AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

OUT OF MANY, ONE: ASSESSING BARRIERS TO INFORMATION SHARING IN THE DEPARTMENT OF HOMELAND SECURITY

HEARING

BEFORE THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

MAY 8, 2003

Serial No. 108–31

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

88–194 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

TOM DAVIS, Virginia, *Chairman*

DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
JOHN SULLIVAN, Oklahoma
NATHAN DEAL, Georgia
CANDICE S. MILLER, Michigan
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio
JOHN R. CARTER, Texas
WILLIAM J. JANKLOW, South Dakota
MARSHA BLACKBURN, Tennessee

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. "DUTCH" RUPPERSBERGER, Maryland
ELEANOR HOLMES NORTON, District of Columbia
JIM COOPER, Tennessee
CHRIS BELL, Texas

BERNARD SANDERS, Vermont (Independent)

PETER SIRH, *Staff Director*
MELISSA WOJCIAK, *Deputy Staff Director*
ROB BORDEN, *Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHILIP M. SCHILIRO, *Minority Staff Director*

CONTENTS

	Page
Hearing held on May 8, 2003	1
Statement of:	
Baroni, Greg, president, global public sector, Unisys Corp.; Steven Perkins, senior vice president, public sector and homeland security, Oracle Corp.; and Mark Bisnow, senior vice president, webMethods, Inc.	110
Cooper, Steven, Chief Information Officer, Department of Homeland Security; and Mark Forman, Associate Director, Information Technology, and e-Government, Office of Management and Budget	15
Dacey, Robert, Director, Information Security Issues and Information Technology Team, General Accounting Office; Randolph C. Hite, Director, Architecture and Systems Issues and Information Technology Team, General Accounting Office; and Charles Rossotti, senior advisor, the Carlyle Group, formerly Commissioner, Internal Revenue Service	49
Letters, statements, etc., submitted for the record by:	
Baroni, Greg, president, global public sector, Unisys Corp., prepared statement of	114
Bisnow, Mark, senior vice president, webMethods, Inc., prepared statement of	133
Cooper, Steven, Chief Information Officer, Department of Homeland Security, prepared statement of	17
Dacey, Robert, Director, Information Security Issues and Information Technology Team, General Accounting Office, prepared statement of	51
Davis, Chairman Tom, a Representative in Congress from the State of Virginia, prepared statement of	4
Forman, Mark, Associate Director, Information Technology, and e-Government, Office of Management and Budget, prepared statement of	28
Perkins, Steven, senior vice president, public sector and homeland security, Oracle Corp., prepared statement of	125
Towns, Hon. Edolphus, a Representative in Congress from the State of New York, prepared statement of	13
Waxman, Hon. Henry A., a Representative in Congress from the State of California, prepared statement of	9

OUT OF MANY, ONE: ASSESSING BARRIERS TO INFORMATION SHARING IN THE DEPARTMENT OF HOMELAND SECURITY

THURSDAY, MAY 8, 2003

HOUSE OF REPRESENTATIVES,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The committee met, pursuant to notice, at 10:05 a.m., in room 2154, Rayburn House Office Building, Hon. Tom Davis of Virginia (chairman of the committee) presiding.

Present: Representatives Tom Davis of Virginia, Shays, Duncan, Blackburn, Waxman, Maloney, Cummings, Tierney, Lynch, Ruppersberger, and Norton.

Staff present: Melissa Wojciak, deputy staff director; Keith Ausbrook, chief counsel; Jennifer Safavian, chief counsel for oversight and investigations; John Hunter and David Young, counsels; Robert Borden, counsel/parliamentarian; David Marin, director of communications; Scott Kopple, deputy director of communications; Ken Feng, investigator/GAO detailee; Teresa Austin, chief clerk; Joshua E. Gillespie, deputy clerk; David Rapallo, minority counsel; Earley Green, minority chief clerk; Jean Gosa, minority assistant clerk; and Cecelia Morton, minority office manager.

Chairman TOM DAVIS. Good morning. A quorum being present, the Committee on Government Reform will come to order.

I would like to welcome everyone to today's hearing on the Department of Homeland Security's efforts to integrate information systems and enhance information-sharing. Earlier this year, with the establishment of the Department of Homeland Security, 22 agencies and more than 170,000 employees, by last count, were consolidated under one new department. It would be a monumental challenge under any circumstance to integrate the disparate information infrastructures of that many government agencies manned by that many employees, but given the critical mission of this new department to protect the Nation against terrorism, this task takes on an unparalleled urgency.

DHS needs to develop and implement a strategic plan to carry out this vital mission, including the ability of the new department to obtain, analyze, and timely distribute essential and actionable information for Federal, State, and local government and private sector use. DHS must also develop and implement security and privacy safeguards, a capital planning and investment control process, programming, performance management, and risk management.

If a strategic plan to integrate information systems is effectively and efficiently implemented, we not only will achieve economies of scale, but also be better prepared to protect the Nation's physical and cyber infrastructure, secure our borders, counteract chemical and biological attacks, and respond to terrorist and natural disaster incidents.

But that is a considerable "if" that we are talking about. The obstacles facing DHS in effectively integrating information functions are formidable. As with the merger of any corporate or government entities, there are obvious challenges in integrating business functions such as payroll, human resources, and communications. But similar to the consolidation of the military service branches within the Department of Defense in 1947, DHS is faced with the need to integrate multiple agencies that have a common security mission, in addition to its many non-security functions.

DHS is further confronted with the task of communicating effectively with other Federal, State, and local entities, as well as the public. It is particularly critical that information be related to our first-responders at the State and local level. They are the front lines of our war against terrorism, and they need to be adequately informed to protect the public.

These challenges are not solely a factor of the new department's size or the magnitude of its mission. The fact is DHS inherited information-sharing problems that already existed within many of the agencies that now make up the new department.

For example, the General Accounting Office identified problems pertaining to terrorist watch lists, which are an integral part of our Nation's ability to secure its borders. The GAO found that the current approach to developing and using watch lists is diffuse and non-standard, and has resulted in nine agencies creating 12 different lists, largely because the lists were developed and have evolved in response to individual agencies' unique mission needs and cultural development.

The extent to which this information can be shared among Federal agencies and between the Federal Government and State and local entities is severely constrained by fundamental differences in the watch list items. These are by no means the only examples of opportunities to improve information-sharing, but they illustrate one of the primary reasons for integrating agencies that are vital to homeland protection under one department.

The Chief Information Officer in DHS is responsible for coordinating information-sharing nationwide and is doing so by creating a national enterprise architecture. This common element in improving information systems integration, according to both GAO and the Office of Management and Budget, seeks to ensure that, as the agencies within DHS invest in information technology and new management strategies, those strategies and technologies serve the overall plan and mission of the department as well as the Federal Government.

With a coordinated strategy for efficient information technology acquisition and implementation, mission-essential decisions can be based on more accurate information while requiring less time. Wise investment in interoperable information technology reduces unnecessary spending and redundant or stovepipe systems.

It took almost 40 years for the military service branches to be integrated effectively under the Department of Defense. With DHS, we simply don't have that kind of time. We are talking about protecting our Nation against very real terrorist threats. Congress must be assured that information integration standards and goals are defined, timely implementation of these benchmarks is achieved, and accountability is maintained.

Last week marked 100 days since the creation of the department. I guess they moved into the new headquarters. They just got the duct tape off the headquarters about 3 weeks ago, or whatever. We know it is a little late in starting. Part of that is our fault in the way of passing the bill and taking such a long time, but the need is urgent, the challenge monumental, and it may be later than we think.

Today we have assembled an impressive group of witnesses to help us understand the current status of information-sharing at DHS and its plans for the future. On the first panel we will hear from Steven Cooper, the CIO; Mark Forman, the Assistant Director of Information Technology and E-Government at the Office of Management Budget, and they will focus on the department's efforts to integrate information systems at DHS and the coordination of those efforts with OMB's governmentwide enterprise architecture.

The second panel will include Robert Dacey and Randolph Hite from the GAO, who will discuss GAO's analysis of the department's information-sharing integration. Also on that panel, the Honorable Charles Rossotti, the former Commissioner of the IRS, who will discuss his efforts to consolidate that agency's information technology functions.

In the third panel we will hear from the private sector, which is directly involved in the department's development. We will hear from Steve Perkins, senior vice president for public sector and homeland security for Oracle Corp.; Greg Baroni, president of global public sector for Unisys, and Mark Bisnow, senior vice president of webMethods.

I would like to thank all of our witnesses for appearing before the committee. I look forward to your testimony.

[The prepared statement of Chairman Tom Davis follows:]

TOM DAVIS, VIRGINIA,
CHAIRMAN

DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
STEVEN C. LaTOURETTE, OHIO
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE
JOHN SULLIVAN, OKLAHOMA
NATHAN DEAL, GEORGIA
CANDICE MILLER, MICHIGAN
TIM MURPHY, PENNSYLVANIA
MICHAEL R. TURNER, OHIO
JOHN B. CARTER, TEXAS
WILLIAM J. JANKLOW, SOUTH DAKOTA
MARSHA BLACKBURN, TENNESSEE

ONE HUNDRED EIGHTH 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
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER, MARYLAND
ELEANOR HOLMES NORTON, DISTRICT OF COLUMBIA
JIM COOPER, TENNESSEE
CHRIS BELL, TEXAS

BERNARD SANDERS, VERMONT,
INDEPENDENT

Opening Statement
Chairman Tom Davis
Committee on Government Reform
"OUT OF MANY, ONE: ASSESSING BARRIERS TO INFORMATION SHARING IN THE DEPARTMENT OF HOMELAND SECURITY"

May 8, 2003

Good morning. A quorum being present, the Committee on Government Reform will come to order. I would like to welcome everyone to today's hearing on the Department of Homeland Security's efforts to integrate information systems to enhance information sharing.

Earlier this year, with the establishment of DHS, 22 agencies and more than 170,000 employees were consolidated under one new department. It would be a monumental challenge under any circumstance to integrate the disparate information infrastructures of that many government agencies manned by that many employees. But, given the critical mission of this new Department to protect the nation against terrorism, this task takes on an unparalleled urgency.

DHS needs to develop and implement a strategic plan to carry out this vital mission, including the ability of the new Department to obtain, analyze, and timely distribute essential and actionable information for federal, state, and local government and private sector use. DHS must also develop and implement security and privacy safeguards, a capital planning and investment control process, program and performance management, and risk management.

If a strategic plan to integrate information systems is effectively and efficiently implemented, we not only will achieve economies of scale, but will also be better prepared to protect the nation's physical and cyber infrastructure, secure our borders, counteract chemical and biological attacks, and respond to terrorist and natural disaster incidents.

But that's a considerable "if" we're talking about. The obstacles facing DHS in effectively integrating information functions are formidable. As with the merger of any corporate or government entities, there are obvious challenges in integrating business functions such as payroll, human resources, and communications. But similar to the consolidation of the military service branches within the Department of Defense in 1947, DHS is faced with the need to integrate multiple agencies that have a common security mission, in addition to its many non-security functions.

DHS is further confronted with the task of communicating effectively with other federal, state, and local entities, as well as the public. It is particularly critical that information be relayed to our first responders at the state and local level. They are on the front lines of our war against terrorism, and they need to be adequately informed to protect the public.

These challenges are not solely a factor of the new department's size or the magnitude of its mission. The fact is, DHS inherited information sharing problems that already existed within many of the agencies that now make up the new Department. For example, the General Accounting Office identified problems pertaining to terrorist watch lists, which are an integral part of our nation's ability to secure its borders. The GAO found that the current approach to developing and using watch lists is diffuse and nonstandard, and has resulted in nine agencies creating twelve different lists, largely because the lists were developed and have evolved in response to individual agencies' unique mission needs and cultural development. The extent to which this information can be shared among federal agencies and between the federal government and state and local entities is severely constrained by fundamental differences in the watch list systems. These are by no means the only examples of opportunities to improve information sharing, but they illustrate one of the primary reasons for integrating agencies that are vital to homeland protection under one department.

The Chief Information Officer in DHS is responsible for coordinating information sharing nationwide, and is doing so by creating a national enterprise architecture. This common element in improving information system integration, according to both GAO and the Office of Management and Budget, seeks to ensure that, as the agencies within DHS invest in information technology and new management strategies, those strategies and technologies serve the overall plan and mission of the Department as well as the federal government. With a coordinated strategy for efficient information technology acquisition and implementation, mission-essential decisions can be based on more accurate information while requiring less time. Wise investment in interoperable information technology reduces unnecessary spending in redundant or stovepipe systems.

It took almost forty years for the military service branches to be integrated effectively under the Department of Defense. With DHS, we simply do not have that kind of time: we're talking about protecting our nation against very real terrorist threats. Congress must be assured that information integration standards and goals are defined, timely implementation of these benchmarks is achieved, and accountability is maintained.

Last week marked one hundred days since the creation of the Department. Now is the time for this Committee to review the status of the Department's efforts to integrate its information sharing functions; what obstacles the Department and other participants have identified and how those obstacles are being addressed; and when we can expect to see measurable progress in integration of information sharing. The need is urgent, the challenge monumental – and it may be later than we think.

We have assembled an impressive group of witnesses to help us understand the current status of information sharing at DHS and its plans for the future. On the first panel, we will hear from Steve Cooper, the Chief Information Officer of the Department of Homeland Security, and Mark Forman, Associate Director for Information Technology and E-Government at the Office of Management and Budget. They will focus on the Department's efforts to integrate

information systems at DHS and the coordination of those efforts with OMB's government-wide enterprise architecture.

The second panel will include Robert Dacey and Randolph Hite from the General Accounting Office, who will discuss GAO's analysis of the Department's information sharing integration. Also on that panel is The Honorable Charles Rossotti, former Commissioner of the Internal Revenue Service, who will discuss his efforts to consolidate that agency's information technology functions.

On the third panel, we will hear from the private sector, which is directly involved in the Department's development of information system integration. We will hear from Steven Perkins, Senior Vice President for Public Sector & Homeland Security for Oracle Corporation, Greg Baroni, President of the Global Public Sector for Unisys Corporation, and Mark Bisnow, Senior Vice President of webMethods, Inc.

I would like to thank all of our witnesses for appearing before the Committee, and I look forward to their testimony.

Chairman TOM DAVIS. I am going to yield to my ranking member, Mr. Waxman, for his opening statement.

Mr. WAXMAN. Thank you very much, Mr. Chairman. Thank you for calling this hearing, and I appreciate all the witnesses being present.

The General Accounting Office recently issued a report concluding that, 20 months after the attacks of September 11, the administration has yet to remedy one of the single most significant problems that led to those attacks, the failure to share critical terrorist information among Federal, State, local, and private entities.

As we now know, we were unable to prevent the attacks on the World Trade Center and the Pentagon in part, because the Federal agencies could not or would not share information. Not only did the Federal Government as a whole fail to connect the dots, but certain agencies wanted to maintain exclusive control over those dots.

One highly publicized example involved was the failure of the FBI and the CIA to share terrorist information about two suspects living in San Diego in 2001. Although several agencies possessed relevant information about the suspects, their locations and their contacts, they did not share it with other agencies that could have acted on it. To our great dismay, these terrorists went on to take part in the September 11 hijackings.

Today, however, despite repeated direction by Congress to consolidate these watch lists and despite promises by President Bush to do so, GAO's report concludes that the administration has failed to address this problem. Nine Federal agencies still maintain 12 different terrorist watch lists. While seven agencies have at least some sort of procedure for sharing information, two agencies have no procedure at all. Only half of these agencies share information with States, and only one-fourth share information with private entities.

According to GAO's investigation, Federal agencies received no direction from the White House on this issue. As a result, GAO reports that Federal agencies continue to develop their own watch lists in isolation from each other, and that information-sharing remains inconsistent and limited.

The administration's failure is magnified by the ping-pong approach it has taken to addressing this problem. First, the President's October 2001 Executive order initially assigned responsibility for ensuring the dissemination of terrorist information to the White House. Then, in the July 2002 National Strategy for Homeland Security, the President directed the FBI to take on this job. Then the White House apparently took back this function. Now, in the latest volley, officials from the new Department of Homeland Security claim they are working on it. This is not a recipe for success.

Perhaps most troubling, Mr. Chairman, is the White House's refusal to cooperate with GAO's investigation. When GAO tried to contact White House officials about their efforts to consolidate watch list information, they did not respond to GAO's inquiries.

As you know, this committee has had difficulties in the past with the White House Office of Homeland Security, even after Governor Ridge finally agreed to testify before us. This latest refusal by the White House continues to impede Congress' oversight abilities.

