. We look forward to working closely with you and the rest of the subcommittee in any way you deem appropriate.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

[The prepared statement of Mr. Johnson follows:]

HEARING TESTIMONY

KPMG Consulting

HOMELAND SECURITY | JUNE 7, 2002 | PUBLIC SERVICES

Statement of
S. Daniel Johnson
Executive Vice President – Public Services
KPMG Consulting, Inc.
Before the
House Subcommittee on Technology and Procurement Policy

Mr. Chairman and Members of the Subcommittee, thank you for this opportunity to share some of KPMG Consulting's views on the topic of homeland security.

KPMG Consulting, Inc. is one of the world's leading systems integration and management consulting firms. We employ over 9,000 people worldwide, fulfill the needs of over 2,500 clients, and have revenues approaching $3 billion. Over two years ago we separated completely from KPMG LLP, the tax and audit firm, and in February of 2001, we were the first of the Big Five to become a publicly held corporation. I lead KPMG Consulting's Public Services sector and am responsible for our federal, state and local, higher education and health care work.

KPMG Consulting is leading or is on teams modernizing some of the federal government's largest justice, defense, and information technology programs, including projects at Customs, the Internal Revenue Service, the Coast Guard, and the Department of Defense. And we have been contracted to provide homeland security work to many other government agencies. For example, at the Immigration and Naturalization Service (INS) we are working on an entry/exit system to document the arrival and departure of aliens at U.S. ports of entry and we are assisting the INS Office of Inspections develop a strategic plan geared towards today's rapidly changing world. We are supporting the Transportation Security Agency (TSA) to define mission activities and business processes, to develop the infrastructure to manage and monitor those processes, and to develop the top-level concept of the automated information system to support performance management. Also at TSA, we are supporting efforts to prepare and coordinate new security operations that will help ensure air passenger safety at the nation's 429 commercial airports.

We also have a significant state and local practice and currently have ongoing projects in approximately 26 states, ranging from statewide information technology systems to helping them improve their business processes. In the aftermath of September 11th, we worked closely with our New York clients to provide recovery assistance to the New York Port Authority and the Department of Finance. This consisted of activities ranging from providing office space to those who had been displaced by the collapse of the World Trade Centers, to providing communications support to help these agencies reestablish their computer network systems.

Mr. Chairman, based on over forty years of experience in serving federal, state, and local customers, I believe we are uniquely qualified to discuss change management issues and technology acquisition measures as they relate to homeland security. Homeland security should be considered as a condition that shatters all the assumptions of the past; affects all levels of government; and requires a new level of cooperation and collaboration between federal, state, and local governments and the private sector. This poses many challenges. Aside from what I believe is the single most important challenge – creating and maintaining a sense of urgency -- I would like to highlight just a few others.

Exposure

The first is mitigating the risk of exposing valuable information to our enemies. While public discourse on our progress in responding to the threat of terrorism is necessary, releasing too much detail of that response could further expose the very vulnerabilities we are trying to address. Mr. Chairman, that exposure should be managed with the highest regard for security. Even the simple act of publicly identifying requirements and solutions could pose a risk since the underlying problem could be taken advantage of by our enemies during the time that solutions are being developed. In addition, the playing field we are on is fluid – today's solutions are not necessarily adequate for tomorrow's problems – and we must make certain we do not expose unforeseen shortcomings in our current efforts.

Cultural limitations

The second challenge is that significant "cultural limitations" continue to exist which will delay the resolution of our nation's vulnerabilities. Limitations to speedy solutions are classic and include: time; the difficulties in changing the government's structure where information and

processes are stove piped within bureaus and agencies to a new model of increased interagency coordination; a need for strong vertical and horizontal authority; a slow transition to performance-based acquisition and accountability; and the shifting of priorities and money before real results can be achieved.

Compounding the problem of shifting funding levels is the likelihood that funding for homeland security will become more and more embedded in agency, state, local and commercial budgets vs. continuous special funding. Homeland security funding could become very difficult to track and therefore could inadvertently be shifted away from real homeland security missions. We feel it is extraordinarily important to match this shift to an even more heightened sense of priority for agency accountability, performance, metrics, and flexibility so that agency leadership and Congress, in its oversight capacity, can be certain that these critical missions are achieved.

Information Technology and Data Gaps

Third: As agencies look across their investments, with an eye towards addressing homeland security missions, they must first understand that gaps in information technology are based on gaps in information and data and not the reverse. Before looking for new technology solutions, agencies must first determine what information is needed and assess whether or not it will be needed in the future. They must match this with their understanding of what the problems are, what technologies exist today to address the problem, and how can they best leverage those technology solutions and improve upon them. Then, and only then, can agencies take the next step of determining what else needs to be done – what other technologies must be acquired. Agencies should be asking themselves: What do we have? Can we connect what already exists? What don't we have? How do we get it? And how do we connect all of this?

One example of how technology can be used to effectively close information gaps, and one that we are intimately familiar with, is the Pennsylvania Criminal Justice Network, commonly called JNET. The project was initiated in 1997 in response to Governor Ridge's priority for consolidated agency projects and was conceived after the Chief Information Officer (CIO) received multiple requests from criminal justice agencies for funding to develop redundant systems. In response, JNET was established to unify disparate justice and public safety networks across the state. It provides a common on-line environment that allows authorized

state, county, and local officials to access offender records and other criminal justice information across participating agencies.