As a result of the White House's actions, GAO reported that it could not determine the substance, status, and schedule of any watch list consolidation activities. Mr. Chairman, how are we to do our job if the White House refuses to provide any information about the substance, the status, or the schedule of the administration's actions? I hope this hearing will be able to shed some light on these very important issues.

Mr. Chairman, I want to point out to the witnesses as well, we will be reviewing the testimony, and we have had a chance to review some of it in advance. I, unfortunately, because of scheduling conflicts, won't be here for most of the testimony that is given at the hearing.

Thank you.

[The prepared statement of Hon. Henry A. Waxman follows:]

Rep. Henry A. Waxman
Opening Statement

"Out of Many, One: Assessing Barriers to Information Sharing in the Department of Homeland Security"

House Committee on Government Reform
May 8, 2003

Mr. Chairman, thank you for calling this hearing, and thanks to all the witnesses for being here.

The General Accounting Office recently issued a report concluding that, twenty months after the attacks of September 11, the Administration has yet to remedy one of the single most significant problems that led to those attacks: the failure to share critical terrorist information among federal, state, local, and private entities.

As we now know, we were unable to prevent the attacks on the World Trade Center and the Pentagon in part because federal agencies could not, or would not, share information. Not only did the federal government as a whole fail to "connect the dots," but certain agencies wanted to maintain exclusive control over those dots.

One highly publicized example involved the failure of the FBI and the CIA to share terrorist information about two suspects living in San Diego in 2001. Although several agencies possessed relevant information about the suspects, their locations, and their contacts, they did not share it with other agencies that could have acted on it. To our great dismay, these terrorists went on to take part in the September 11 hijackings.

Today, however, despite repeated direction by Congress to consolidate terrorist and criminal watch lists, and despite promises by

President Bush to do so, GAO's report concludes that the Administration has failed to address this problem.

Nine federal agencies still maintain 12 different watch lists. While seven agencies have at least some sort of procedure for sharing information, two agencies have no procedure at all. Only half of these agencies share information with states, and only one fourth share information with private entities.

According to GAO's investigation, federal agencies "received no direction" from the White House on this issue. As a result, GAO reports that federal agencies continue to develop their own watch lists in isolation from each other, and that information sharing remains inconsistent and limited.

The Administration's failure is magnified by the ping-pong approach it has taken to addressing this problem. First, the President's October 2001 executive order initially assigned responsibility for ensuring the dissemination of terrorist information to the White House. Then, in the July 2002 National Strategy for Homeland Security, the President directed the FBI to take on this job. Then, the White House apparently took back this function. Now, in the latest volley, officials from the new Department of Homeland Security claim they are working on it. This is not a recipe for success.

Perhaps most troubling, Mr. Chairman, is the White House's refusal to cooperate with GAO's investigation. When GAO tried to contact White House officials about their efforts to consolidate watch list information, they did not respond to GAO's inquiries. As you know, this Committee has had difficulties in the past with the White House Office of Homeland Security, even after Governor Ridge finally agreed to testify before us. This latest refusal by the White House continues to impede Congress' oversight abilities.

As a result of the White House's actions, GAO reported that it could not determine "the substance, status, and schedule of any watch list consolidation activities." Mr. Chairman, how are we to do our job if the White House refuses to provide any information about the substance, the status, or the schedule of the Administration's actions?

I hope this hearing will be able to shed some light on these very important issues.

Chairman TOM DAVIS. Thank you very much, Mr. Waxman.
Any other members wish to make statements? Mr. Lynch.
Mr. LYNCH. I will pass, Mr. Chairman. Thank you, though.
[The prepared statement of Hon. Edolphus Towns follows:]

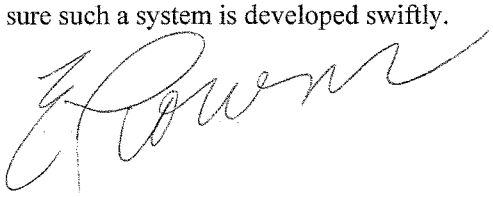
Congressman Ed Towns
Information Barriers to the Homeland Security Department
May 8, 2002

Thank Mr. Chairman for holding this important hearing. As a member of Congress who had constituents who lost their lives on 911, I know that there is no more important work than what we are doing here today.

The findings presented by the GAO on the lack of progress on an integrated, inter-agency terrorist watch list are troubling. Didn't 911 serve enough of a wake-up call to agency directors and employees that the old way of doing business no longer cuts it? I personally will not stand, and I am confident that this Committee and this Congress will not stand for an agency culture that impedes the sharing of terrorist watch lists and other critical information.

In addition to agency culture issues, there are clearly technology problems that need to be solved. Whether it's the White House Office of Homeland Security or the Department of Homeland Security, someone needs to take charge to develop this new information system.

I hope today's witnesses can shed light on why it has taken so long to develop the integrated information system that our nation needs, and what needs to be done to make sure such a system is developed swiftly.



Chairman TOM DAVIS. Well, let's move right on to our first panel. As you know, it is the policy of the committee, we swear in all witnesses. Will you please rise with me and raise your right hands?

[Witnesses sworn.]

Chairman TOM DAVIS. Thank you very much. I think we have your total testimony. We have already looked at it. We finished a markup at about 11 p.m., and then we went into your testimony and we are ready to grill you. So 5 minutes apiece.

You know the rules. The lights are here, and then we will get right into questions.

Thank you. Mr. Cooper, thanks for being here. We will start with you, and then I will go to Mr. Forman.

STATEMENTS OF STEVEN COOPER, CHIEF INFORMATION OFFICER, DEPARTMENT OF HOMELAND SECURITY; AND MARK FORMAN, ASSOCIATE DIRECTOR, INFORMATION TECHNOLOGY, AND E-GOVERNMENT, OFFICE OF MANAGEMENT AND BUDGET

Mr. COOPER. OK, thank you very much and good morning, Mr. Chairman and members of the committee. I would like to submit my written testimony for the record.

Chairman TOM DAVIS. It is all in the record. Thank you.

Mr. COOPER. OK. Now I would like to offer a brief oral statement and share with the committee a little bit of what we have been doing since January 24 of this year, when the legislation enacted the Department of Homeland Security. I am very pleased to appear before the committee to discuss activity from that date and to discuss an overview of the role and responsibilities that I have as the Chief Information Officer of the new Department of Homeland Security.

Since January, we have been very focused for January, February, and most of March, on day one, what we call "day one activities," to actually establish the new Department of Homeland Security. The new department, actually, the headquarters personnel had no facilities. They weren't actually employees of the department, and from an information technology enablement standpoint, there was an awful lot of work that had to be done.

We actually have done some very major work and accomplished some very major things, the first of which and foremost is that we had no infrastructure, we had no network, we had no capability to communicate among ourselves and with the rest of the world. So we did, in time and very short notice, implement our wide area network to connect our multiple locations and to connect us to the outside world, our sister Federal agencies, State and local and tribal governments and, as appropriate, enable communications with the critical infrastructure owned by the private sector.

We also implemented our dhs.gov Web site, so that we had a way for the public to actually access a little bit of what we were doing and understand some of our goals and objectives. That is up; that is operational.

Internally, we implemented a portal to enable our headquarters personnel initially, and now the 170,000 employees that comprise the new department, to actually be able to communicate via an online, DHS online, intranet portal with collaboration capability. We

implemented desktop capability, local area network capability across the multiple facilities that we now occupy as a headquarters entity.

Then, finally, but not least, we actually have enabled e-mail connectivity across our 170,000 employees, including the new agencies that have become part of the department. It is not something that is necessarily visible, but it is something that took a lot of work and a lot of time.

Once we accomplished that, our focus reshifted to our enterprise architectural activity. We actually had begun an awful lot of enterprise architectural activity for homeland security when I was in the White House Office of Homeland Security, working very closely with the Federal Enterprise Architecture Program Office and team, headed by Norm Lorentz and Bob Haycock, and working closely with Mark Forman.

What we have done is to continue to map out the enterprise architecture targets, framework, deliverables. Those are outlined in my written testimony. I would be happy to respond to questions if there are questions related to the detail about those things.

But the enterprise architecture, quite simply, for those who may not be as familiar with it, is an architectural framework; it is a decisionmaking framework at its highest or starting component. It is first and foremost about the business strategy.

From the business strategy, we began with the National Strategy for Homeland Security, released by the President last summer, to then drive down into the business processes that the new department has responsibility for, the functional responsibilities like prevention, detection, protection, alerts and warnings, incident management, crisis management, communication, response, and recovery.

We identified, and continue to identify, the information necessary to carry out these processes and functions. Those three components—the strategy, the business layer, and the information layer—comprise what we call the business architecture. Then behind that or supporting that we have the information technology architecture, which automates and enables the achievement of business goals, objectives, and metrics.

That information technology architecture is comprised primarily of a couple of layers, the first being applications and/or decision support systems. These are the various automated applications, programs, initiatives that support all of the mission capability, enterprise activity.

Then, last, we have the information technology infrastructure upon which all of this rides. The infrastructure is pretty much like the electric lights in a building: You flip the switch; the lights come on; you're happy. You never see it unless it doesn't work. Then we jump in and we fix it.

I will stop there. Thank you, and I will be responding to any questions that you might have.

[The prepared statement of Mr. Cooper follows:]

Statement of
Steven I. Cooper
Chief Information Officer
Department of Homeland Security

before the

Committee on Government Reform
House of Representatives
May 8, 2003

Mr. Chairman and Members of the Committee:

I am pleased to appear before the Committee today to discuss information integration at the Department of Homeland Security (DHS). First, I want to thank the Chairman and the other members of the Committee for your leadership in the strategic use of information technology in the federal government and in homeland security. These strategic investments will improve the performance and accountability of the federal government as a whole, and homeland security, specifically. Information is a vital foundation for the Department's operations and consequently for improving our Nation's homeland security.

I have served as the Chief Information Officer (CIO) for DHS since its inception January 24, 2003. In this role, I provide strategic direction and oversight for information technology programs within DHS. From February 2002 until the formation of DHS, I served as a Special Assistant to the President and Senior Director for Infrastructure Integration for the White House Office of Homeland Security.

The *National Strategy for Homeland Security* set forth a vision to mobilize and organize our Nation to secure the U.S. homeland from terrorist attacks. This document identified three strategic objectives of homeland security:

- Prevent terrorist attacks within the United States;
- Reduce America's vulnerability to terrorism; and
- Minimize the damage and recover from attacks that do occur.

As stated in the *National Strategy*, although American information technology is the most advanced in the world, our country's information systems have not adequately supported homeland security missions. Databases used for law enforcement, immigration, intelligence, public health surveillance, and emergency management have not been integrated in ways that allow us to comprehend each other's data or "connect the dots" to better prevent terrorist attacks and protect our people and infrastructure from terrorism.

Technologies and cultures of agencies have to "Islands of Technologies" and barriers to information integration. We must leverage cultural beliefs and diversity to achieve collaborative change while at the same time consolidating redundant or duplicative efforts. In addition, there are deficiencies in the communications systems used by Federal, State and Local entities, and most state and local first responders do not use modern, compatible wireless communications equipment. To secure the homeland better, we must link the vast amounts of knowledge residing within each government agency while ensuring adequate privacy.

Information Sharing is a key foundation that cuts across all mission areas, all levels of government, and all sectors of our society. The *National Strategy for Homeland Security* identifies five major initiatives:

- Integrate information sharing across the federal government;
- Integrate information sharing across state and local governments, private industry, and citizens;
- Adopt common "meta-data" standards for electronic information relevant to homeland security;
- Improve public safety emergency communications; and
- Ensure reliable public health information.

We must put in place mechanisms that provide the right information to the right people in a timely manner.. With the use of information technology, homeland security officials throughout the United States will have a more complete, common awareness of threats and vulnerabilities as well as knowledge of those personnel and resources that are available to conquer those threats. Officials will receive actionable information they need from all levels of government and the private sector so that they can anticipate threats and respond rapidly and effectively. This information integration will better enable officials to protect the physical and cyber infrastructure, secure our country's borders, prevent biological or chemical attacks, and provide an effective first response to a terrorist or natural disaster incident.

Our vision is to ensure a world-class information management infrastructure that provides *timely, accurate, useful, and actionable information* to all individuals who require it.

This strategy and vision will be enabled by a disciplined **capital planning and investment control process** guided by a business-driven **enterprise architecture**.

INVESTMENT REVIEW PROCESS

In July 2002, under direction of the Office of Management and Budget in consultation with the White House Office of Homeland Security, an Information Technology Review

group was formed to review all IT investments over $500,000 for infrastructure or business applications by agencies that had been identified to move into the proposed Department of Homeland Security. This early start at investment review allowed early implementation of decisions to foster a migration from "bureau-centric" investments to "Department-level" investments. Actions to date have saved over $20 M, due to three Enterprise-wide software agreements.

With the formation of DHS in March 2003, information technology investments, including mission-specific investments, are now receiving a department-wide review. Information integration will be one of the benefits of the capital planning and investment and control process. Each investment is reviewed to ensure alignment with business process, consistency with technical frameworks and standards, and use of DHS-wide "meta data". This review process will identify and eliminate duplication of applications, gaps in information or misalignment with business goals and objectives.

ENTERPRISE ARCHITECTURE

In July 2002, we began to develop a business-driven Homeland Security Enterprise Architecture. Architecture working groups were established to collect, organize and publish the "as is" architecture for the major components proposed to come to DHS. Using this baseline information, we developed harmonized concepts of operation for use by DHS transition teams. The "as is" architecture for DHS is about 70 % complete. An inventory of "as is" applications is also about 70% complete. This inventory contains approximately 100 major applications and over 2,000 IT applications. The final DHS "as is" architecture and inventory will be completed in June 2003. During the process, the technical reference model for each DHS component will be collected, compared and evaluated. Information technology solutions will be grouped into the following categories: Nearly 100% commonality; roughly 80% commonality; and little commonality.

Analysis has already led to--

- Enterprise-wide software licensing efforts within the department, linked to the President's E-Government initiative across the federal enterprise;
- Identification of areas where a common technical solution could be rapidly selected and deployed; and
- Identification of instances where additional analysis is needed before enterprise technical solutions are possible.

The "to be" DHS architecture will be developed over this summer based on the business strategies of the DHS mission elements and on information technology opportunities. The initial "to be" architecture will be completed in August 2003.

Once we have formulated our "to be" architecture, we can develop the migration strategy needed to move from where we are today to where we want to be as a department. We plan to develop a plan, or road map, that provides a phased approach to achieving the "to be" architecture by fall 2003. We plan to initiate a competitive procurement in May 2003 for support of this architecture effort.

To better address horizontal information integration, DHS has coordinated its enterprise architecture development with other key Federal agencies, including the Departments of Justice, Energy and Defense, and the Intelligence Community. To address vertical information integration, DHS included National Association of State and Local CIOs (NASCIO) in our architecture development efforts through several coordination workshops. These relationships will continue during the development of the "to be" architecture and as we execute our roadmap.

INFORMATION TECHNOLOGY PRINCIPLES

We developed a modest set of information technology principles to both guide our initial investment decisions and our development of the "to be" enterprise architecture vision. Some of these principles reflect best practices successfully used in both industry and government. A few key principles include--

1. A proper balance of security and privacy. Implementations must ensure adequate and appropriate protection of legal civil liberties, and processes must be established to ensure information is accurate and privacy is protected. At the same time, information integration must be exploited to significantly improve our nation's homeland security.
2. Information systems should be built once and re-used within other DHS domains. Information should be captured once and re-used for multiple purposes.
3. The strategic, operational and governance activities of the department's Information Technology functions should be organized to ensure alignment with the business strategies of the department and its organizational elements.
4. Information Technology functions should use a balanced scorecard to guide and measure progress among and across the IT function.
5. Data and information generated by the department's organizational elements are the property of the department. These assets will be secure and available to those who have a legitimate need to use them.
6. We will deploy solutions that maximize value in support of mission and department objectives, using commercial off-the-shelf products and software wherever possible.
7. We should adopt common meta-data standards for homeland security information within DHS and promote common meta-data standards among key federal, state, local, and industry partners.
8. We should embrace open standards and non-proprietary approaches whenever possible.

INITIATIVES IN INFORMATION SHARING

Several key information-sharing initiatives have been initiated to address critical homeland security information sharing needs.

Events of September 11, 2001, reinforce the need to share and provide actionable information. "Watch" lists contain information on terrorists that support a variety of homeland security missions. As part of the transition process, we began to identify and begin the integration of "watch" lists within the Federal government. Eleven lists were identified in the "as is" inventory. Virtually all lists derive from one database. A plan to improve the dissemination of information from this database at three levels of classification has been developed, including a concept of operations, phasing and technical approach. Clearly we need to work with the other federal agencies involved with watch lists to address possible issues of redundancy and duplication.