The JNET example is notable in that it has faced and overcome many of the challenges that exist at the federal level today, namely territorial issues about sharing information with other agencies, privacy concerns, and the need for strong executive sponsorship. For example, each participating agency controls what information it shares and who is authorized to see it. Territorial concerns have been addressed by implementing the architecture gradually and in stages. As agencies began to see the benefit of information sharing in their everyday jobs, they became more comfortable in sharing greater amounts of information. The governance structure of the program also has played a key role in JNET's success, leading the General Accounting Office (GAO) to cite it as a leadership example for CIOs (GAO-01-376G).

This system has also played a role on the federal level and was used immediately after September 11th by the FBI to identify suspects from United Airlines Flight 93 that crashed in Western Pennsylvania. Using JNET, the FBI was able to identify a suspected terrorist by checking the flight passenger list against a driver's license photo. Another suspected terrorist was identified using arrest record information and was located in a correctional facility.

JNET currently includes several federal agencies, 17 state agencies, the cities of Pittsburgh and Philadelphia, 20 counties as well as some smaller municipalities. As of May 2002, 3,200 individuals are using the system; approximately 300 are on the municipal level. 5,000 users are expected by the end of the year.

Leverage existing capabilities

Fourth: Even prior to September 11th, a great deal of effort was being directed at reforming federal, state and local government management and processes. The pace of this transformation quickened in the early nineties with the growing emphasis on acquisition reform and I commend this subcommittee and its members on those efforts. The resulting agency modernizations and reengineering efforts underway now should serve as the foundations for many agencies' responses to homeland security threats. We urge you to exploit those management realignments wherever possible and to resist the temptation to start from scratch

at each agency. We recommend that you leverage the best practices at those agencies in order to drive expansion of capabilities across government.

Similarly, the federal government should get a firm grasp on the technologies that are being employed today and the information they currently have available and try to match those technologies to identifiable problems. Agencies should then leverage those investments across government versus instituting new technology solutions when they don't have a clear characterization of what is needed.

Acquiring New Technology

Lastly: Mr. Chairman, we commend you for introducing H.R. 4629, which "would establish a program to encourage and support carrying out innovative proposals to enhance homeland security". Its provisions for the streamlined acquisition of innovative solutions are certainly needed. In addition to the provisions of the bill, we feel this panel should urge federal agencies to make certain that before the government test bed concept takes hold, the government clearly understands the business problems it is trying to solve.

As stressed in H.R. 4629, it is important to focus on the selection of the right technologies. Of equal importance, however, is the successful deployment and use of these technologies in fulfilling the mission and objectives of homeland security.

In our experience, application of the IT investment and portfolio management disciplines, promoted by the Clinger-Cohen Act, General Accounting Office guidance, and the Office of Management and Budget budgeting process, is essential to the success of any program, especially a technology program of the magnitude of homeland security. These disciplines will establish a solid and consistent framework in order to initially justify the value of the technologies being selected and improve the probability that these technologies will successfully enable the mission and goals of homeland security.

Similar to the standards promoted in the very disciplined Exhibit 300 reporting process that agencies go through to rationalize their IT investments (OMB Circular A130 requirements for

budgeting), a set of standard criteria should be established in order to streamline and focus the screening of these technology proposals and to normalize the evaluation of their potential as well as provide a mechanism to monitor the implementation and deployment process. Using this type of an approach, each proposal is viewed as a component of an overall homeland security technology portfolio. The portfolio would be continuously monitored and adjusted as new proposals were presented and technologies were tested and implemented and would ensure that all components of homeland security are considered against the framework of: detection; prevention; preparedness; response; and recovery.

The IT portfolio discipline is an essential management element that will provide all involved a clear view of the nation's commitment to homeland security priorities and objectives and how they are being enabled by technology investments.

Mr. Chairman, again, thank you for holding this important hearing today. I look forward to working closely with you and the rest of this subcommittee in any way you deem appropriate.

Mr. TOM DAVIS OF VIRGINIA. Mr. Pomata, you are our cleanup speaker here.

Mr. POMATA. Thank you. Mr. Chairman, thank you for the opportunity to testify today. My name is Len Pomata, and I serve as the president of webMethods' Federal business unit, part of webMethods, Incorporated, a Fairfax, Virginia, company.

WebMethods manufactures integration software, a technology that enables the government agencies and companies of all sizes to connect their computers and data systems together. The technology is straightforward, cost-effective, reliable, secure, and readily available. It facilitates the right information getting to the right people at the right time.

It is interesting that much of America's investment to date in homeland security has been spent on the last line of defense, guards, gates, and guns. That's a natural and critical part of the response, but there is a part of the September 11th answer that has still received too little public attention, and that is the use of information technology as a proactive first line of defense. It is ironic, because it is information technology and those capabilities that give America one of the greatest competitive advantages in combating terrorism and securing the homeland.

The INS and the FBI are currently highly visible examples of the need for integration software and the sharing of information across agencies. Like most Americans, I applaud these agencies for their dedicated employees and their leadership, but there are lessons we have learned and can learn from the events of September and the importance of sharing critical information. In some instances agencies had identified important information, but the information was not effectively coordinated into a common view or given to relevant officials.

I realize that in many instances substantial policy and political issues may argue against sharing, but there is no technological reason. My point, Mr. Chairman, is that sharing of critical information, both inside and outside the government, is straightforward and relatively easy. Linking systems has become secure and affordable. At webMethods, we know this because we do this every day in our business.

Public and private sector organizations alike face the cultural policy issues, but I would like to mention a few lessons that we have learned in addressing this with our customers.

First, organizations don't have to share or integrate entire systems, only that which is important, only that which is defined as part of their critical mission. Defining those as precisely as possible can make the cultural and political boundaries and barriers seem much lower than they may first appear.