In March 2003, a policy and technical framework to promote information sharing among the Department of Justice, the Intelligence Community and the Department of Homeland Security was completed that provides a framework for implementing an integrated "watch" list. Additionally, in collaboration with the Department of Justice, DHS has supported the extension of law enforcement information sharing networks such as the Regional Information Sharing Network (RISSNET) to provide a distribution channel for law enforcement homeland security information.

In another project, DHS has been working with "best of breed" regional information sharing groups such as the Emergency Response Network of Dallas, Texas (ERN), to provide homeland security information to a broad cross-section of first responders. We have connected the Department's Homeland Security Center to the ERN as a pilot for information exchange with State and Local governments, and with private sector critical infrastructure.

The Emergency Preparedness and Response component of DHS is providing secure video conference capability to governors and emergency response centers for each of the 56 states, territories or protectorates. These videoconference capabilities will support communication and information sharing of sensitive information with the states and territories. DHS is also the managing partner for the Disaster Management E-Gov Initiative, a Presidential Management Agenda program designed to provide an easy to use, unified point of access to disaster management knowledge and services. The program has a portal, tools for responders, and an interoperability backbone.

Utilizing lessons learned from the private sector on the importance of communication, DHS has implemented a single external portal, and a single internal portal, to provide for effective and consistent communications external to DHS and also internally to DHS employees. In addition, with little lead time, DHS has deployed DHS desktop server and

office environments for all DHS Headquarters personnel. We are implementing a secure intranet to all 170,000 DHS employees with a single "meta" directory for all DHS employees. The intranet provides all DHS employees with access to the internal portal and collaboration suite of tools and the ability to receive and send e-mail messages with the simple dhs.gov address.

INFORMATION SHARING STRATEGY

Major objectives of our information sharing strategy include--

- Successful delivery of major Departmental IT initiatives. Information sharing will be achieved through data consistency (shared definitions of basic business objects such as "person" or "incident"). The DHS/CIO is supporting development of standardized data definitions to enable effective information sharing.
- Aggressive identification of opportunities for enterprise solutions and infrastructure investments at the department level. Examples include Targeting, Case Management, Intelligence Analysis, Infrastructure, Financial, Human Resource Management, Portal and Content Management, Geospatial, and Smartcard/Authentication.
- Information technology investments will be evaluated and managed using a balanced scorecard. Balanced scorecards are a strategic tool for managing IT projects, enabling the translation of mission and strategy into tangible objectives and measures using common, shared definitions, tools, and products. IT projects submitted to DHS require the inclusion of balanced scorecards. The four perspectives of the DHS balanced scorecard ensure we meet our mission strategy and align our IT functions:

  - *Customer:* Focuses on identifying the customer and measures associated with value provided to the customer, customer satisfaction, etc.
  - *Financial:* Focuses on readily measurable economic consequences of actions already taken.
  - *Internal Business Process:* Focuses on the internal processes that will have the greatest impact on customer satisfaction and achieving the business unit's financial objectives.
  - *Learning and Growth:* Focuses on the people, systems, and organizational procedures that are critical to building long-term organizational growth and improvement.

CONCLUSION

DHS remains in the early stages of the development of its enterprise architecture and use of capital planning and investment control. Even now though, and clearly into the future, these tools are being used to guide the development of DHS and the related foundational

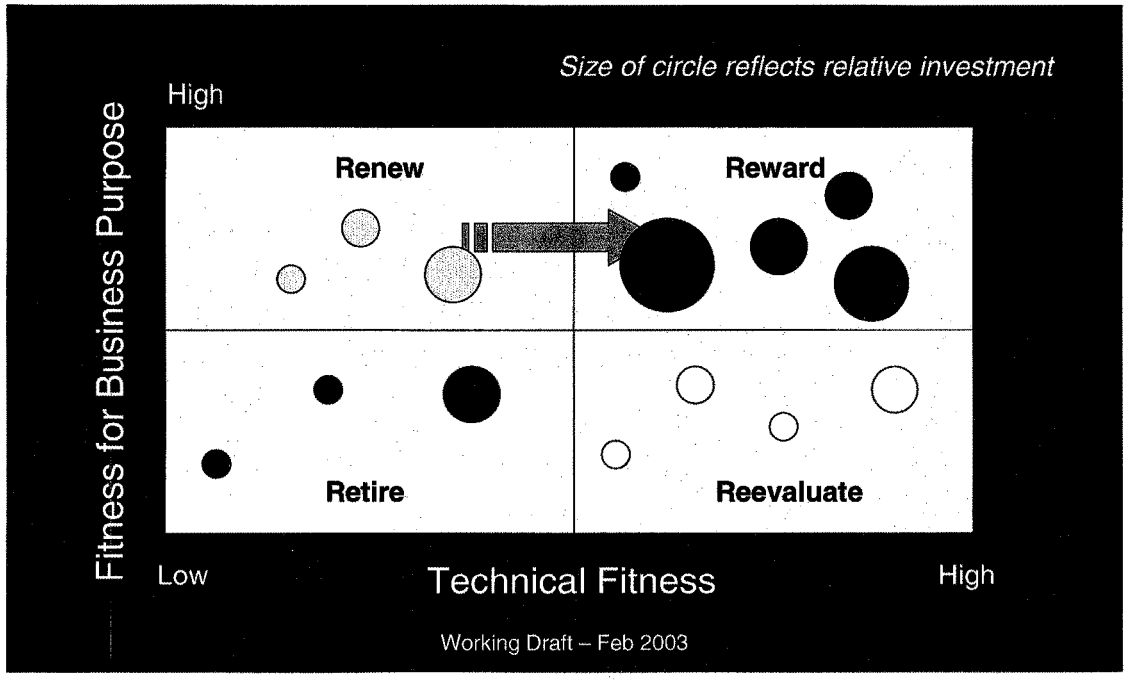
effort associated with information integration. DHS is committed to using the enterprise architecture to guide information sharing investment decisions.

We offer four final observations for your consideration:

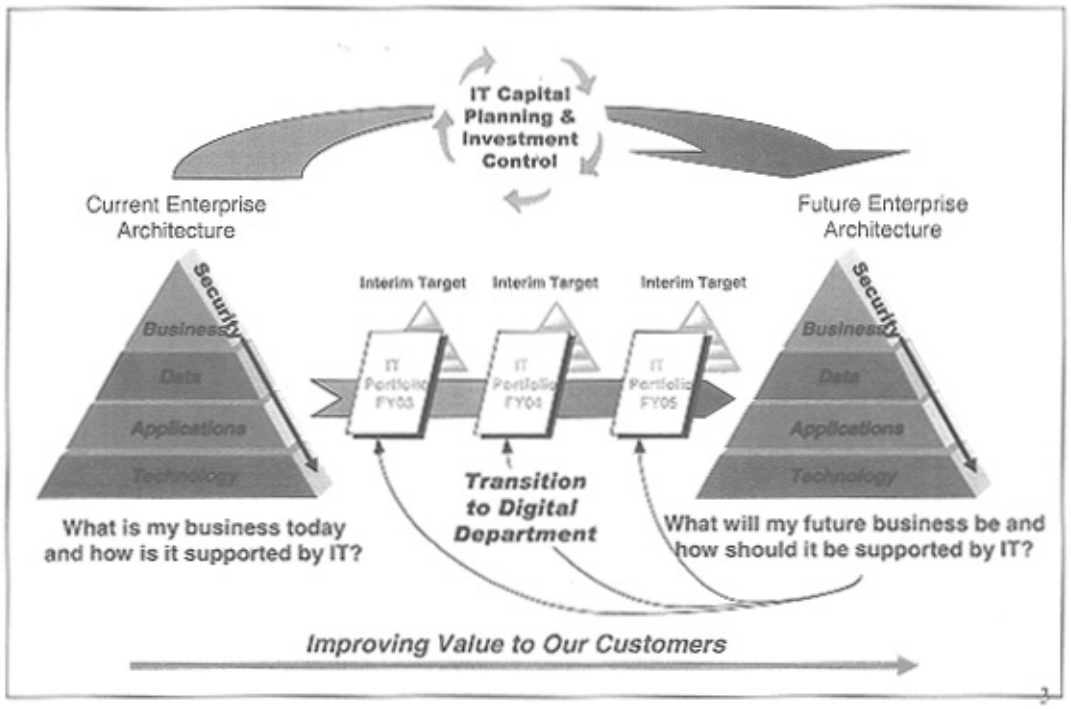
- First, information sharing is fundamental to the achievement of homeland security mission.
- Second, DHS will aggressively develop and use a capital planning and investment control process to guide information integration investments.
- Third, DHS will aggressively develop and use a "to be" enterprise architecture to guide information integration efforts.
- Fourth, DHS will continually strive to be one unified department and resist compartmentalization.

There is significant momentum in the DHS for the use of enterprise architectures to promote information integration. With the support of the Congress, this momentum can be sustained and will help ensure that enterprise architectures play a major role in improving the performance and accountability of IT investments at both the department and government-wide levels.

Portfolio Management



The Elements of Transformation: All major functional areas are addressed in an integrated, coordinated manner



Chairman TOM DAVIS. Thank you very much.

Mark, welcome back.

Mr. FORMAN. Thank you, Mr. Chairman and members of the committee. This is my first hearing as Administrator for E-Government and Information Technology, under legislation that the chairman sponsored. So it is good to be here in that role.

Chairman TOM DAVIS. Did you get a pay raise with that?

Mr. FORMAN. No.

Chairman TOM DAVIS. OK. You got a fancy, new title anyway. [Laughter.]

Mr. FORMAN. And some additional responsibilities and accountabilities.

Thank you for inviting me to discuss the administration's work in homeland security. Mr. Chairman, making organizations share information is like trying to glue together thousands of puzzle pieces. If the pieces are put together correctly, you get a pretty picture. If you just apply the glue without an orderly approach to building the puzzle, you could end up with something quite messy.

Bringing together 22 previously separate agencies and offices under one department requires more architecting than merely gluing together all of their IT. The administration uses best practices in e-business and IT management to assist in setting priorities and defining an action plan.

Last June, the President stated, "Development of a single enterprise architecture for the Homeland Security Department will result in elimination of the suboptimized, duplicative, and poorly coordinated systems and processes that are prevalent in government today."

Indeed, the administration believes that DHS leadership should use enterprise architecture analysis to integrate homeland security business processes and organizations, with IT being the key enabler. As identified in the National Strategy for Homeland Security, Federal homeland security IT investment should first improve response time, the time to detect and respond to potential threats, and, second, improve decisionmaking: making sure that we get the right decisions at the right time.

Achieving significant improvement requires significant change in longstanding organizations, their processes, information flows, and IT investments. OMB provides guidance and works with Federal agencies to ensure that the Federal Government applies best practices in IT management. Through traditional budget and management processes, we hold all agencies accountable for meeting statutory and policy requirements.

Four key elements are: first, enterprise architectures. An enterprise architecture describes how an organization performs its work using its people, its business processes, data, and technology. By aligning organizations, business processes, information flows, and technology, enterprise architecture tools are used to build a blueprint for improving efficiency and effectiveness of an organization. We are actively working with the department to ensure that they develop a comprehensive enterprise architecture that optimizes existing investments inherited from the legacy agencies.

Second, managing and budgeting IT investments. OMB IT management, OMB Circular A–130, and the budget, OMB Circular A–

11, provide guidance on information-sharing on a system-by-system basis through the agency budget request or business case for each IT investment. We are working with all agencies to ensure that they appropriately leverage and consolidate their IT investments: infrastructure, business management systems, and mission-related IT within and across their directorates.

In particular, the merging of 22 previously separate agencies has resulted in the Department of Homeland Security inheriting a number of redundant and overlapping IT systems and processes. The Director of OMB, in Memoranda M02–12 and M02–13, issued guidance under the Clinger/Cohen Act on consolidating and integrating IT investments across agencies performing homeland security missions. Through the fiscal year 2005 budget process, OMB will work with the department to eliminate redundant and non-integrated operations, systems, and processes for business and mission areas.

Third, e-government initiatives. As you know, the administration has been aggressively working over the past year and a half in the development and implementation of 24 governmentwide Presidential e-government initiatives. Implementation of the President's e-government initiatives related to homeland security will overcome information-sharing difficulties between Federal, State, and local organizations and first-responders.

In addition, many of the other Presidential e-government initiatives provide solutions that must be adopted by all departments, including the Department of Homeland Security. These initiatives include e-authentication as well as new, line-of-business consolidation initiatives on public health information.

Two of the President's initiatives I would like to point to in particular: Project SAFECOM and Disaster Management, which directly support and promote improving information-sharing between Federal, State, and local first-responders. I go in more detail in my written testimony on the content of those specific initiatives.

As managing partner, DHS is responsible for ensuring the accuracy of the business case for these initiatives, submitting the business cases to OMB, and ensuring management of the project to achieve cost, schedule, and performance goals for the implementation of the operations phase.

The fourth area is the President's Management Agenda. OMB monitors agency IT and e-government progress on a regular basis through the President's Management Scorecard under the expanding e-government score. Because the Department of Homeland Security is new, its status is scored as red. Again, I discuss that more in my written testimony.

Let me conclude by saying that achieving true homeland security will require IT investments to significantly improve response time and decisionmaking. While we recognize the department is currently grappling with cultural legacies of 22 component agencies, we fully expect that DHS leadership will continue to build an integrated and interoperable structure, resulting in a business-driven enterprise architecture that reflects the President's vision of eliminating suboptimized, duplicative, and poorly coordinated systems.

Thank you.

[The prepared statement of Mr. Forman follows:]

STATEMENT OF

MARK A. FORMAN

ADMINISTRATOR, OFFICE OF ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY

OFFICE OF MANAGEMENT AND BUDGET

BEFORE THE

COMMITTEE ON GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

May 8, 2003

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me to discuss how the Administration is working to improve Homeland Security through improved Federal IT management, including improved coordination and elimination of redundant IT investments, E-Government efforts, and use of enterprise architectures (EA).

Mr. Chairman, making organizations share information is like trying to glue together thousands of puzzle pieces. If the pieces are put together correctly, you get a pretty picture. If you just apply the glue without an orderly approach to building the puzzle, you could end up with something quite messy that doesn't look at all like the real picture. One of the challenges for the Department of Homeland Security is to get better results from available information. The need is not about connecting dozens of overlapping databases, but bringing order and structure to homeland security efforts by eliminating redundant systems, developing information sharing solutions, and making it all work together. As laid-out in the President's Management Agenda initiatives for E-Government and Information Technology, we believe we can obtain measurably better results in mission critical areas by simplifying and unifying organizations, processes, and information technology.

Bringing together twenty-two previously separate agencies and offices under one Department requires more architecting than merely gluing together all of their IT. As recognized by the Chairman's invitation letter, interoperability needed for Homeland Security must extend beyond information sharing. The Administration uses best practices in e-business and IT management to assist in

setting priorities and defining an action plan. Last June, the President's proposal for the Department of Homeland Security highlighted the use of EA techniques to improve both sharing and use of information. The President stated: "Development of a single enterprise architecture for the department would result in elimination of the sub-optimized, duplicative, and poorly coordinated systems <and processes> that are prevalent in government today. There would be rational prioritization of projects necessary to fund homeland security missions based on an overall assessment of requirements rather than a tendency to fund all good ideas beneficial to a separate unit's individual needs even if similar systems are already in place elsewhere."

Indeed, the Administration believes good EA analysis is needed to build integrated business processes and organizations. To be an effective tool, the EA has to reflect organizational decisions made by agency leadership and be owned and used by agency leadership in making resource decisions. Agency decisions must reflect the key elements of the President's Management Agenda, optimizing performance while trading-off human capital, IT and other resources. As identified in the National Strategy for Homeland Security, there are two primary measures of performance to be used in the federal homeland security IT initiatives: (1) improving response time - the time to detect and respond to potential threats; and (2) improving decision-making - making the right decisions at the right time. All homeland security IT investments must accelerate our response times and improve our decision making, and doing so requires significant changes in long-standing organizations, processes, information flows, and IT investments.

Mr. Chairman, as we have discussed before, there are a number of issues that must be addressed to get value from the Department of Homeland Security's IT investments. At a minimum we have identified agency culture, public trust, resources, stakeholder resistance, and lack of both a Federal EA as well as individual agency EAs as all potential barriers to be overcome through effective management of IT resources.

Improving Agency use of Information and IT

OMB provides guidance and works with Federal agencies to ensure that the Federal government applies best

practices in IT management. Through traditional budget and management processes, we hold all agencies accountable for meeting the statutory and policy requirements defined below. Four of the key components are:

1. Enterprise Architectures.

An EA describes how an organization performs its work using people, business processes, data, and technology. By aligning organizations, business processes, information flows, and technology, EA tools are used to build a blueprint for improving efficiency and effectiveness of an organization. OMB operates the Federal Enterprise Architecture Program Management Office, created last year, to work with Federal agencies in developing a government-wide EA. The FEA is a business-focused framework developed for OMB, federal agencies and Congress to use in improving the performance of government.

The FEA framework addresses five important areas of enterprise architecture, tying together the business, performance, service, technology, and data layers.

Through the *Business Reference Model (BRM)* we identify the Federal government's business operations and the agencies that perform them. This information helps to prevent potentially redundant IT investments in the Federal government's business lines, ultimately resulting in cost savings and productivity growth. *Version 2.0* of the model will be released later this month for all agencies to use in the FY 2005 budget formulation process.

The *Performance Reference Model (PRM)* is a framework that agencies will use to link IT investments to mission performance measures. The model allows OMB and agencies to identify common measurements and set baselines and targets. OMB has released the Working Draft PRM for Federal agency review and comment.

The *Service Component Reference Model (SRM)* provides the foundation for the re-use and sharing of IT across Federal agencies, and potentially across Federal, state and local governments.

The *Technical Reference Model (TRM)* outlines the technology elements that support the service components. The TRM will be used to facilitate both interoperability and the transition to e-government by reducing the complexity and isolated nature of many Federal systems, encourage the sharing of infrastructures across agencies, and reduce IT costs.

The *Data and Information Reference Model (DRM)* will provide a consistent framework to characterize and describe the data that supports Federal business lines. This will promote interoperability, as well as the horizontal and vertical sharing of information. OMB is working collaboratively with a small group of interested Federal agencies to define and validate the model, and a draft will be released soon for agency review and comment soon.

In addition, OMB and the Federal CIO Council are developing the Federal Enterprise Architecture Management System (FEAMS). FEAMS is a web-based tool to enhance FEA analysis and maintenance, and agencies' capital planning and investment control efforts. In addition to storing the FEA reference models, FEAMS will include general information on agencies' IT initiatives.

We are actively working with the Department to ensure that they develop a comprehensive EA that optimizes the existing investments inherited from the legacy agencies. This includes identifying redundant investments, developing new solutions, and linking together existing systems.

2. Managing and Budgeting IT Investments

OMB IT management (OMB Circular A-130) and budget (OMB Circular A-11) guidance addresses information sharing at a system by system basis through the agency budget request or business case for each IT investment. We are working with all agencies to ensure that they appropriately leverage and consolidate their IT investments (infrastructure, business management systems, and mission-related IT) within and across their directorates.

In particular, the merging of twenty-two previously separate agencies has resulted in DHS inheriting a number of redundant and overlapping IT systems and processes. The Director of OMB, in Memoranda M-02-12 and M-02-13, issued guidance under the Clinger-Cohen Act on consolidating and integrating IT investments across agencies performing homeland security missions. Through the FY 2005 budget process, OMB will work with the Department to eliminate redundant and non-integrated operations, systems, and processes for business and mission areas. Through consolidated business cases, the relevant systems for consolidation are listed, plans for migration and elimination are reported, and an integrated business process identified. Additionally, each business case must identify specific performance measures - how are we

advancing our homeland security goals through the requested investment, what performance improvement will we achieve? IT investments that support homeland security missions must be appropriately integrated in order to leverage technology for mission effectiveness while preventing redundant investments and wasted resources.

Additionally, I would like to highlight recent guidance issued by the Director of OMB to Federal agencies on planning for the President's FY 2005 Budget Request. To further strengthen IT and E-Government efforts, Federal agencies were instructed to ensure that IT budget information is fully integrated with each FY 2005 budget request justification, demonstrate solid business cases for IT projects, and identify all IT investments within their budget request. DHS will be held to this standard like any other Department. We are working with them to strengthen the use of IT in homeland security efforts.

3. E-Government Initiatives.

As you know, the Administration has been aggressively working over the last year and a half in the development and implementation of twenty-four government-wide Presidential E-Government initiatives. Implementation of the President's E-Government initiatives related to homeland security will overcome information sharing difficulties between Federal, state, and local organizations and first responders. In addition, many of the other Presidential E-Government Initiatives provide solutions that must be adopted by all departments. These initiatives include E-Authentication as well as a new initiative on public health information.

The goal of E-Authentication is to minimize the burden on businesses, the public and government when obtaining services online by providing a secure infrastructure for online transactions, eliminating the need for separate processes for the verification of identity and electronic signatures. However, a large portion of E-Authentication involves policy work. As the Federal government modernizes internal processes to reduce costs for agency administration and moves to cross agency applications that are available to all Federal employees, common solutions for authentication are needed. The first step of which is the development of policy to implement standardized

identity credentials across the Federal government, which all Departments will implement.

Public Health Monitoring involves activities associated with monitoring the public health and tracking the spread of disease. For FY 2003 and FY 2004 requests for projects valued at $ 267 M and $ 296 M were received by OMB. Requesting agencies included HHS and VA. Areas of potential overlap included: health information surveillance, emergency response and addressing "early warning" and alerts, decision support and case management functionality.

Two of the President's initiatives, Project Safecom, and Disaster Management, directly support and promote improving information sharing between Federal, state, and local first responders. The goal of Project Safecom is to provide interoperable wireless options for Federal, state and local public safety organizations and ensure they can communicate and share information as they respond to emergency incidents. Disaster Management provides Federal, state, and local emergency managers online access to disaster management-related information, planning and response tools. Both of these initiatives strongly support "vertical" (i.e. intergovernmental) integration necessary to meet homeland security goals.

Because these two initiatives clearly support homeland security missions and activities within the Department of Homeland Security, OMB placed it as the managing partner for the initiatives. As managing partner, DHS is responsible for ensuring the accuracy of the business cases for these initiatives, submitting the business cases, and ensuring the management of the projects to achieve the cost, schedule and performance goals for the implementation and operations phases.

Additionally, as part of the recent OMB guidance to agencies on FY 2005 budget planning, and to ensure that E-Government initiatives are appropriately supported, OMB will provide each agency's funding or other resource requirements as outlined in the FY 2004 President's Budget, for participation in the Presidential E-Gov Projects, consistent with requirements under the E-Government Act of 2002.

4. President's Management Agenda

OMB monitors progress on all of these items on a regular basis through the President's Management Agenda Scorecard under the Expanding E-Government Score. Inability to achieve the core criteria under the E-Government Scorecard will prevent an agency from "getting to green". As true information sharing is dependent on a number of factors as I have discussed -- development and implementation of an effective EA, appropriate planning and budgeting for IT investments, and successful achievement of E-Government initiatives, -- failure to overcome barriers will directly impact an agency's E-Government Score. Because the Department of Homeland Security is new, it's status is scored as "red." We are actively working with them to achieve real progress in the next several months.

Conclusion

The Administration will continue to work collaboratively across Federal agencies, with Congress, State and local governments, and the private sector to strengthen information sharing in support of homeland security efforts. Achieving true homeland security will require IT investments that both guarantee real-time information sharing, and successfully improve response time and decision-making. To meet these goals and assist in overcoming information sharing barriers, we require wise IT investments that support homeland security missions, enhance productivity, ultimately facilitating information sharing while ensuring security and privacy.

While we recognize that the Department is currently grappling with cultural legacies of twenty-two component agencies, we fully expect that DHS leadership will continue to build an integrated and interoperable structure, resulting in a business driven EA that reflects the President's vision of eliminating "sub-optimitized, duplicative, and poorly coordinated systems." OMB will continue to work with DHS leadership, including the Chief Information Officer to ensure that their EA efforts, their integration of business process, and consolidation and elimination of redundant IT investments remains a top priority and is addressed in a timely manner. We will assess their efforts on a regular basis and use the President's Management Agenda Scorecard to monitor their progress against detailed milestones.

Chairman TOM DAVIS. Thank you. Let me just start the questioning.

I mean you are trying to integrate 22 component agencies, but some of these agencies are miserable failures stand alone. INS is just a mess. I think we saw some of that in September 11. I have looked at it, talked with contractors. What is our strategy there? I know it is now different agencies. How long is that going to take and how much will it cost, do you think? Do you have a figure on that yet or is it a little premature?

Mr. COOPER. Chairman Davis, I don't have a figure yet. What we have begun are formal program reviews. My focus is very heavy on the information technology component.

We are working through these as rapidly as we can. We are running them in priority order, meaning the priority dictated by the business community, our business leadership, the Under Secretaries, Deputy Secretary; and then, as guided by Secretary Ridge.

We have about 20 or 25 of the highest priority initiatives over the next several weeks, and as rapidly as we can we will come back and offer additional information, additional insight gleaned from these program reviews.

Chairman TOM DAVIS. One thing that has impressed me about the way we've handled this is initially, when you get different agencies like this and you're trying to solve problems, traditionally Government has just sent a lot of money out the door, contractors working without really taking a look at the requirements that we have, taking a look at how it is going to integrate. We have been a little slow to start. I don't think there is any question about that.

I don't think it is too early to give a grade, and people get impatient, you know, but it is a smarter way to go. At the end of the day, I think our moneys would be spent smarter and we will get a better system. At least that is my impression from the way things are being handled. Is that fair, do you think?

Mr. COOPER. Yes, I agree. One of my concerns is that I think if we simply begin to, if you will forgive the expression, kind of throw money at the problem before we clearly understand where are the highest priorities, where are the best opportunities for integration, where are the greatest opportunities for us to realize value, I think we run the possibility of wasting some of that money and some of that effort.

Chairman TOM DAVIS. Absolutely. Absolutely. I know a lot of companies out in my district that are a little impatient. They have geared up for this. A lot of them have some very innovative solutions they want to offer. But I think you are smart to sit back and make sure we have an integrated plan on how it is all going to fit together, that you have set your priorities.

You stated in your testimony that the "as-is" architecture is about 70 percent complete at this time, and the inventory of your "as-is" applications is also about 70 percent complete. You expect to have both the "as-in" architecture and inventory completed by next month? Is that roughly——

Mr. COOPER. The end of June——

Chairman TOM DAVIS. The end of June?

Mr. COOPER [continuing]. Is our target date now.

Chairman TOM DAVIS. Now? Are you completing the process? As you go through this, can you tell us what you found in any redundant systems and give us any examples?

Mr. COOPER. We have already begun to identify some opportunities. For example, in our infrastructure component, we have certainly identified that we have multiple physical networks, for example. The question is, how many of those do we actually need? What is the optimal number?

We would like to actually move toward one unclassified network. Now that is going to take a little bit of time, but over the next probably 18 to 24 months that should be something that I think we can address.

So an example is to begin to consolidate the number of unclassified networks that we have. Another example: In our management types and administrative types of applications, human resources, financial management, some of the administrative and management applications, we certainly don't need the 20-plus human resources applications that existed legitimately, not because anybody did anything wrong, but because each agency required a human resource capability. Then that was, indeed, automated.

But, as a new, single department, we have an opportunity to consolidate it. We are working closely with OMB and under their guidance. So those are some examples of opportunities.

Another example is actually in what we call the mission-critical space. There are a number of organizations and agencies that had, for example, alert and warning types of applications. So one legitimate opportunity is to evaluate, might there be some advantage and some value and, admittedly, some cost savings if we move from a dozen alert and warning types of applications to perhaps a smaller number? It might not be one, but it certainly might be two or three, as opposed to a dozen.

Chairman TOM DAVIS. Well, the next phase, then, would be the "to-be" architecture?

Mr. COOPER. Yes.

Chairman TOM DAVIS. And you state the initial plan will be completed in August 2003. Can you elaborate on what the "to-be" architecture, what it will encompass, and what do you mean by the "initial plan?"

Mr. COOPER. OK.

Chairman TOM DAVIS. It would be, I mean, when will it be finally complete, examples of that?

Mr. COOPER. When we say a "to-be" architecture, what we are really talking about is the desired state or the target state for how we do business; what are our objectives; what are our goals; what are our measurements, our metrics. Let me use an example out of Border and Transportation Security.

As we look across the business processes that comprise how people and cargo enter the United States and then leave the United States, one of the opportunities is to re-engineer that business process, take a holistic look across all of the separate agencies that came into the department, each with its own process, look at them kind of side by side, and look for a seamless, end-to-end, horizontal process that really addresses the movement of people, beginning with a visa application process and continuing all the way through

when they actually enter the United States, travel in the United States, and then leave the United States.

Our desired-state architecture would actually re-engineer that process. At a macro level, it would now repaint a picture. The desired state differs from the existing state. We then can take the gap and make determinations about, how do we move from where we are to where we want to be? That is what we then call our migration strategy or our road map, and we expect to have the first release of our road map by the end of the fiscal year, by the end of September 2003.

Chairman TOM DAVIS. Thank you. Thank you very much.

Mr. Lynch.

Mr. LYNCH. Thank you, Mr. Chairman.

Mr. Cooper and Mr. Forman, I want to thank you for coming before the committee and helping us with our work. In another configuration, this committee is responsible with an ongoing investigation of the FBI, and Chairman Davis is doing a wonderful job on that, along with our ranking member, Mr. Waxman.

Now what we have learned in that investigation of the FBI—and I don't mean to single them out, but that is the agency we are investigating—we have found a couple of things. No. 1, when an agency's task and directive is to operate in secrecy, and when an agency is encouraged and directed under law and regulation to operate in secrecy, it is against the culture, No. 1, to share information. So we are working against a very strong culture of—I mean, obviously, if you want things to be secret, you don't share information.

Second, the thing we have also seen at the FBI, and it exists at other agencies, is that so much of the culture there is based on career advancement, that if you are an FBI agent, a supervisor, and you are undertaking an investigation, a very important one, whether it involves organized crime or terrorist activity, you want to advance your career. The last thing you want to do is share that information that you have that might be important to your success with another competing agency.

So we have a culture here that is directly opposed to the free sharing of information, and I worry for the American people, not only because of the flat-out atrocities that I have seen within the FBI, but also because our national security, especially after September 11, requires the sharing of this information.

Now I appreciate all the work you are doing on technology, but this is a human fault in our system. I have two questions.

My first question to either of you gentlemen would be: What are we doing to encourage information-sharing and a change in that culture of secrecy and obsessive control of information within these agencies? Anytime you are ready.

Mr. COOPER. Let me begin. One of the things that we are doing that we have actually found has helped, and is helping, break down some of the cultural biases against sharing, we have created a couple of, what we call, integrated teams. We have pulled people together from across the various intelligence communities, intelligence members, including the FBI, to first agree upon a shared vision, and with the shared vision, we can then set kind of goals and objectives around, if we have this shared vision and if it does

require the sharing of information held within each member of the community, how then might we be able to share that information in order to support that common goal or objective.

We have had some good dialog. We have been able to actually reach agreement, and that agreement has actually now taken the form of Memorandums of Understanding and Memorandums of Agreement signed between and among the FBI and other Federal departments and Federal agencies at the business level, the leadership level, that set this forth in writing and do commit those agencies to working together to share information, in compliance with that shared vision.

Mr. LYNCH. Let me ask you, do the memoranda, do they include any specific incentive for agents to share information or any specific penalties if they do not share information that should be shared?

Mr. COOPER. The memoranda that I have seen do not contain that specific information.

Mr. LYNCH. OK. Well, until we get to that root problem, I think that all this other stuff is just window-dressing. That is the core of our problem right there, is the secrecy and the unwillingness of people to share information. If you are not getting at that problem, all the new computers and all the networks in the world, they are not going to help us. We are going to be before this committee again someday asking how come we didn't all know about, you know, some type of threat.

OK. That being the case, I want to point out just to the GAO report which was——

Chairman TOM DAVIS. The gentleman's time has expired, but I will let him finish up here. I will let you make this final comment here.

Mr. LYNCH. Thank you, Mr. Chairman. Thank you.

One question, and you can do with it what you will. The GAO report talks about these terrorist lists, and it seems like every agency has one. We have very little coordination in terms of consolidating or agreeing on these terrorist/criminal watch lists. The GAO report, at page 28, has a very dismal assessment on how these agencies are actually coordinating on this specific point, and this is a good example; in spite of congressional direction and executive direction to get their act together and coordinate their lists and decide a concerted approach, it has not happened.

It has been 20 months since September 11, and I know that you work with the White House and related offices. I was wondering why, after 20 months, we don't have an effective response to this particular situation.