Second, simply connecting data bases and applications does not produce the right information to the right people. It is necessary to define the mission and particular information to be shared in a logical process, and not an artificial organization. That is what determines what—and you need to determine who is providing and who is receiving information. Those are the critical parts.

Third, it should be remembered the purpose of integrating information is not just to distribute it, but to be able to push it or give

it to those—that right information to the high-level officials as well as down to the field agents that may need it in a push technology.

Fourth, as customers like Covisint, an e-business exchange for major automakers, we have discovered the utility of building an online hub, for instance, that has competitive organizations plugging in, and without disclosing proprietary information works very well in the commercial sector, and this is a model that I think the government may use for sharing information in the public sector.

You know, there is a temptation to think that with so much money already spent on information systems, surely we can be much better at coordinating information; but these systems have become increasingly more complex, and have been dedicated to very specific tasks, and have become individual silos and islands of information, which actually can sometimes hamper the facilitation of information coordination. These systems contain mountains of information, and, as a result, helping them simply to communicate with each other has the potential to tap tremendous new value from existing resources.

Traditionally this integration of disparate systems, applications, and data bases has taken place through costly, time-consuming customization efforts. Until recently, it would require deploying scores of programmers and software writers to go into a company or agency and manually write code to create custom connections among these systems. In recent years, particularly in the last 12 to 17 months, this has become virtually unnecessary. It can now be done far more quickly, cheaply, and reliably, largely through off-the-shelf software. As a result, companies and agencies can now modernize and extend the life of old systems and avoid the huge expense of replacing them, much like the Navy might view in extending the life with modernization of one of their ships.

Integration software can make this happen now amongst the vast—and makes this happen now amongst the vast majority of the top 2,000 global companies. Government, too, is now appreciating the power and the potential of this latest IT revolution.

Integration software depends on language protocols. One of those is XML. Recently the GAO emphasized the importance of XML and the need for government to focus on it in terms of standards and utilization. As the GAO pointed out, XML offers the greatest potential for agencies to share information with each other and across the government. XML is here now and is the language that can be used to integrate complex technology systems, built over time, multiple platforms, and they can work together.

Mr. Chairman and members of the committee, every American recognizes the importance of homeland security, and for obvious reasons. My message to you is that government, recognizing the importance of information technology, information sharing, and new integration technologies, can contribute to this effort. This subcommittee in particular, and the committee in general, has been the voice of ensuring the effective use of different technology gets distributed across the government. Mr. Chairman, I applaud this hearing and encourage you to continue this program.

Finally, Mr. Chairman, I, as well as some of the other panelists, would like to take this opportunity to express my strong support for H.R. 4629, your bill. As any business executive can tell you,

even the brightest and best ideas would not advance unless there was a process and organization that could properly review them and advance them. Especially in times that call for urgent action, there must be an effective and efficient clearinghouse within the government to consider leading-edge technology. Your idea was well thought out and responded to concerns of your February hearing. I know that the committee considers the testimony of its witnesses, and I appreciate the opportunity for the private sector to be at this hearing. I stand ready to answer any questions.

Mr. TOM DAVIS OF VIRGINIA. Thank you.

[The prepared statement of Mr. Pomata follows:]

Testimony of
Mr. Len Pomata
President
webMethods Federal

To The
United States House of Representatives
Committee on Government Reform
Subcommittee on Technology and Procurement Policy

10:00 AM
June 7, 2002

Mr. Chairman,

Thank you for the opportunity to testify today. My name is Len Pomata, and I serve as President of webMethods Federal, a business unit of webMethods, Inc., based in Fairfax, Virginia. webMethods manufactures integration software, a technology that enables large government agencies and companies of all sizes to connect their computer systems and databases. The technology is straightforward, cost effective, reliable, secure, and readily available. It facilitates the right information getting to the right people at the right time.

It is interesting that much of America's investment to date in homeland security has been on the last line of defense...guns, guards and gates. That's a natural and critical part of the response, but there is a part of the 9/11 answer that has still received too little public attention, and that is the use of information technology as a pro-active, initial line of defense.

This is ironic, because it is in Information Technology capabilities that America has one of its greatest competitive advantages to combat terrorism and secure the homeland.

The INS and FBI are current high visibility examples of the need for integration software and the sharing of information across agencies. Like most Americans, I applaud the work of these agencies, their dedicated employees, and their leadership. But there are lessons we can learn from the events of last September and the importance of sharing critical information. In some instances, agencies have identified important information, but that information was not effectively coordinated into a common view available to relevant officials.

I realize that in many instances substantive policy and political issues may argue against information sharing - but there is no technological reason. My point, Mr. Chairman is that the sharing of critical information both inside and outside government is straightforward and relatively easy. Linking systems has become secure and affordable. At webMethods we know this because we are in the business of doing it everyday. You will hear from other members of the panel who also share this view.

Public and private sector organizations alike face cultural and policy issues, and I would mention several lessons we've learned in addressing our customers' needs.

First, organizations don't usually need to integrate their entire systems, only certain key data elements. Defining those as precisely as possible can make the cultural and policy barriers much lower than they may at first appear.

Second, simply connecting databases and applications does not produce the right information for the right people. It is necessary to define the mission of the particular information-sharing so that a logical process, not an artificial organization, determines who is providing and receiving the information.

Third, it should be remembered that the purpose of integrating information is not just to distribute it, but also to "push" the right information both to high level decision makers and down to the field.

And fourth, at customers like Covisint, an ebusiness exchange for major automakers, we have discovered the utility of building an online hub that competitive organizations can plug into without disclosing proprietary information, which is a model the government might consider for homeland security.

There is a temptation to think that, with so much money already spent on information systems, surely there must be better coordination of information already. But as systems have become increasingly more powerful and complex, they have been dedicated to specific tasks and organizations, and have become individual silos and islands of information, hampering rather than facilitating coordination.

But the systems contain mountains of information, and, as a result, helping them simply to communicate with each other has the potential to tap tremendous new value from existing resources.

Traditionally, this integration of disparate systems, applications, and databases has taken place through costly and time-consuming customization efforts. Until recently it would require the deployment of scores of software writers to go into a company or agency and manually write software code to create connections among systems.

In recent years, this has become not virtually unnecessary; It can now be done far more quickly, cheaply, and reliably through largely off-the-shelf software. As a result, companies and agencies can now modernize and extend the life of old systems and avoid the huge expense of replacing them...just as the Navy might extend the life of ships with modernization programs rather than the much greater cost of replacement.

The integration software that can make this happen is now in use among the vast majority of the top 2000 companies in the world. Government too is appreciating the power and potential of this latest IT evolution. Integration software depends on language protocols. One of these is XML. A recent GAO report emphasized the importance of XML and the need for government to focus on it in terms of standards and utilization. As the GAO pointed out, XML offers the greatest

potential for agencies to share information with each other and across the government. XML is here and now, and it is the language that allows software to tie complex technology systems, built over time and on many platforms, together as one.

Mr. Chairman and Members of the Committee. Every American recognizes the importance of homeland security today and for obvious reasons. My message to you is that the government, recognizing the important role of information technology, information sharing, and new integration technologies can contribute to this effort. This Subcommittee in particular and this Committee in general has been the voice for insuring the effective use of different information technologies across government. Mr. Chairman, I applaud this hearing and encourage you to continue a program of diligent oversight on this subject.

Finally, Mr. Chairman, I would like to take this opportunity to express strong support for your bill HR 4629. As any business executive can tell you, even the best and brightest ideas would not advance unless there is a process and organization to properly review and support their advancement. Especially in a time that calls for urgent action, there must be an efficient clearinghouse for government to consider leading-edge technology solutions. Your idea was a well-thought out response to concerns expressed in your February hearing. I know that the committee considers seriously the testimony of its witnesses and we appreciate the opportunity for the private sector to make a difference. We greatly appreciate your leadership.

Once again, I thank you for the opportunity to testify and I stand ready to answer any questions.

Mr. TOM DAVIS OF VIRGINIA. I am going to recognize.

Ms. Davis to start the questions, but I've got to ask this question: This XML, this is new to me. Is this kind of a universal language that everybody can tap into?

Mr. FITZGERALD. Central markup language.

Mr. POMATA. And it is used within the Internet. It's an Internet technology language. It allows many different types of systems over many different platforms to communicate through the Internet and share information.

Mr. TOM DAVIS OF VIRGINIA. How widely used is that in the private sector?

Mr. POMATA. Very, very extensively.

Mr. FITZGERALD. Pervasively.

Mr. TOM DAVIS OF VIRGINIA. You have got to remember, I left PRC in, what, 1994.

Mr. POMATA. A few years ago.

Mr. TOM DAVIS OF VIRGINIA. I'm just trying to get it.

OK. Ms. Davis.

Ms. JO ANN DAVIS OF VIRGINIA. Thank you, Mr. Chairman.

And thank you, gentlemen, for being here.

And, Dr. Sugar, it is a pleasure to see you again.

You know, I sit on the House Armed Services Committee, and you talk about turf wars, you have got the Army, Navy, Air Force, Marines, and there is a little turf war there sometimes. But in this war in Afghanistan, I was able to watch how, when there was a requirement, we had an Army fellow on a horse, and we had a Navy pilot in the sky, and within a 2-week period they developed technology on a Palm Pilot for that Army fellow, the soldier on the horse, to let the Navy pilot know exactly where to drop the bomb. So in a 2-week period, we can get the technology.

And, Mr. Johnson, I want to go to you.

Well, Dr. Sugar, I heard you say that requirements were—you were still waiting on the requirements. And you heard me in the former panel ask those why we don't have them; and, if I heard you correct, Mr. Johnson, you said that relatively, you know, in a short period of time, you could get those requirements. Those weren't your words, but that's what I gleaned out of it. But we are 9 months since September 11th, and we don't have requirements. We are nowhere close in many of these agencies to seeing what we need to help us with homeland security, and we are getting ready here to vote on the proposed new Department of Homeland Security.

Should we be having a struggle getting those requirements from these agencies? I know you are contracted with some of them, but not all of them. Can you help us out, help me out, there to understand why we don't have them?

Mr. JOHNSON. Well, I think the driver here is the sense of urgency. When we were prosecuting the war in Afghanistan, the sense of urgency was very, very high in terms of being able to get things done on short notice. The example I used in Pennsylvania, again, was a situation where it is a somewhat smaller group of people, a little narrowly focused effort to go forward with. But the driver is—this country can do amazing things in short order when there is a sense of urgency to drive it to that, and I think many

of us see that we don't see that sense of urgency as being pushed down through the organization to execute those things in a rapid fashion.

Ms. JO ANN DAVIS OF VIRGINIA. Well, I would certainly hope we don't have a another disaster for that sense of urgency.

Dr. Sugar, do you want to add something?

Mr. SUGAR. Could I add to that? I certainly agree on the urgency sense. There is no question about that necessity is the mother of invention. When lives are on the line, people do remarkable things and put aside partisan and parochial boundaries.