Mr. COOPER. I believe that the current state is much, much better than it was 20 months ago. There is a working group. That working group is now guided by the TTIC, T-T-I-C, Terrorist Threat Integration Center. We are a member of that working group. The members of the intelligence community are members of that working group. The FBI is a member of that working group. It is an example of a working group that I just referred to.

I think, literally for the first time in history, there are documents that are being circulated for signature that do contain some very specific examples and requirements around the sharing of informa-

tion. Let me actually pull one paragraph out of the Memorandum of Understanding that is being shaped that speaks to data bases and the integration of these data bases, "The parties agree to establish procedures and mechanisms to provide the Department of Homeland Security, as appropriate and practicable, other covered entities with access to data bases containing covered information. To this end, parties shall establish a working group within 30 days of the date of this agreement." That is kind of what is underway now.

So we are actually spelling out in writing that everyone will kind of sign up to the mechanisms that I think will get us to the integration that we are talking about.

Mr. LYNCH. I want to thank you again, Mr. Cooper and Mr. Forman, for your good work. Could I ask you, might we get a copy of that memorandum, not on the record but for our review?

Mr. COOPER. Certainly, I think this is under the guidance of the TTIC. So, if I may respond, check with them and then respond?

Mr. LYNCH. That would be great. Thank you very much. Thank you, Mr. Chairman.

Chairman TOM DAVIS. I thank the gentleman. The vice chairman of the committee, Mr. Shays.

Mr. SHAYS. I thank the gentleman. I really have to work to get into this issue, but I think it is hugely important. Probably my biggest disappointment with the Department of Defense is most of our IT stuff has turned out not to work out as well as we wanted. We spent a fortune.

I am interested to know, how is the Department of Homeland Security incorporating data and systems architectures for external entities like DOD, CIA, FBI in the design of DHS objective systems. I mean, what are we doing? I would like both of you to be able to answer that for me.

Mr. FORMAN. Let me start out, if I may, because one of my not only initiatives, but now accountable responsibilities to this committee is to put in place the governance process and that enterprise architecture framework for the Federal Government.

There is no question that we are living through a change in technology that ties directly to the way we manage the Federal Government. We can't, as you pointed out, rely on hooking together a lot of data bases or computers to fix what is fundamentally a broken business architecture.

In fact, I would have to say most of the work done over the last 2 years has been on that architecture in this area, leading to the Department of Homeland Security Act that was signed, and now the department has begun, up and running. Now it takes a lot of work.

There are decisions that are going to be made, not just by this department, the Department of Homeland Security, but by the Justice Department, the Department of Health and Human Services. Here, again, I refer to my testimony. In our gusto to respond to initiatives, take public health information networks as a perfect example, we now have 18 new systems in the President's budget that was requested in response to congressional action on bioterrorism networks. I view it as my job to make sure that we now don't invest in the 19th system because we have this fragmented structure

that turns into multiple computers on people's desks in the health information centers at the county level and hospitals.

This architecting issue is real and relates to roles and responsibilities of multiple organizations. So we have to get the business model right, and that ties to processes.

There are responsibilities for Federal CIOs under the Clinger/Cohen Act and under the E-Government Act of 2002, but this is going to take a lot of engagement from Members of Congress, from this committee's leadership position, through the appropriations process, as well as senior political officials in each of the departments to understand how to work together.

Fundamentally, we are talking about business processes that did not exist and, hence, information systems we are trying to hook together that were built for different purposes. That has to be done in a rigorous architecting process.

Mr. SHAYS. Mr. Forman, let me ask you, is it an advantage that we are reorganizing into a Department of Homeland Security? Does this give us opportunities or just made life more difficult for us?

Mr. FORMAN. It is a requirement. We could not do this without appointing an organization. We couldn't have people, given their current roles and responsibilities under statutory requirements, merely sharing information without somebody in charge of making decisions on the basis of that information, and, hence, the need for the Department of Homeland Security fills an important gap in our world, we would say, the business architecture and the reality. Nobody had those roles and responsibilities before creation of the department.

Mr. SHAYS. Thank you. Mr. Cooper.

Mr. COOPER. One of the things that we are doing to add a little bit more specificity, deliberately and consciously, to kind of reach out to other Federal agencies, we have begun the development of joint exhibit 300's to submit to OMB in a couple of specifics. Let me give you some real examples.

Wireless technology and the use of wireless technology for interoperability, this also now reaches out to State and local, tribal government as well. By teaming together with, for example, the Department of Justice and the Department of Treasury, we are kind of the lead three agencies in this, and by crafting a joint exhibit 300, we are actually putting together a plan that encompasses capability that already exists as well as the need for new capability that we might identify that call all of us to work together collaboratively and submit this, then, to OMB, so that we are actually bringing forward a more powerful opportunity to request funding and support and reach out across the Federal environment.

Two other key areas that we are doing this in: One is in intelligence information, meaning we are specifically looking at all of the applications, not just within the Department of Homeland Security, that might pull together; we can consolidate; we can integrate.

A third area is in the area of identity credentialling. There are a number of initiatives that are underway across several Federal agencies. We are trying to pull those together, so that we can basically do this once in an optimal manner and then move forward together.

Mr. SHAYS. Thank you, Mr. Chairman.

Chairman TOM DAVIS. Thank you. Mr. Ruppersberger.

Mr. RUPPERSBERGER. Yes, sure, thank you for being here. Look, this is an exercise that we are all moving forward with; we are learning a lot. We need to learn from our mistakes. As has been stated before, there is an issue as it relates to culture, the need-to-know basis in all the agencies.

There is so much information and things that we can talk about, and I have 5 minutes. So I am going to throw out a couple of questions and then be quiet. That way, I won't be penalized for going over my 5 minutes.

Basically, I am going to address some of the questions from a local and State issue, and I think that one of the main issues that we are dealing with now is how we work that communication level between the different areas. Terrorism is unlike other types of investigations where a lot of times "need to know" is very important.

I think the three areas, and there are three topics and issues that I think are extremely important as far as consistent procedures, and that would be, No. 1, information-sharing. Information-sharing, in my opinion—or I would like your opinion—on how we develop a workable plan to share the data throughout the necessary channels.

Also, the second issue is knowledge management. Knowledge management determines what should be done with information once an agency or department gets this information.

The third would be data mining. Data mining is basically receiving the data, storage, and the ability to retrieve that information.

Now, from a local perspective, I represent the Baltimore region. I was a former county executive. So I have had a lot of communications with the former police chief and still police chief of Baltimore County. Some of his issues are that he thinks communication has improved within the last year, but still there is not specifics of origins of information they receive, not allowed to evaluate the quality of threats or leads as it relates to them. It is coming down almost as a mandate.

Two, local investigators—in the same area—local investigators might determine the information is too glossed-over to be useful, and this is kind of frustrating.

The FBI and others are trying to be more up front, but the information is just not accurate or timely. Sometimes you get notice, you get more from what you read in the newspaper than you do from those agencies. So the timeliness of that data, the information.

Third, immigrants are not in a data base. They need that information if they stop someone. That is extremely an important issue, I think.

The National Crime Information Center/exit registration system is not connected to what they need in the field.

Now I also represent Baltimore City. Mayor Martin O'Malley, who is very active with the—what; is it major city mayors—and he is up front on the issue of where we need to go and what their concerns are.

No. 1 I think is the security clearance. There are certain people within his organization/administration that have not been ap-

proved or received it. So when there is information that might have to deal with a fire department or if the mayor himself might receive information, he is not able to get that and to be able to analyze it and take the steps to where they need to move.

So some type of data base compatibility also is an issue. There is no way to search and post information within and between jurisdictions. An example: Someone who was stopped in New Jersey about taking pictures of bridges, now why wouldn't Philadelphia, Baltimore, and Washington maybe receive that information?

Responsibility/authority, Federal agency authority and clear. Locals get conflicting information from Customs, Immigration. Kind of no clearinghouse. We need to focus on the consistency of the information.

A Federal alert system of value; warnings, in his opinion—this isn't mine—are useless; get more from media than the Department of Homeland Security at the local level. Unspecified threats more important to cities and outlying areas. That is his opinion. He does have the Port of Baltimore and a major city area.

Now I am throwing that out because I think that there is a lot to talk about here, and we can't accomplish it in a 5-minute situation. But it is a culture. There is a foundation that we are trying to create. I see, personally, a lot more cooperation, but there is still that culture of "need to know." A lot of times you need to know that.

I happen to be on the Intelligence Committee, and there is nothing we can talk about there. So that is a culture, but it is a necessary situation until it is retrieved.

A lot of comments. Could you please respond to some of the issues that I raised?

Mr. COOPER. I think, first of all, that you are absolutely on target with the content and the points that you are raising. We are, in some form or another, addressing almost everything that you have outlined here. At the moment, we are not as far along in some of these areas as others. Again, this is complex, as you, yourself, have indicated.

We have it underway, and our focus has started on the information-sharing. We feel that we have to get the basics in place before, for example, we can move to kind of the higher level of knowledge management and before we can really take advantage of some of the tools and capabilities related to data mining capability from an information technology standpoint.

But, specifically around information-sharing and information-integration, we have a number of pilot initiatives underway where we have reached out to State and local government, where we actually are putting connectivity in place, albeit in a pilot manner at the moment, to share information in a two-way flow, both from State and local government and appropriate authorities, members of the first-responder community to us, and then in turn——

Mr. RUPPERSBERGER. And, by the way, I would agree because a lot of your leads come from the local, from the street, so to speak.

Mr. COOPER. Absolutely, yes, sir.

Mr. RUPPERSBERGER. So it needs to go both ways——

Mr. COOPER. Yes, sir.

Mr. RUPPERSBERGER [continuing]. And then be analyzed.

Mr. COOPER. It absolutely does.

Mr. RUPPERSBERGER. That is probably one of the biggest issues, is analyzing information.

Mr. COOPER. Yes.

Mr. RUPPERSBERGER. As we even know with September 11, we have the technology and the ability to receive a lot of it, but it is analyzing that information.

Mr. COOPER. Yes, absolutely. A lot of this activity is being guided by our Information Analysis and Infrastructure Protection Directorate, which, as you know, is one of the new directorates that was established by the legislation.

So we are also being challenged a bit by a startup. In other words, there weren't existing entities as part of our incoming agencies that had full responsibility and a significant amount already in place. It is underway. We are making progress.

In addition, we are also including State and local representation in our enterprise architecture work. This is another mechanism by which we actually can hear and validate from the local communities, from the State communities, from the first-responder communities, what is it that they believe are the highest priority processes and, in turn, they are working with us to actually re-engineer and improve these processes.

Once that work is completed along the schedule that I outlined, we then, in turn, can begin to apply information technology tools, methods, and techniques to more rapidly integrate and achieve information-sharing.

Chairman TOM DAVIS. The gentleman's time has expired.

Mr. RUPPERSBERGER. Can I ask just one question or comment?

Chairman TOM DAVIS. Sure.

Mr. RUPPERSBERGER. Thank you. It is a big issue that we are dealing with. I think something that has worked in the past, and I would just like your comments on this, and it was used by the FBI when they started to get involved in the narcotics enforcement, where you would have strike forces involving FBI, DEA, local, and State. In order to break a culture, it seems to me that a lot of it is trust and working together, so that a strike force concept develops those relationships. A lot of it is relationships.

I mean, you see right there that there are certain FBI offices that might not get along with certain locals in one jurisdiction but they do in another. I think that is something that maybe we should look at, as we are developing how to break down this barrier of information and getting the information out so it is useful or coming both ways. I just would like your comments, whether you think that strike force—and maybe we shouldn't use the words "strike force," but that is what worked in the past, and I think it still is working.

Mr. COOPER. I certainly agree. In fact, we actually have followed your recommendation, and we have, although not a lot in number, we have a couple of those strike force types of teams.

One example is in our enterprise architecture work, where we really do have a working group comprised of State and local Chief Information Officers and/or their designated architectural representatives, subject matter experts, who are working side by side with the Federal teams that are involved to establish a true na-

tional enterprise architecture for homeland security that is aligned with our Federal enterprise architecture, guided by OMB. So that is one example.

Another example is we have a number of—admittedly, this is in the information technology arena—but we have a number of technical working groups that are actually local, State, in a couple of cases private sector involvement, along with our Federal subject matter experts, to actually define things like some of our technical standards around data-sharing and information-sharing.

So we have taken your advice. We actually have a couple of these in motion.

Mr. RUPPERSBERGER. Thank you. Mr. Chairman, if you don't mind, I am going to try to make this an issue between the State and local and the Federal Government in this information.

Chairman TOM DAVIS. Mr. Tierney.

Mr. TIERNEY. Thank you, Mr. Chairman. I thank the witnesses for being here this morning to try to help us.

Just in looking through this and realizing that we were trying to develop some watch lists at one point in time, and having some difficulty deciding who was responsible for that, Mr. Cooper, you have been in both different branches of this. I was a little disturbed with GAO's report when they indicated that the White House was unresponsive to its queries about what was going on with the consolidation of lists and with the exchange of information.

Today, who is responsible, ultimately, for putting together these systems? Is it the White House Office of Homeland Security or is it the Department of Homeland Security or is it somewhere in between?

Mr. COOPER. At the moment, it is a coalition that includes the Department of Homeland Security, the Terrorist Threat Integration Center, the FBI, and the Department of State, and members of the intelligence community.

Mr. TIERNEY. Now who of that group is in charge?

Mr. COOPER. They are at work. It is being guided by the TTIC, T-T-I-C, the Terrorist Threat Integration Center. That business group is at work to actually define the process and the governance by which your question can be answered.

Mr. TIERNEY. You're kidding me? All this time after September 11, 2001, we are sitting here saying the White House doesn't accept responsibility for this; the Department of Homeland Security doesn't accept responsibility for this. Some bureaucracy of an amalgamation of different agencies, whatever, is getting to the point where they are now trying to sit down and decide who is going to be in charge? Where is the leadership in that?

Mr. COOPER. I think the leadership is working together to further define and refine a true process for an integrated watch list activity.

Mr. TIERNEY. You say that with a straight face, which I think is admirable, but, I mean, does that disturb you somewhat, that this is the point we are at?

Mr. COOPER. It is the point that we are at, and I think that shortly we will have definitive answers.

Mr. TIERNEY. Can you define "shortly" for me?

Mr. COOPER. Can I get back to you?

Mr. TIERNEY. OK. [Laughter.]

Chairman TOM DAVIS. It is above his pay grade.

Mr. TIERNEY. Well, no, I am not trying to be difficult with the witness. You understand I am not trying to be difficult with you; I am trying to get an answer on this.

Mr. COOPER. No, I understand. Part of it is our fault——

Mr. TIERNEY. Our chairman indicates that it is above your pay grade.

Mr. COOPER. Yes. I am honestly not trying to duck the question, but——

Mr. TIERNEY. No, I understand.

Mr. COOPER [continuing]. But I am not in the lead on this particular activity. Therefore, I think it would be imprudent of me to actually speak on behalf of the group that is doing the work.

Mr. TIERNEY. All right. Fair enough. I am just stunned, I guess, to think that, you know, originally, we had the White House Office set up. It seems to have some rationale to continue to function. I mean it seems to me to be a great rationale to have from the White House somebody in charge of pulling together not just the Department of Homeland Security, but those agencies that aren't within the Department of Homeland Security.

I was one who criticized that consolidation for not including the FBI and the CIA, for this very reason. To find out now that we are, 2 years later almost, and this still isn't done, to me is just staggering. I think that there is an absolute abdication of leadership here from the White House and people that could be doing it. Maybe it is the vacancy in that position that creates part of the problem, although I notice that the President still is seeking funding for 2004 for an agency that doesn't seem to have leadership and doesn't seem to be doing what I thought was one of the primary responsibilities that were given to it.

Mr. FORMAN. I don't think it is quite fair to say that there is no leadership. I thought the leadership was quite clear in the President's budget this year, how he outlined it in the State of the Union, TTIC, the Terrorist Threat Integration Center.

There is no question that we have to get the agencies to work together. That takes identification of business process and across organization, very similar to what we see in industry with the matrix unit today.

So to say that any one department should be accountable for working with other departments, I understand that perfectly. This has to cut across departments because there are multiple players that have to be involved. There are different business processes that will run——

Mr. TIERNEY. That is exactly the point, isn't it: that in order for different agencies cutting across an area to work together, there has to be somebody leading it who gives them the authority and the will to cut across and deal with one another? So I take exception to your offering up here of your opinion, which I appreciate, but I am going to tell you, I take real exception to it.