There is also an issue of skills, and skills and the ability to know how to define requirements, how to transform a nebulous set of needs or vague sense of wants into very specific actionable statements and quantitative measures that can be used, and then put in place the technology that solves the problem. That's a skills set which doesn't generally reside, quite frankly, in most of the agencies in the U.S. Government, and generally does not reside in great abundance in the State and local government agencies around the country. That is not an indictment of them, it is just simply a fact that it is just not something that has been done. It has been developed in the Intelligence Community, it has been developed in the Department of Defense. Certainly the ballistic missile program and all these things have enforced that discipline.

So, there is an issue of not just urgency and a desire, but there is an issue of skills and capability.

One thought could be that, for the Office of Homeland Security and perhaps even for this agency that might be created by such a bill as proposed here, you could have either a DARPA-like or a systems-engineering-like organization, a seat-like organization whose job it is to look at being sort of a central clearinghouse of requirements and standards so that you don't have to replicate the creation of something every police department in the Nation is going to need, you know, at every police department. So the thought of skills and methodology would be very helpful here as well.

Ms. JO ANN DAVIS OF VIRGINIA. Well, let me ask, on the Department of Homeland Security that is proposed, as I understand it, there is going to be one element that would analyze all the information. So if I am hearing you correct—all the information from, I guess, the FBI, everyone, I guess. If I'm hearing you all correctly, that wouldn't even be—I mean, it's not possible because we can't get the information to them; is that correct?

Mr. FITZGERALD. That's——

Ms. JO ANN DAVIS OF VIRGINIA. Is that what I'm hearing?

Mr. FITZGERALD [continuing]. Pretty much correct. Grants will be given by the Justice Department to local police departments to build systems, and then we will have necessary standards associated with those, so when the information that they gather is requested, it may not be able to be understood by the Office of Homeland Defense.

Ms. JO ANN DAVIS OF VIRGINIA. Thank you, Mr. Chairman. I think that is all I have.

Mr. TOM DAVIS OF VIRGINIA. Thank you very much.

Mr. Turner.

Mr. TURNER. Thank you, Mr. Chairman.

Dr. Sugar, talk to us a little bit about the problem that you mentioned briefly in your testimony that you had with the Postal Service on the liability issue for the anthrax, the detection equipment purchase.

Mr. SUGAR. Yeah. And, again, this is not the forum to talk about a very specific issue and a specific contract, but it does, I think, represent a problem we are all facing.

We have a system which we think can solve a problem. We had a certain quantity of these things planned to be ordered. We had to cut back that quantity because we were unwilling to take it past the stage of prototype demonstration until we were certain that putting it in the field, and if there were any unintended consequences, it would not come back and materially impact or financially destroy our company. That's really the situation.

Now, there is an indemnification, I guess the 85804, which is in place for—which is public law, which helps; it's nuclear and other identification, and that is very helpful. It is used certainly in all of our defense work.

What's not as clear is when we migrate the products to other civilian agencies, the State and local agencies or, frankly, even the private sector, for example, a private company that owns and operates a nuclear power plant and wants to utilize one of our great devices that one of our companies comes up with, how do you ensure that we're not going to end up, you know, having a situation where no good deed ever goes unpunished? We do something good, and we have something happen bad. It's a serious issue.

I'm not a lawyer, but I know that this is now becoming—emerging as a stumbling block on even the very few RFPs and programs we're seeing. I think you're going to see this become a very broad issue. It's going to become a policy issue for the Nation.

On the other hand, I would say that no Federal agency wants to take on unlimited liability that may be created by a contractor who provides a device which then reflects back on the government.

So we're going to have to find some way as a Nation to figure out how to share this so we can get on with applying technology correctly.

Mr. TURNER. So you're saying there's no statutory authority now for an agency to negotiate this issue of liability with a private sector vendor?

Mr. SUGAR. I think there is in some cases. I know, for example, with the U.S. Navy we can receive, because we build nuclear aircraft carriers, a nuclear indemnification as part of 85804. I'm not sure how widely that is allowed with other agencies or whether it, in fact, becomes a local decision of the contracting officer on any given procurement.

Mr. FITZGERALD. Capping liabilities would clearly be a step in the right direction.

Mr. TURNER. Thank you.

Mr. TOM DAVIS OF VIRGINIA. Thank you. I appreciate you raising the liability issue, because we don't think about that.

Many times as we go out to contracting and—government lawyers are trained to protect the government. If something goes wrong, it's the other guy's fault; and, of course, it has the end result of sometimes discouraging some of those innovative ideas, in-

novative companies, from doing business with the government. You get higher markups in the private sector, you know, why do you have to come here?

So I appreciate you raising that. I think we will take a closer look at that.

Any more specific examples that you can give to the subcommittee in terms of where that has been a deterrent or where maybe a company has in good faith provided a service and it went awry and they ended up losing their shirt? I know some State and local government instances of that, but at the Federal level that would be helpful to get it into the record so the members could understand why they're waiving something that otherwise it seems we wouldn't do. So I appreciate you raising that factor, and we'll take a closer look at that.

You know, virtually all of the private-sector witnesses here today have, in one way or another, expressed a concern about our ability to take advantage of the technology that the private sector has to offer. I think there's a great frustration at this point among companies who have invested in new ideas and think they can be of service, maybe make a profit along the way. But you have ideas that we're just not utilizing. What are the specific problems you face in getting that to market at this point?

Maybe this homeland security agency will be more of a clearinghouse. Maybe our legislation, if it is enacted, can at least give you some kind of organized route where you can pursue some of these. But do you have particular concerns regarding attacks on computer systems and infrastructure and intellectual property piracy issues?

Let me just try to hit those two offhand. Does anybody want to go——

Mr. FITZGERALD. Yeah, sure.

For Oracle Corp., I think our frustration comes in—we built systems specifically for the government for intelligence and defense purposes to share classified data, various classifications to audit all data to make sure we know who sees what. Once we spent the millions and tens of millions of dollars to build these systems, the government tends not to include them as part of the procurement process; and we sit there and scratch our heads at that. We've built a solution specifically to attack a problem like this, and then when it's waived or it's—agencies are given waivers around the policies associated with security and the sharing of classified data, we wonder why we spent the money to do it.

So I guess our situation is slightly different, Congressman Davis, in the sense that we stepped up the ante and put the money to do the development. Then we find that many agencies won't use what we've developed, and it's been developed for that purpose.

Mr. TOM DAVIS OF VIRGINIA. Let me ask—Mr. Pomata, let me ask you. You've been in the business a long time.

The Federal Government has a history of failed system development efforts. A lot of times we've spent a lot of money and we don't get what we want. It used to be that it was driven by the procurements itself, that we were so afraid of—once you'd go out with an RFP, you were so afraid of changing it even as your needs changed, because you'd have to go back out to the street. You're afraid of protests.

We've tried to loosen that up a little bit. I don't know how it's actually working, but we're trying to loosen it up a little bit so that the government buyers who know what they want can go off and they have GWACS and schedules and areas where they can go out and say, here's what we want, how do you provide it? And not have to go out the route we used to have to have.

Can you think of other steps that the government can take to ensure that systems that we get work properly? You've sat on the other side of this for years.

Mr. POMATA. I think a couple things. I think——

Mr. TOM DAVIS OF VIRGINIA. Go ahead.

Mr. POMATA. Did you——

Mr. TOM DAVIS OF VIRGINIA. No. I was going to go with you first.

Mr. POMATA. Sorry. One of the things I think of is that requirements need to be well defined. We know that. But as procurements progress, there are typically requirement changes. So there needs to be some flexibility on both sides to be able to understand as changes come up how to handle them.

The other thing we found is that a lot of the requirements in the IT world and a lot of the way procurements were proposed and executed was that, rather than utilize commercial standards, rather than utilize commercial off-the-shelf software, the government always insisted that they had unique requirements and that they had to be custom tailored to what they needed to do, as opposed to try to change some of the processes to conform and to use off-the-shelf software, a lower risk approach. So, typically, the risk is higher when you try to customize things.

Mr. TOM DAVIS OF VIRGINIA. And more expensive, too.

Mr. POMATA. And more expensive. And I think part of the solution there is for—even in homeland defense certainly there are mission-critical things that are going to be very specific and very important to the way the government needs to look at data and needs to do business, but I would suggest there are robust off-the-shelf technologies available that can be implemented quicker, faster and more—and cheaper into the systems at lower risks to solve the government's problem. I think we should look at that.

Mr. TOM DAVIS OF VIRGINIA. OK. Does anyone else want to add anything to that?

Mr. JOHNSON. Yes, I'd like to add a few things.

There are a couple of aspects that are common to many of the failures that we've seen. One is in some cases a lack of top leadership which can push down activity requirements and implementation across multiple stovepipes. In other words, without top management, emphasis on a major program of that size is typically doomed to failure.

A second one is there has to be a very strong government project manager and project team involved going forward, and oftentimes there's a shortage of those within government agencies.

A third one is that these large-scale systems and implementation efforts are certainly team approaches. They cannot be executed from an arm's-length arrangement between contractor and government agency. The team going forward needs to be effectively transparent and committed to the success of the program, rather than operating in an impeding communication kind of atmosphere.

Mr. TOM DAVIS OF VIRGINIA. OK. Anyone else on that?

Let me address the culture issues. Improving information sharing for homeland security is one of the largest changes to management initiatives I think that's ever been attempted. Many view the culture gap between the public and the private sectors as just a significant impediment to leveraging private sector management expertise to private and the information sharing that we need to get to. Any suggestions for bridging the gap?

Mr. FITZGERALD. Well, I think it's somewhat hard, because there's an arm's-length relationship between the government and the contractors on many of these projects. We all have to remember, at the same time, we all have the best interests of the country involved. We want to bring our skills to bear on these innovative solutions, as the bill you're sponsoring points out, and there has to be a little bit of a trust factor. I know trust is a difficult commodity to have between government and industry, but the stakes are very high.

Mr. TOM DAVIS OF VIRGINIA. Now, you all hire people who worked for the government to come work for you.

Mr. FITZGERALD. Yes.

Mr. TOM DAVIS OF VIRGINIA. They could have some knowledge to try to at least do translations and speak the language.

Mr. FITZGERALD. Yeah. And that does help, Congressman. But, again, there is still an insular attitude toward the private sector. So I think there just has to—and I'm not sure what the answer to that is. We really don't. We've all struggled with that. But I know from speaking with the other members with me today, I mean, we're all sitting here with one purpose. We are interested, we are capable, and we all believe in what we have ahead of us is a very important project.

Mr. TOM DAVIS OF VIRGINIA. Dr. Sugar, let me ask you a question. In your testimony, you talked about much of what Northrop Grumman has done for years and that the defense program area can be adopted for use domestically by State and even local organizations. In your experience, do the State and local organizations have the human resources needed to implement these programs?