This is an abject failure in leadership because a leader would have taken what is probably one of our principal concerns here and put somebody in charge of making sure there was coordination on this effort and making a determination of how that information

was going to be shared. We wouldn't be sitting here looking, almost 2 years later, and realizing that we still don't have the kind of communication systems between these agencies that should have been resolved.

We have had a position that has been vacant for a period of time, where it still seems to reside, although the White House, for some inexplicable reason, won't deal with the GAO and give them any answers or information. So it makes it difficult for us to do our oversight functions.

So not only does there appear to be a lack of leadership, it appears to be a lack of cooperation with Congress in trying to get the oversight that could help us define how that leadership ought to be directed and how we could get to the bottom of this problem.

So I appreciate your kibitzing there on that, but I just strongly disagree with you. It is a lack of leadership, and I hope that this committee or bureaucracy, whatever that has been set up to resolve this issue, moves quickly. I think, preferably, it could have been done with one person making a firm decision and giving some direction.

But thank you.

Chairman TOM DAVIS. Thank you. Mrs. Blackburn.

Mrs. BLACKBURN. Thank you, Mr. Chairman. I am kind of sitting down here between two seats, I think.

I apologize that I had to miss much of your testimony. I was over in the Judiciary Committee in a hearing there.

But I did want to step in. I think I am one of these committee members that has been increasingly frustrated as we look at the lack of interaction between the public and private sector in integrated technologies and interactive technologies and in the incredible amount of money that is spent without a resolution to having systems that talk to one another.

I am going to pick up where Mr. Ruppersberger kind of left off there. He was talking with you about having an interface with your local, State, and Federal Government and involving your local and State governments in some input as you look at developing your enterprise architecture, and the overlay, the template that you are going to work from on this.

Then you started touching on it and stopped off. So let's carry the rest of this conversation.

You talked a little bit about your tech working groups and mentioned that you had some private sector input into those groups. So let's go back to that, and let me ask you how you are integrating the private sector into this process in developing the enterprise architecture. From the get-go, are you looking at doing this as a template that will be from the top down that will help interface all of your local and State agencies?

Mr. COOPER. Initially, what we are actually trying to do is gain some input as we work through to our first release, this road map, this migration strategy that I had mentioned earlier, which we are on target to release at the end of September, as we head into October of this year.

We are doing a couple of things. First of all, we are reaching out through some of the information technology associations like the Information Technology Association of America or the Private Sec-

tor Council or the Industry Advisory Council, organizations and associations like that. So that we basically can pose questions or areas of interest to the associations and ask them, "Would you, please, now ask your membership to give us some type of feedback or comment as appropriate?" We are doing that as we move between now and September.

We then intend, as we release our initial version of our work in September, that will go out; that will be widely released to the private sector and to State and local governments, so that we then can work with them to validate, improve, edit, recorrect, adjust, align, whatever, as appropriate. So that, in fact, we then collaboratively produce a more effective enterprise architecture.

Mrs. BLACKBURN. OK, so September is when you are looking at being your initial presentation?

Mr. COOPER. Yes, Ma'am.

Mrs. BLACKBURN. OK. As you work through this process, your timeline going forward from that, when do you think that you will have a workable rollout, something——

Mr. COOPER. Actually, the September rollout will be a workable rollout. We will begin to use that rollout for decisionmaking.

Mrs. BLACKBURN. All right.

Mr. COOPER. We will continue to refine it.

Mrs. BLACKBURN. OK, continue? OK. And then what, as you have talked to the different agencies and associations, what type response are you getting? What type of innovation or ideas are you seeing come forward?

Mr. COOPER. Very positive. We have had a significant number of members of those organizations provide input and approach us, directly approach my office and members of my office to offer ideas, to offer suggestions. As rapidly and as effectively as we can, we are trying to absorb as much of that comment and incorporate it. We are trying to listen. We are trying to buildupon the good ideas that we are receiving.

Mrs. BLACKBURN. Before my time expires, an estimation of total cost, do you have that?

Mr. COOPER. For the enterprise architecture activity——

Mrs. BLACKBURN. Yes.

Mr. COOPER [continuing]. Between now and September? It is estimated at about $3 million for this fiscal year.

Mrs. BLACKBURN. OK, and are you all developing, more or less, a group of lessons learned or best practices that can be applied to other agencies?

Mr. COOPER. In concert with our work, we are trying to kind of record those as effectively as we can. We are working with the Federal CIO Council Best Practices Committee and being guided both by them, but also trying to collect what we learn, so that we then can disseminate it out across the Federal environment.

Mrs. BLACKBURN. Excellent. Thank you.

Mr. FORMAN. If I may just add onto that, it is important to understand that the Federal enterprise architecture is based on a component-based model. That is the way the industry is moving today on both the IT side and where the large corporations are moving.

That is essentially what people would call "plug-and-play." We require that for all departments to be involved. At the Federal level, the CIO Council, the National Association of State CIOs, and several local government groups are jointly involved in defining that. We have financed the State architecture work by NASCIO, National Association of State CIOs, explicitly so we can make this link up together.

Mrs. BLACKBURN. I appreciate that, but I am one of those freshman that came from a State senate, where it was not uncommon to spend $100 million a year on interactive technologies or on IT in general, some program that doesn't work, doesn't talk to the other.

The lessons learned from September 11 were that your first-responders can't communicate, and you have a situation of, who's on first? So those confidences and the knowledge that you are working not only with different levels of government, but with the private sector, and that you are building a basis of best practices to move forward, is good to know.

Mr. FORMAN. I appreciate that.

Chairman TOM DAVIS. Thank you very much. I want to thank the first panel for your questions. Some members are going to have some written questions, and we may have some followups. But I think you have been very forthright about it. I think we have shared with you some of our concerns that you share with us, and we appreciate the job you are doing.

We will move on to the second panel at this point. We have a great panel. We have Robert Dacey, the Director of Information Security Issues, and Randolph Hite, the Director of Architecture and System Issues at the General Accounting Office.

We are also honored to have Charles Rossotti, the former Commissioner of the Internal Revenue Service, where he had a distinguished record there, as he had in private business before he came here. He is currently a senior advisor for the Carlyle Group.

If you all would make your way to the front?

Mr. Rossotti, thank you. I understand you flew in from California to do this, and we just really appreciate having you here.

If you could stay on your feet, I am going to swear you in.

[Witnesses sworn.]

Chairman TOM DAVIS. Thank you. We will start with the GAO representatives. We have your total statement. You can take up to 5 minutes, and then we can get right into the questions.

The light in front is green, and then it is orange with a minute to go, and when it is red, you can try to sum up. Your total statements are in the record.

Mr. Rossotti, I understand you are going to ad lib it up there. We are just happy to have you here. Thank you very much.

Why don't we start with you, Mr. Dacey.

STATEMENTS OF ROBERT DACEY, DIRECTOR, INFORMATION SECURITY ISSUES AND INFORMATION TECHNOLOGY TEAM, GENERAL ACCOUNTING OFFICE; RANDOLPH C. HITE, DIRECTOR, ARCHITECTURE AND SYSTEMS ISSUES AND INFORMATION TECHNOLOGY TEAM, GENERAL ACCOUNTING OFFICE; AND CHARLES ROSSOTTI, SENIOR ADVISOR, THE CARLYLE GROUP, FORMERLY COMMISSIONER, INTERNAL REVENUE SERVICE

Mr. DACEY. Mr. Chairman and members of the committee, we are pleased to be here today to discuss the integration of information-sharing functions at the Department of Homeland Security. As you requested, I will briefly summarize our written statement, which provides details on the department's information-sharing responsibilities, challenges, and key management issues.

The Homeland Security Act of 2002 brought together 22 diverse organizations and created a new Cabinet-level department to help prevent terrorist attacks in the United States, to reduce the vulnerability of the United States to terrorist attacks, and to minimize damage and assist in recovery from attacks, should they occur. Achieving the complex mission of the department requires the ability to effectively share a variety of information among its own entities and with other Federal entities, State and local governments, the private sector, and others.

For example, the department needs to be able to access, receive, and analyze substantial amounts of law enforcement intelligence and other threat, incident, and vulnerability information from both Federal and non-Federal sources; to analyze such information, to identify and assess the nature and scope of terrorist threats; to administer the Homeland Security Advisory System, and provide specific warning information and advice on appropriate protective measures and countermeasures; to share information both internally and externally with agencies and law enforcement on such things as goods and passengers inbound to the United States and individuals who are known or suspected terrorists or criminals, and to share information among emergency responders in preparing for and responding to terrorist attacks and other emergencies.

The GAO has made numerous recommendations over the last several years related to information-sharing functions which have now been transferred to the department. For example, although improvements have been made, further efforts are needed to address several information-sharing challenges to the Government's Critical Infrastructure Protection [CIP], efforts.

These challenges include: developing a comprehensive and coordinated national CIP plan to facilitate information-sharing that clearly delineates the roles and responsibilities of Federal and non-Federal entities, defines interim objectives and milestones, sets timeframes for achieving them, and establishes appropriate performance measures.

Second, developing fully productive information-sharing relationships within the Federal Government and between the Federal Government and State and local governments and the private sector.

The third challenge is improving the Federal Government's capabilities to share appropriate, timely, and useful warnings and other

information concerning both physical and cyber threats with Federal entities, State and local governments, and the private sector, and providing appropriate incentives for non-Federal entities to increase information-sharing with the Federal Government and enhance other CIP efforts.

In addition, GAO recently identified challenges in consolidating and standardizing watch list structures and policies which are essential to effectively sharing information on suspected terrorists and criminals.

The success of homeland security also relies on establishing effective systems and processes to facilitate information-sharing among and between government entities and the private sector. Through our work, we have identified potential information-sharing barriers, critical success factors, and other key management issues that the department should consider as it establishes such systems and processes.

For example, as part of information technology management, which we have discussed earlier today, the department should develop and implement an enterprise architecture to integrate the many existing systems and processes required to support its mission and to guide the department's investments in new systems in the coming years.

Two, to develop and implement discipline system acquisition and investment management processes to effectively select, control, and evaluate IT system projects.

And, three, to ensure effective information security to protect the sensitive information that the department maintains and develop secure communications networks to safely transmit information.

Other key management issues include developing a performance focus, integrating staff from different organizations, and ensuring that the department has properly skilled staff and ensuring effective agency oversight.

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

[The prepared statement of Mr. Dacey follows:]

United States General Accounting Office

GAO

Testimony
Before the Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Thursday, May 8, 2003

HOMELAND SECURITY:

Information Sharing Responsibilities, Challenges, and Key Management Issues

Statement of

Robert F. Dacey, Director,
Information Security Issues

Randolph C. Hite, Director,
Information Technology Architecture and Systems Issues

GAO-03-715T

May 8, 2003

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-03-715T, a testimony before the Committee on Government Reform, House of Representatives

HOMELAND SECURITY

Information Sharing Responsibilities, Challenges, and Key Management Issues

Why GAO Did This Study

The Homeland Security Act of 2002, which created the Department of Homeland Security, brought together 22 diverse organizations to help prevent terrorist attacks in the United States, reduce the vulnerability of the United States to terrorist attacks, and minimize damage and assist in recovery from attacks that do occur. To accomplish this mission, the act established specific homeland security responsibilities for the department, which included sharing information among its own entities and with other federal agencies, state and local governments, the private sector, and others.

GAO was asked to discuss DHS's information sharing efforts, including (1) the significance of information sharing in fulfilling DHS's responsibilities; (2) GAO's related prior analyses and recommendations for improving the federal government's information sharing efforts; and (3) key management issues DHS should consider in developing and implementing effective information sharing processes and systems.

www.gao.gov/cgi-bin/getrpt?GAO-03-715T.

To view the full testimony, click on the link above.
For more information, contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

What GAO Found

DHS's responsibilities include the coordination and sharing of information related to threats of domestic terrorism within the department and with and between other federal agencies, state and local governments, the private sector, and other entities. To accomplish its missions, DHS must, for example access, receive, and analyze law enforcement information, intelligence information, and other threat, incident, and vulnerability information from federal and nonfederal sources; and analyze such information to identify and assess the nature and scope of terrorist threats. DHS must also share information both internally and externally with agencies and law enforcement on such things as goods and passengers inbound to the United States and individuals who are known or suspected terrorists and criminals.

GAO has made numerous recommendations related to information sharing. Although improvements have been made, more efforts are needed to address the following challenges, among others, that GAO has identified.

- Developing a comprehensive and coordinated national plan to facilitate information sharing on critical infrastructure.
- Developing productive information sharing relationships between the federal government and state and local governments and the private sector.
- Providing appropriate incentives for nonfederal entities to increase information sharing with the federal government and enhance other critical infrastructure protection efforts.

Through our prior work, we have identified potential information sharing barriers, critical success factors, and other key management issues that DHS should consider as it establishes systems and processes to facilitate information sharing among and between government entities and the private sector. It will be important for the department to understand the numerous potential barriers to information sharing and develop appropriate strategies to address them, considering any related provisions of the Homeland Security Act. Our work has also identified critical success factors for information sharing that DHS should consider as it proceeds. Further, as part of its information technology management, DHS should develop and implement an enterprise architecture to integrate the many existing systems and processes required to support its mission and to guide the department's investments in new systems to effectively support homeland security in the coming years. Other key management issues include ensuring that sensitive information is secured, developing secure communications networks, integrating staff from different organizations, and ensuring that the department has properly skilled staff.

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss challenges for the Department of Homeland Security (DHS) in integrating its information gathering and sharing functions. The Homeland Security Act of 2002 brought together 22 diverse organizations and created a new cabinet-level department to help prevent terrorist attacks in the United States, reduce the vulnerability of the United States to terrorist attacks, and minimize damage and assist in recovery from attacks that do occur. To accomplish this mission, the Act established specific homeland security responsibilities for the department and directed it to coordinate its efforts and share information among its own entities and with other federal agencies, state and local governments, the private sector, and others.

In my testimony today, I will summarize GAO's analysis of information sharing as an integral part of fulfilling DHS's mission and responsibilities. I will then discuss GAO's related prior analyses and recommendations for improving the federal government's information sharing efforts. Lastly, I will discuss the key management issues DHS should consider in developing and implementing effective information sharing processes and systems.

In preparing this testimony, we relied on prior GAO reports and testimonies on combating terrorism, critical infrastructure protection (CIP), homeland security, information sharing, information technology (IT), and national preparedness, among others. We also reviewed and analyzed the *National Strategy for Homeland Security*, the *National Strategy to Secure Cyberspace*, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, the *National Strategy for Combating Terrorism*,[1] the Homeland Security Act of 2002,[2] and other relevant federal policies. Our work was performed during April and May 2003 in accordance with generally accepted government auditing standards.

Results in Brief

The Homeland Security Act of 2002 and other federal policy, including the *National Strategy for Homeland Security*, assign responsibilities to DHS for the coordination and sharing of information related to threats of domestic terrorism, within the department and with and between other federal agencies, state and local governments, the private sector, and other entities. For example, to accomplish its missions, the new department must (1) access, receive, and analyze law enforcement information, intelligence information, and other threat, incident, and vulnerability information from federal and nonfederal sources; (2)

[1] The White House, *The National Strategy for Homeland Security (Washington, D.C.: July 2002)*; *The National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003); *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, D.C.: February 2003); and *The National Strategy for Combating Terrorism* (Washington, D.C.: February 2003).
[2] Public Law 107-296.

analyze such information to identify and assess the nature and scope of terrorist threats; and (3) administer the Homeland Security Advisory System and provide specific warning information and advice on appropriate protective measures and countermeasures. Further, DHS must share information both internally and externally with agencies and law enforcement on such things as goods and passengers inbound to the United States and individuals who are known or suspected terrorists and criminals. It also must share information among emergency responders in preparing for and responding to terrorist attacks and other emergencies.

GAO has made numerous recommendations over the last several years related to information sharing functions that have been transferred to DHS. One significant area concerns the federal government's CIP efforts, which is focused on the sharing of information on incidents, threats, and vulnerabilities, and the providing of warnings related to critical infrastructures both within the federal government and between the federal government and state and local governments and the private sector. Although improvements have been made, further efforts are needed to address the following critical CIP challenges:

- developing a comprehensive and coordinated national plan to facilitate CIP information sharing that clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets timeframes for achieving objectives, and establishes performance measures;
- developing fully productive information sharing relationships within the federal government and between the federal government and state and local governments and the private sector;
- improving the federal government's capabilities to analyze incident, threat, and vulnerability information obtained from numerous sources and share appropriate, timely, useful warnings and other information concerning both cyber and physical threats to federal entities, state and local governments, and the private sector; and
- providing appropriate incentives for nonfederal entities to increase information sharing with the federal government and enhance other CIP efforts.