Mr. SUGAR. Well, the fact is it varies, but generally not at the levels that you'd want. I think that the challenge here is to create standard solutions that we can replicate, that are easy to use, that we can also assist with training and to conduct exercises in standard ways so that you're not reinventing the wheel.

You know, if you think about it, we have 40 or 50 Federal agencies, 50 States and probably 200 cities of more than 100,000 or 200,000 people. So you can imagine that if everybody is trying to solve a problem like this, you might have 10,000, 50,000 solutions, and that is total chaos. And the irony is it's basically the same problem. It's the same problem being replicated.

So one value we could have here from your bill and from a central department is that a certain class of problems which are going to clearly be what you might call killer apps in the software business, where you have a standard need for a baggage detection or a standard need for a sniffer for biochem or something, can be identified. Requirements can be quickly finalized for it. RFPs can

go out. The best ideas from industry can be brought together, and that can become a standard solution.

It doesn't even necessarily have to be the same guy. It can be a standard set of specifications that apply; and as long as you comply with that you've got a qualified device that is homeland security, department-qualified, and that becomes the standard.

By the way, if that is used in some way which creates an unintended consequence but you did comply with this in good faith, you have some limitations around your liability. I think that is the way to address the issue of the training and viability for the people around——

Mr. TOM DAVIS OF VIRGINIA. We don't even have to legislate this. We're such a huge purchaser in the market that if we could keep our procurement needs consistent we would be able to define the marketplace. But we're not consistent. That's one of the problems.

Mr. FITZGERALD. In the granting process as well, too, because many of these systems will be purchased through grants from various agencies.

Mr. TOM DAVIS OF VIRGINIA. That's where Mr. Forman and the previous panel just need to step up. Still so often within agencies we're finding disparate ways to get there, and it's just not consistent. That really rings true.

Well, I want to thank you all. Those are all the questions I have.

Any other questions for the panelists?

I said I'd get us out at 12, and we're a few minutes late, but actually the questions took a little longer.

I think this has been a good panel and a very timely panel, and I appreciate the thoughtfulness and reflection that each of you have brought to this today.

Let me sum up. I'm going to enter into the record the briefing memo distributed to the subcommittee members.

[The information referred to follows:]

DAN BURTON, INDIANA,
CHAIRMAN

BENJAMIN A. GILMAN, NEW YORK
CONSTANCE A. MORELLA, MARYLAND
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
STEPHEN HORN, CALIFORNIA
JOHN L. MICA, FLORIDA
THOMAS M. DAVIS, VIRGINIA
MARK E. SOUDER, INDIANA
STEVEN C. LaTOURETTE, OHIO
BOB BARR, GEORGIA
DAN MILLER, FLORIDA
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
DAVE WELDON, FLORIDA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
C.L. "BUTCH" OTTER, IDAHO
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE

ONE HUNDRED SEVENTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051
TTY (202) 225–6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
PATSY T. MINK, HAWAII
CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
ROD R. BLAGOJEVICH, ILLINOIS
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, MAINE
JANICE D. SCHAKOWSKY, ILLINOIS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS

BERNARD SANDERS, VERMONT,
INDEPENDENT

SUBCOMMITTEE ON TECHNOLOGY AND PROCUREMENT POLICY

OVERSIGHT HEARING

"Meeting the Homeland Security Mission: Assessing Barriers to and Technology Solutions for Robust Information Sharing"

BRIEFING MEMORANDUM

June 7, 2002 at 10 a.m.

Room 2154 Rayburn House Office Building

Introduction

On June 7, 2002, at 10:00 a.m., in Room 2154 of the Rayburn House Office Building, the Subcommittee on Technology and Procurement Policy will conduct a hearing to continue its oversight of governmentwide information sharing issues in the wake of the September 11, 2001 terrorist attacks. The hearing will examine management and technology barriers to facilitating Homeland Security initiatives, and it will review government and private sector solutions to these barriers. It will also look at a problem discussed in the Subcommittee's February 26, 2002 hearing--the lack of a comprehensive process in the government to evaluate private sector solutions for achieving the homeland security mission.

Advances in information technology provide both public and private sector organizations with the tools to make great gains in productivity and efficiency. They also hold much promise for responding to terrorist threats and attacks. However, overcoming stovepipes of knowledge and a lack of coordination in the sharing of information from an inter- and intra-governmental perspective, as well as from agencies to employees, agencies to businesses, and agencies to citizens must be addressed. Despite longstanding efforts to improve cross-agency relationships, including information sharing, there has been relatively little success in developing systems that enable different departments and agencies to share their information with other entities in a predictable and rapid manner. Fortunately, the

Administration has devoted a significant percentage of increased spending in the FY 2003 budget for homeland security to information sharing. This hearing will assess how programmatic changes, management initiatives, and technology acquisitions can contribute to the better sharing of information.

Witnesses

The Subcommittee will hear testimony from the following witnesses:

Panel One

Randall Yim
Managing Director, National Preparedness Team
United States General Accounting Office (GAO)

Mark Forman
Associate Director, Information Technology and E-government
United States Office of Management and Budget (OMB)

Robert J. Jordan
Director, Information Sharing Task Force
Federal Bureau of Investigation (FBI)

George H. Bohlinger
Executive Associate Commissioner for Management
United States Immigration and Naturalization Service (INS)

William F. Raub, Ph.D.
Deputy Director, Office of Public Health Preparedness
United States Department of Health and Human Services (HHS)

Panel Two

Ronald D. Sugar, Ph.D.
President & Chief Operating Officer
Northrop Grumman Corp.

Leonard Pomata
President, Federal Group
webMethods, Inc.

S. Daniel Johnson
Executive Vice President, Public Services
KPMG Consulting, Inc.

Kevin J. Fitzgerald
Senior Vice President, Government, Education & Healthcare
Oracle Corp.

Background

After terrorist attacks of 9/11/01, there has been a sea change in the mission of government: the first priority of the nation has become homeland security (HLS). To win this fight against terrorism, Federal, state and local agencies must be able to effectively detect, prevent, and respond to terrorist activity. We also must be ready to manage the consequences of future attacks, treat casualties, and protect critical infrastructures.

Thus, defending America in the new war against terrorism will require every level of government to work together with citizens and with the private sector. Effective use of accurate information from divergent sources is critical to our success. More than ever, we are engaged in an information war. Indeed, in this war, our enemies are hiding in information across a spectrum of databases. They are obscured by stovepipes of knowledge. As we have seen, the terrorists of 9/11 generated transactions and data points across numerous systems—including visas, border crossings, traffic stops, cash transactions, airline tickets, and others. Looking forward from 9/11, we must concentrate on how to effectively "connect the dots" of the vast amount of information now available so that important pieces of information can be shared and appropriate actions can be taken to prevent terrorism.

The President, Governor Ridge and the Office of Homeland Security (OHS), and numerous federal, state and local agencies and task forces have accomplished much since September 11th. Perhaps most importantly, they have reassured a Nation in anguish over its loss and in anger over its vulnerability. They also have identified many of the impediments to better detection, prevention, and response to terror. In addition, OHS is planning three pilot projects that have potential for widespread impact in the near future—1) consolidation of the 55 watch lists of suspected terrorists; 2) creation of a HLS portal to streamline access to information; and 3) collecting publicly available information for use in the homeland security mission.

However, much remains to be done. Coordination of the widest possible range of infrastructures in both the public and private sector to establish homeland security communications, information sharing, and response procedures is a task of herculean proportions. Fortunately, America is up to the challenge. Pushing the right information to the right people at the right time is a task our Nation's IT companies and government agencies can accomplish.

Billions in funding already have been committed to fighting the war on terrorism. While new funding is certainly needed if the government is going to effectively modernize, share information, and win the war, we also need to continually evaluate the success or failure of our efforts to date, ensure that the private sector is our full partner,

and integrate definable performance metrics into our IT planning and spending. When it comes to the war on terrorism and protecting the homeland, Americans are not asking for more spending; they asking for more spending that works. Identifying our immediate, near term, and long-range HLS needs should be coupled with a process that keeps us focused spending money wisely.

Unfortunately, as Tom Siebel, a witness at the Subcommittee's February 2002 hearing said, "We are unaware of any organized, cohesive, comprehensive process within the government to evaluate private sector solutions to the problem of homeland security." The government in general and OHS in particular have been overwhelmed by a flood of industry proposals offering wide-ranging solutions to our homeland security challenges. Many technology firms with the expertise to address HLS needs have indicated they are having a hard time getting a real audience for their products, one that doesn't result in a virtual dead-end. Addressing the procurement challenges to achieving homeland security must be a priority so that we can leverage America's private sector innovation for the benefit of all Americans.

After the February hearing, I introduced legislation to facilitate private sector innovation in the fight against terrorism by establishing a new program at the Office of Federal Procurement Policy. HR 4629 would create an interagency team of subject matter experts to issue agency announcements seeking unique and innovative anti-terror solutions, screen and evaluate innovative proposals from industry, and send them to the proper federal agencies for action. This legislation would also launch a program offering monetary awards to companies with the best, most cutting-edge terror-fighting solutions. In addition, it would establish an acquisition pilot to encourage agency professionals to creatively use existing streamlined authorities to purchase commercial, off-the-shelf solutions and to test the applicability of waivers to speed up the contracting process.

Additionally, I applaud the Administration in its recent announcement that the White House Office of Science and Technology Policy will help facilitate this process by serving as a "clearinghouse" for the thousands of technology ideas submitted to the Office of Homeland Security. The Subcommittee also looks forward to reviewing the national strategy that OHS expects to issue in mid July. Hopefully, it will address the diverse threats we face, establish relevant national priorities and processes, incorporate flexibility for individualized responses, and enhance opportunities for the appropriate sharing of information.

Although we can never be 100% secure from attack, nor 100% prepared for any emergency, we can be better prepared and more secure. After 9/11, the value of hindsight and the urge to be "Monday morning quarterbacks" have led some to focus on what was missed by agencies rather on what can be done to proactively prevent future terrorist attacks. Instead, as Robert Gates, former head of the CIA, recently noted, what is needed is a thoughtful Congressional inquiry to identify the structural, technological, and bureaucratic impediments to information sharing and better coordination across the government.

The Subcommittee expects to hear testimony from government witnesses in key agencies about their agendas in the fight against terrorism, their plans for managing change to overcome stovepipes of information and distrust, their assessment of the barriers that exist to achieving Homeland Security initiatives, and their technology procurement needs for robust information sharing. It will also hear from some of the world's leading technology companies about how they can help address the homeland security mission and overcome these barriers.

Mr. TOM DAVIS OF VIRGINIA. We'll hold the record open for 2 weeks from today for those who want to forward submissions for possible inclusion. I suggest, with the delay of regular mail going in and out of the Capitol campus, that you e-mail these submissions to the attention of my counsel, George Rogers, and we'll get them in.

All right. Thank you very much. These proceedings are closed.

[Whereupon, at 12:12 p.m., the subcommittee was adjourned.]

○