In addition, GAO recently identified challenges in consolidating and standardizing watch list structures and policies, which are essential to effectively sharing information on suspected terrorists and criminals.[3]

The success of homeland security also relies on establishing effective systems and processes to facilitate information sharing among and between government entities and the private sector. Through our prior work, we have identified potential information sharing barriers, critical success factors, and other key management issues that DHS should consider as it establishes systems and

[3]Watch lists are automated databases that contain various types of data on individuals, from biographical data—such as a person's name and date of birth—to biometric data such as fingerprints.

processes to facilitate information sharing among and between government entities and the private sector. It will be important for the department to understand the numerous potential barriers to information sharing and develop appropriate strategies to address them, considering any related provisions of the Homeland Security Act. Our work has also identified critical success factors for information sharing that DHS should consider as it proceeds. Further, as part of its information technology management, DHS must develop and implement an enterprise architecture to integrate the many existing systems and processes required to support its mission and to guide the department's investments in new systems to effectively support homeland security in the coming years. Other key management issues include ensuring that sensitive information is secured, developing secure communications networks, integrating staff from different organizations, and ensuring that the department has properly skilled staff.

Information Sharing Is Integral to Fulfilling DHS's Mission

With the terrorist attacks of September 2001, the threat of terrorism rose to the top of the country's national security and law enforcement agendas. As stated by the President in his *National Strategy for Homeland Security* in July 2002, our nation's terrorist enemies are constantly seeking new tactics or unexpected ways to carry out their attacks and magnify their effects, such as working to obtain chemical, biological, radiological, and nuclear weapons. In addition, terrorists are gaining expertise in less traditional means, such as cyber attacks. In response to these growing threats, Congress passed and the President signed the Homeland Security Act of 2002 creating the DHS. The overall mission of this new cabinet-level department includes preventing terrorist attacks in the United States, reducing the vulnerability of the United States to terrorist attacks, and minimizing damage and assisting in recovery from attacks that do occur. To accomplish this mission, the act established specific homeland security responsibilities for the department and directed it to coordinate its efforts and share information within DHS and with other federal agencies, state and local governments, the private sector, and other entities. This information sharing is critical to successfully addressing increasing threats and fulfilling the mission of DHS.

Threats, Incidents, and the Consequences of Potential Attacks Are Increasing

DHS's responsibilities include the protection of our nation's publicly and privately controlled resources essential to the minimal operations of the economy and government against the risks of physical as well as computer-based or cyber attacks. Over the last decade, physical and cyber events, as well as related analyses by various entities, have demonstrated the increasing threat to the United States.

With the coordinated terrorist attacks against the World Trade Center in New York City and the Pentagon in Washington, D.C., on September 11, 2001, the threat

of terrorism rose to the top of the country's national security and law enforcement agendas. Even before these catastrophic incidents, the threat of attacks against people, property, and infrastructures had increased concerns about terrorism. The terrorist bombings in 1993 of the World Trade Center in New York City and in 1995 of the Alfred P. Murrah Federal Building in Oklahoma City, which killed 168 people and wounded hundreds of others, prompted increased emphasis on the need to strengthen and coordinate the federal government's ability to effectively combat terrorism domestically. The 1995 Aum Shinrikyo sarin nerve agent attack in the Tokyo subway system also raised new concerns about U.S. preparedness to combat terrorist incidents involving weapons of mass destruction.[4] However, as clearly demonstrated by the September 11, 2001, incidents, a terrorist attack would not have to fit the definition of weapons of mass destruction to result in mass casualties, destruction of critical infrastructures, economic losses, and disruption of daily life nationwide.

U.S. intelligence and law enforcement communities continuously assess both foreign and domestic terrorist threats to the United States. The U.S. foreign intelligence community—the Central Intelligence Agency, the Defense Intelligence Agency, the Federal Bureau of Investigation (FBI), and the Department of State's Bureau of Research and Intelligence—monitors the foreign-origin terrorist threat to the United States. In addition, the FBI gathers intelligence and assesses the threat posed by domestic sources. According to the U.S. intelligence community, conventional explosives and firearms continue to be the terrorists' weapons of choice. The community also believes that terrorists are less likely to use weapons of mass destruction, although the possibility that terrorists will use these weapons may increase over the next decade.

Nevertheless, in February 2003, the Director of Central Intelligence testified[5] that in his view, we have entered a new world of proliferation, where there are knowledgeable non-state purveyors of weapons of mass destruction materials and technology that are increasingly capable of providing technology and equipment that previously could only be supplied by countries with established capabilities. He also stated that although there have been successes on many fronts in the war on terrorism, recent events underscore the threat that the al Qaeda network continues to pose to the United States. He further stated that even without an attack on the U.S. homeland, more than 600 people were killed in acts of terror last year—200 in al Qaeda-related attacks alone—including 19 U.S. citizens. In addition, he stated that terrorism directed at U.S. interests goes beyond Middle Eastern or religious extremist groups, adding that the Revolutionary Armed Forces of Colombia has shown a new willingness to inflict casualties on U.S. nationals. Table 1 summarizes key physical threats to homeland security.

[4] A weapon of mass destruction is a chemical, biological, radiological, or nuclear agent or weapon.
[5] Testimony of Director of Central Intelligence George J. Tenet before Senate Select Committee on Intelligence on *The Worldwide Threat 2003: Evolving Dangers in a Complex World* (Feb. 11, 2003).

Table 1: Physical Threats to Homeland Security

Threat	Description
Chemical weapons	Chemical weapons are extremely lethal and capable of producing tens of thousands of casualties. They are also relatively easy to manufacture, using basic equipment, trained personnel, and precursor materials that often have legitimate dual uses. As the 1995 Tokyo subway attack revealed, even sophisticated nerve agents are within the reach of terrorist groups.
Biological weapons	Biological weapons, which release large quantities of living, disease-causing microorganisms, have extraordinary lethal potential. Like chemical weapons, biological weapons are relatively easy to manufacture, requiring straightforward technical skills, basic equipment, and a seed stock of pathogenic microorganisms. Biological weapons are especially dangerous because we may not know immediately that we have been attacked, allowing an infectious agent time to spread. Moreover, biological agents can serve as a means of attack against humans as well as livestock and crops, inflicting casualties as well as economic damage.
Radiological weapons	Radiological weapons, or "dirty bombs," combine radioactive material with conventional explosives. The individuals and groups engaged in terrorist activity can cause widespread disruption and fear, particularly in heavily populated areas.
Nuclear weapons	Nuclear weapons have enormous destructive potential. Terrorists who seek to develop a nuclear weapon must overcome two formidable challenges. First, acquiring or refining a sufficient quantity of fissile material is very difficult—though not impossible. Second, manufacturing a workable weapon requires a very high degree of technical capability—though terrorists could feasibly assemble the simplest type of nuclear device. To get around these significant though not insurmountable challenges, terrorists could seek to steal or purchase a nuclear weapon.
Conventional means	Terrorists, both domestic and international, continue to use traditional methods of violence and destruction to inflict harm and spread fear. They have used knives, guns, and bombs to kill the innocent. They have taken hostages and spread propaganda. Given the low expense, ready availability of materials, and relatively high chance for successful execution, terrorists will continue to make use of conventional attacks.

Source: National Strategy for Homeland Security

In addition to these physical threats, terrorists and others with malicious intent, such as transnational criminals and intelligence services, pose a threat to our nation's computer systems. As dramatic increases in computer interconnectivity, especially in the use of the Internet, continue to revolutionize the way much of the world communicate and conducts business, this widespread interconnectivity also poses significant risks to the government's and our nation's computer systems and, more importantly, to the critical operations and infrastructures they support. For example, telecommunications, power distribution, water supply, public health services, national defense (including the military's warfighting capability), law enforcement, government services, and emergency services all depend on the security of their computer operations. If not properly controlled, the speed and accessibility that create the enormous benefits of the computer age also allow individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes.

Government officials are increasingly concerned about cyber attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the FBI, terrorists, transnational criminals, and intelligence services are quickly becoming aware of and are using information exploitation tools such as computer viruses, Trojan

horses, worms, logic bombs, and eavesdropping sniffers that can destroy, intercept, degrade the integrity of, or deny access to data.[6] In addition, the disgruntled organization insider is a significant threat, since these individuals often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets without possessing a great deal of knowledge about computer intrusions. As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available IT, the likelihood increases that cyber attacks will threaten vital national interests. Table 2 summarizes the key cyber threats to our infrastructure.

Table 2: Cyber Threats to Critical Infrastructure Observed by the FBI

Threat	Description
Criminal groups	There is an increased use of cyber intrusions by criminal groups who attack systems for purposes of monetary gain.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities.
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.
Hacktivists	Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message.
Information warfare	Several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that, according to the Director of Central Intelligence,[a] can affect the daily lives of Americans across the country.
Insider threat	The disgruntled organization insider is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data.
Virus writers	Virus writers are posing an increasingly serious threat. Several destructive computer viruses and "worms" have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernoby!) Virus, Nimda, and Code Red.

Source: Federal Bureau of Investigation unless otherwise indicated.

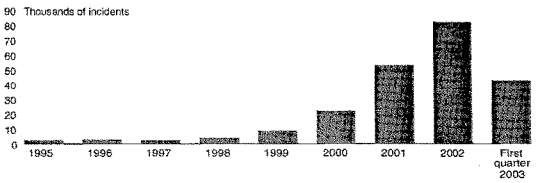
[a]Prepared Statement of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, Feb. 2, 2000.

[6] *Virus:* a program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate. *Trojan horse:* a computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute. *Worm:* an independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate. *Logic bomb:* in programming, a form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment. *Sniffer:* synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.

As the number of individuals with computer skills has increased, more intrusion or "hacking" tools have become readily available and relatively easy to use. A hacker can literally download tools from the Internet and "point and click" to start an attack. Experts also agree that there has been a steady advance in the sophistication and effectiveness of attack technology. Intruders quickly develop attacks to exploit vulnerabilities discovered in products, use these attacks to compromise computers, and share them with other attackers. In addition, they can combine these attacks with other forms of technology to develop programs that automatically scan the network for vulnerable systems, attack them, compromise them, and use them to spread the attack even further.

Along with these increasing threats, the number of computer security incidents reported to the CERT® Coordination Center (CERT/CC)[7] rose from 9,859 in 1999, to 52,658 in 2001, to 82,094 in 2002, and to 42,586 for the first quarter of 2003. And these are only the reported attacks. The Director, CERT® Centers, stated that as much as 80 percent of actual security incidents goes unreported, in most cases because the organization (1) was unable to recognize that its systems had been penetrated because there were no indications of penetration or attack or (2) was reluctant to report incidents. Figure 1 shows the number of incidents reported to the CERT/CC from 1995 through the first quarter of 2003.

Figure 1: Information Security Incidents Reported to Carnegie-Mellon's CERT Coordination Center: 1995 through First Quarter 2003



Source: Carnegie-Mellon's CERT® Coordination Center

According to the National Security Agency, foreign governments already have or are developing computer attack capabilities, and potential adversaries are developing a body of knowledge about U.S. systems and methods to attack these systems. Since the terrorist attacks of September 11, 2001, warnings of the potential for terrorist cyber attacks against our critical infrastructures have also

[7] The CERT Coordination Center (CERT/CC) is a center of Internet security expertise at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

increased. For example, in February 2002, the threat to these infrastructures was highlighted by the Special Advisor to the President for Cyberspace Security in a Senate briefing when he stated that although to date none of the traditional terrorists groups, such as al Qaeda, have used the Internet to launch a known assault on the United States' infrastructure, information on water systems was discovered on computers found in al Qaeda camps in Afghanistan.[8] Also, in his February 2002 statement for the Senate Select Committee on Intelligence, the director of central intelligence discussed the possibility of cyber warfare attack by terrorists.[9] He stated that the September 11 attacks demonstrated the nation's dependence on critical infrastructure systems that rely on electronic and computer networks. Further, he noted that attacks of this nature would become an increasingly viable option for terrorists as they and other foreign adversaries become more familiar with these targets and the technologies required to attack them.

Since September 11, 2001, the critical link between cyberspace and physical space has also been increasingly recognized. In his November 2002 congressional testimony, the Director, CERT Centers at Carnegie-Mellon University, noted that supervisory control and data acquisition (SCADA) systems and other forms of networked computer systems have been used for years to control power grids, gas and oil distribution pipelines, water treatment and distribution systems, hydroelectric and flood control dams, oil and chemical refineries, and other physical systems, and that these control systems are increasingly being connected to communications links and networks to reduce operational costs by supporting remote maintenance, remote control, and remote update functions.[10] These computer-controlled and network-connected systems are potential targets for individuals bent on causing massive disruption and physical damage, and the use of commercial, off-the-shelf technologies for these systems without adequate security enhancements can significantly limit available approaches to protection and may increase the number of potential attackers.

Not only is the cyber protection of our critical infrastructures important in and of itself, but a physical attack in conjunction with a cyber attack has been highlighted as a major concern. In fact, the National Infrastructure Protection Center (NIPC) has stated that the potential for compound cyber and physical attacks, referred to as "swarming attacks," is an emerging threat to the U.S.

[8] "Administrative Oversight: Are We Ready for A Cyber Terror Attack?" Testimony before the Senate Committee on the Judiciary, Subcommittee on Administrative Oversight and the Courts, by Richard A. Clarke, Special Advisor to the President for Cyberspace Security and Chairman of the President's Critical Infrastructure Protection Board (Feb. 13, 2002).

[9] Testimony of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, Feb. 6, 2002.

[10] Testimony of Richard D. Pethia, Director, CERT Centers, Software Engineering Institute, Carnegie Mellon University, before the House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Nov. 19, 2002.

critical infrastructure.[11] As NIPC reports, the effects of a swarming attack include slowing or complicating the response to a physical attack. For example, cyber attacks can be used to delay the notification of emergency services and to deny the resources needed to manage the consequences of a physical attack. In addition, a swarming attack could be used to worsen the effects of a physical attack. For example, a cyber attack on a natural gas distribution pipeline that opens safety valves and releases fuels or gas in the area of a planned physical attack could enhance the force of the physical attack.

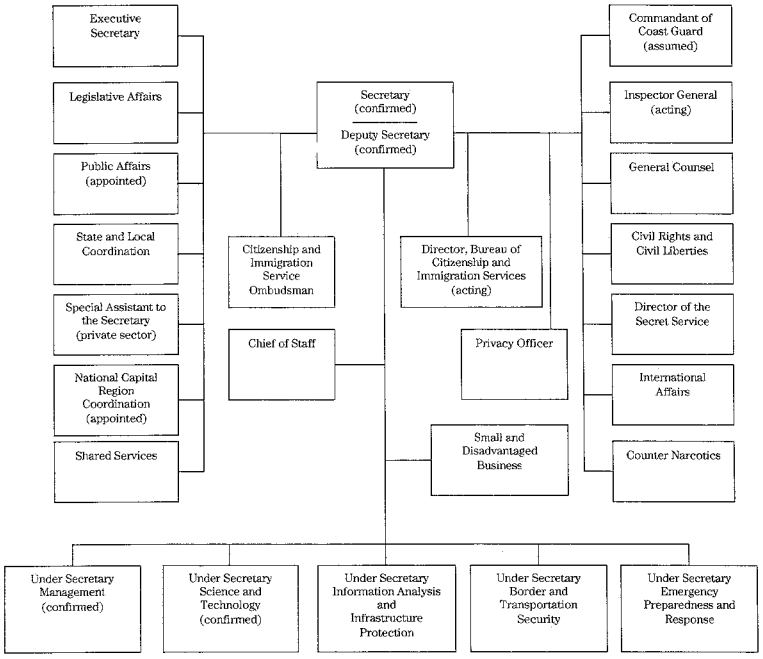
Information Sharing is Critical to Meeting DHS's Mission

As our government and our nation has become ever more reliant on interconnected computer systems to support critical operations and infrastructures and as physical and cyber threats and potential attack consequences have increased, the importance of sharing information and coordinating the response to threats among stakeholders has increased. Information sharing and coordination among organizations are central to producing comprehensive and practical approaches and solutions to combating threats. For example, having information on threats and on actual incidents experienced by others can help an organization identify trends, better understand the risk it faces, and determine what preventive measures should be implemented. In addition, comprehensive, timely information on incidents can help federal and nonfederal analysis centers determine the nature of an attack, provide warnings, and advise on how to mitigate an imminent attack. Also, sharing information on terrorists and criminals can help to secure our nation's borders.

The Homeland Security Act of 2002 created DHS with the primary responsibility of preventing terrorist attacks in the United States, reducing the vulnerability of the United States to terrorist attacks, and minimizing damage and assisting in recovery from attacks that do occur. To help DHS accomplish its mission, the act establishes, among other entities, five under secretaries with responsibility over directorates for management, science and technology, information analysis and infrastructure protection, border and transportation security, and emergency preparedness and response. Figure 2 shows DHS's organization and positions filled, as currently reported by DHS.

[11] National Infrastructure Protection Center, *Swarming Attacks: Infrastructure Attacks for Destruction and Disruption* (Washington, D.C.: July 2002).

Figure 2: Department of Homeland Security



Source: DHS.

As part of DHS's responsibilities, the act includes several provisions specifically related to coordinating and sharing information within the department and among other federal agencies, state and local governments, the private sector, and other entities. It also includes provisions for protecting CIP information shared by the private sector and for sharing different types of information, such as grand jury

and intelligence information. Other DHS responsibilities related to information sharing include

- requesting and receiving information from other federal agencies, state and local government agencies, and the private sector relating to threats of terrorism in the United States;
- distributing or, as appropriate, coordinating the distribution of warnings and information with other federal agencies, state and local governments and authorities, and the public;
- creating and fostering communications with the private sector;
- promoting existing public/private partnerships and developing new public/private partnerships to provide for collaboration and mutual support; and
- coordinating and, as appropriate, consolidating the federal government's communications and systems of communications relating to homeland security with state and local governments and authorities, the private sector, other entities, and the public.

Each DHS directorate is responsible for coordinating relevant efforts with other federal, state, and local governments. The act also established the Office for State and Local Government Coordination to, among other things, provide state and local governments with regular information, research, and technical support to assist them in securing the nation. Further, the act included provisions as the "Homeland Security Information Sharing Act" that requires the President to prescribe and implement procedures for facilitating homeland security information sharing and establishes authorities to share different types of information, such as grand jury information; electronic, wire, and oral interception information; and foreign intelligence information.

The following sections illustrate how DHS will require successful information sharing within the department and between federal agencies, state and local governments, and the private sector to effectively carry out its mission.

Information Analysis and Infrastructure Protection Directorate

The Information Analysis and Infrastructure Protection Directorate (IAIP) is responsible for accessing, receiving, and analyzing law enforcement information, intelligence information, and other threat and incident information from respective agencies of federal, state, and local governments and the private sector, and for combining and analyzing such information to identify and assess the nature and scope of terrorist threats. IAIP is also tasked with coordinating with other federal agencies to administer the Homeland Security Advisory System to provide specific warning information along with advice on appropriate

protective measures and countermeasures.[12] Further, IAIP is responsible for disseminating, as appropriate, information analyzed by DHS within the department, to other federal agencies, to state and local government agencies, and to private sector entities.

The Homeland Security Act of 2002 makes DHS and its IAIP directorate also responsible for key CIP functions for the federal government. CIP involves activities that enhance the security of our nation's cyber and physical public and private infrastructure that are critical to national security, national economic security, and/or national public health and safety. Information sharing is a key element of these activities. Over 80 percent of our nation's critical infrastructures are controlled by the private sector. As part of their CIP responsibilities, IAIP is responsible for (1) developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States and (2) recommending measures to protect the key resources and critical infrastructure of the United States in coordination with other federal agencies and in cooperation with state and local government agencies and authorities, the private sector, and other entities.

Federal CIP policy has continued to evolve since the mid-1990s through a variety of working groups, special reports, executive orders, strategies, and organizations. In particular, Presidential Decision Directive 63 (PDD 63) issued in 1998 established CIP as a national goal and described a strategy for cooperative efforts by government and the private sector to protect the physical and cyber-based systems essential to the minimum operations of the economy and the government. To accomplish its goals, PDD 63 established and designated organizations to provide central coordination and support. These included the Critical Infrastructure Assurance Office (CIAO), an interagency office established to develop a national plan for CIP, and NIPC, which was expanded to address national-level threat assessment, warning, vulnerability, and law enforcement investigation/response. The Homeland Security Act of 2002 transferred these and certain other CIP entities and their functions (other than the Computer Investigations and Operations Section of NIPC) to DHS's IAIP directorate.

Federal CIP policy beginning with PDD 63 and reinforced through other strategy documents, including the *National Strategy for Homeland Security* issued in July 2002, called for a range of activities intended to establish a partnership between the public and private sectors to ensure the security of our nation's critical infrastructures. To ensure coverage of critical infrastructure sectors, this policy identified infrastructure sectors that were essential to our national security, national economic security, and/or national public health and safety. For these sectors, which now total 14, federal government leads (sector liaisons) and private-sector leads (sector coordinators) were to work with each other to

[12] The Homeland Security Advisory System uses five levels (Severe, High, Elevated, Guarded, and Low) to inform federal, state, and local government agencies and authorities, the private sector, and the public of the nation's terrorist threat conditions.

address problems related to CIP for their sector. In particular, they were to (1) develop and implement vulnerability awareness and education programs and (2) contribute to a sectoral plan by

- assessing the vulnerabilities of the sector to cyber or physical attacks;
- recommending a plan to eliminate significant vulnerabilities;
- proposing a system for identifying and preventing major attacks; and
- developing a plan for alerting, containing, and rebuffing an attack in progress and then, in coordination with the Federal Emergency Management Agency as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

CIP policy also called for sector liaisons to identify and assess economic incentives to encourage the desired sector behavior in CIP. Federal grant programs to assist state and local efforts, legislation to create incentives for the private sector and, in some cases, regulation are mentioned in CIP policy.

Federal CIP policy also encourages the voluntary creation of information sharing and analysis centers (ISACs) to serve as mechanisms for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the federal government through NIPC. ISACs are critical since private-sector entities control over 80 percent of our nation's critical infrastructures. Their activities could improve the security posture of the individual sectors, as well as provide an improved level of communication within and across sectors and all levels of government. While PDD 63 encouraged the creation of ISACs, it left the actual design and functions of the ISACs, along with their relationship with NIPC, to be determined by the private sector in consultation with the federal government. PDD 63 did provide suggested activities, which the ISACs could undertake, including

- establishing baseline statistics and patterns on the various infrastructures;
- serving as a clearinghouse for information within and among the various sectors;
- providing a library for historical data for use by the private sector and government; and
- reporting private-sector incidents to NIPC.

As we reported in our April 8, 2003,[18] testimony, table 3 shows the sectors identified in federal CIP policy, the lead agencies for these sectors, and whether or not an ISAC has been established for the sector.

[18]U.S. General Accounting Office, *Information Security Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures*, GAO-03-564T (Washington, D.C.: Apr. 8, 2003).

Table 3: Lead Agencies and ISAC Status by CIP Sector

Sectors	Designated lead agency	ISAC established
Sectors identified by PDD 63		
Information and telecommunications	Homeland Security*	
Information technology		✓
Telecommunications		✓
Research and education networks		✓
Banking and finance	Treasury	✓
Water	Environmental Protection Agency	✓
Transportation	Homeland Security*	
Aviation		
Surface transportation		✓
Maritime		prospective
Trucking		✓
Emergency services**	Homeland Security*	
Emergency law enforcement		✓
Emergency fire services		✓
Government**	Homeland Security*	
Interstate		✓
Energy	Energy	
Electric power		✓
Oil and gas		✓
Public health	Health and Human Services	
Sectors identified by *The National Strategy for Homeland Security*		
Food		✓
Meat and poultry	Agriculture	
All other food products	Health and Human Services	
Agriculture	Agriculture	
Chemical industry and hazardous materials	Environmental Protection Agency	
Chemicals		✓
Defense industrial base	Defense	
Postal and shipping	Homeland Security	
National monuments and icons	Interior	
Other *communities* that have established ISACs		
Real estate		✓

*The lead agencies previously designated by PDD 63 were (from top to bottom) the Department of Commerce, Department of Transportation, Department of Justice/Federal Bureau of Investigation, and the Federal Emergency Management Agency.

**PDD 63 identified as critical sectors (1) emergency law enforcement and (2) emergency fire services and continuity of government. In the *National Strategy for Homeland Security*, emergency law enforcement and emergency fire services are both included in an emergency services sector. Also, continuity of government, along with continuity of operations, is listed as a subcomponent under the government sector.

As called for by the *National Strategy for Homeland Security*, on February 14, 2003, the President also released the *National Strategy to Secure Cyberspace* and the complementary *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. These two strategies identify priorities, actions, and responsibilities for the federal government (including lead agencies and DHS) as well as for state and local governments and the private sector. These two strategies also emphasize the importance of developing mechanisms for the

public and private sectors to share information about vulnerabilities, incidents, threats, and other security data. For example, the *National Strategy to Secure Cyberspace* calls for the development of a National Cyberspace Security Response System. To be coordinated by DHS, this system is described as a public/private architecture for analyzing and warning, managing incidents of national significance, promoting continuity in government systems and private-sector infrastructures, and increasing information sharing across and between organizations to improve cyberspace security. The system is to include governmental and nongovernmental entities, such as private-sector ISACs. The strategies also encourage the continued establishment of ISACs and efforts to enhance the analytical capabilities of existing ISACs.

As we previously reported, according to a DHS official, the department is continuing to carry out the CIP activities of the functions and organizations transferred to it by the Homeland Security Act of 2002.[14] And although NIPC has experienced the loss of certain senior leadership prior to its transition to the new department and has identified some staffing needs, this official stated that the department is able to provide the functions previously performed by NIPC. Further, he stated that the department is enhancing those activities as it integrates them within the new department and is developing a business plan. The official also stated that the department is continuing previously established efforts to maintain and build relationships with other federal entities, including the FBI and other NIPC partners, and with the private sector.

To fulfill its mission, the IAIP directorate will need to ensure effective information sharing with other federal entities. For example, information sharing with the recently formed Terrorist Threat Integration Center (TTIC) is a central function of the directorate. TTIC was created to merge and analyze terrorist-related information collected domestically and abroad to enhance coordination, facilitate threat analysis, and enable more comprehensive threat assessments. DHS plans to provide staff to work at TTIC, and the center is to provide DHS with a comprehensive assessment of threat information that will guide the department's response to any potential attacks. In addition, IAIP will need to establish effective information sharing with the numerous CIP entities not transferred to DHS. In July 2002, we issued a report identifying at least 50 organizations that were involved in national or multinational cyber CIP efforts, including 5 advisory committees, 6 Executive Office of the President organizations, 38 executive branch organizations associated with departments, agencies, or intelligence organizations, and 3 other organizations.[15] Only 5 of the CIP organizations transferred to DHS.

[14] GAO-03-564T.

[15] U.S. General Accounting Office, *Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems*, GAO-02-474 (Washington, D.C.: July 15, 2002).

The Directorate of Border and Transportation Security

According to the act, the Border and Transportation Security Directorate (BTS) is responsible for, among other things, (1) preventing the entry of terrorists and the instruments of terrorism into the United States; (2) securing the borders, territorial waters, ports, terminals, waterways, and air, land, and sea transportation systems, including managing and coordinating those functions transferred to the department; (3) carrying out immigration enforcement functions; (4) establishing and administering rules for granting visas, and (5) administering customs laws. A number of federal entities are under its responsibility, such as the Transportation Security Administration, U.S. Customs Service, the border security functions of the Immigration and Naturalization Service (INS), Animal and Plant Health Inspection Service, and the Federal Law Enforcement Training Center.

To successfully protect the borders and transportation systems of the United States, BTS faces the challenge of sharing information across the various organizations under its responsibility. According to the *National Strategy for Homeland Security*, to successfully prevent the entry of contraband, unauthorized aliens, and potential terrorists, DHS will have to increase the level of information available on inbound goods and passengers to the border management component agencies under the BTS. For example, the strategy discusses the need to increase the security of international shipping containers—noting that 50 percent of the value of U.S. imports arrives via 16 million containers. To increase security, U.S. inspectors will need shared information so that they can identify high-risk containers. In addition, protecting our borders from the entry of unauthorized aliens and potential terrorists will require the sharing of information between various law enforcement and immigration services. For example, we recently reported on the use of watch lists as important tools to help secure our nation's borders.[16] These lists provide decision makers with information about individuals who are known or suspected terrorists and criminals so that these individuals can either be prevented from entering the country, apprehended while in the country, or apprehended as they attempt to exit the country.

The Emergency Preparedness and Response Directorate

According to the act, the Emergency Preparedness and Response Directorate (EPR) ensures that the nation is prepared for, and able to recover from, terrorist attacks, major disasters, and other emergencies. In addition, EPR is responsible for building a comprehensive national incident management system with federal, state, and local governments and authorities to respond to such attacks and disasters. This project will require developing an extensive program of information sharing among federal, state and local governments. Further, EPR is

[16] U.S. General Accounting Office, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, GAO-03-322 (Washington, D.C: Apr. 15, 2003).

to develop comprehensive programs for developing interoperable communications technology and helping to ensure that emergency response providers acquire such technology. Among the functions transferred to EPR are the Federal Emergency Management Agency, the Integrated Hazard Information System of the National Oceanic and Atmospheric Administration, and the Metropolitan Medical Response System.

Information sharing is important to emergency responders to prepare for and respond to terrorist attacks and other emergencies. For example, if a biological attack were to occur, it would be important for health officials to quickly and effectively exchange information with relevant experts directly responding to the event in order to respond appropriately. To support this type of exchange, the Centers for Disease Control and Prevention (CDC) created the Epidemic Information Exchange (*Epi-X*), a secure, Web-based communications network that serves as an information exchange between CDC, state and local health departments, poison control centers, and other public health professionals. According to CDC, *Epi-X's* primary goals include informing health officials about important public health events, helping them respond to public health emergencies, and encouraging professional growth and the exchange of information. CDC has also created an emergency operations center to respond to public health emergencies and to allow for immediate secure communication between CDC, the Department of Health and Human Services, federal intelligence and emergency response officials, DHS, and state and local public health officials.

Information Sharing Challenges

GAO has made numerous recommendations over the last several years related to information sharing functions that have been transferred to DHS. One significant area of GAO work concerns the federal government's CIP efforts, which is focused on the sharing of information on incidents, threats, and vulnerabilities, and the providing of warnings related to critical infrastructures both within the federal government and between the federal government and state and local governments, and the private sector. Although improvements have been made in protecting our nation's critical infrastructures and continuing efforts are in progress, further efforts are needed to address the following critical CIP challenges that GAO has identified:

- developing a comprehensive and coordinated national plan to facilitate CIP information sharing, which clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets timeframes for achieving objectives, and establishes performance measures;
- developing fully productive information sharing relationships within the federal government and between the federal government and state and local governments and the private sector;

- improving the federal government's capabilities to analyze incident, threat, and vulnerability information obtained from numerous sources and share appropriate timely, useful warnings and other information concerning both cyber and physical threats to federal entities, state and local governments, and the private sector; and
- providing appropriate incentives for nonfederal entities to increase information sharing with the federal government.

In addition, GAO recently identified challenges in consolidating and standardizing watch list structures and policies, which are essential to effectively sharing information on suspected criminals and terrorists.

A Complete and Coordinated National CIP Plan Needs to Be Developed

An underlying issue in the implementation of CIP is that no national plan to facilitate information sharing yet exists that clearly delineates the roles and responsibilities of federal and nonfederal CIP entities, defines interim objectives and milestones, sets timeframes for achieving objectives, and establishes performance measures. Such a clearly defined plan is essential for defining the relationships among all CIP organizations to ensure that the approach is comprehensive and well coordinated. Since 1998, we have reported on the need for such a plan and made numerous related recommendations.

In September 1998, we reported that developing a governmentwide strategy that clearly defined and coordinated the roles of federal entities was important to ensure governmentwide cooperation and support for PDD 63.[17] At that time, we recommended that the Office of Management and Budget (OMB) and the Assistant to the President for National Security Affairs ensure such coordination.

In January 2000, the President issued *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue* as a first major element of a more comprehensive effort to protect the nation's information systems and critical assets from future attacks. The plan proposed achieving the twin goals of making the U.S. government a model of information security and developing a public/private partnership to defend our national infrastructures. However, this plan focused largely on federal cyber CIP efforts, saying little about the private-sector role.

In September 2001, we reported that agency questions had surfaced regarding specific roles and responsibilities of entities involved in cyber CIP and the timeframes within which CIP objectives were to be met, as well as guidelines for measuring progress.[18] Accordingly, we made several recommendations to

[17]U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, GAO/AIMD-98-92 (Washington, D.C.: Sept. 23, 1998).
[18]U.S. General Accounting Office, *Combating Terrorism: Selected Challenges and Related Recommendations*, GAO-01-822 (Washington, D.C.: Sept. 20, 2001).

supplement those we had made in the past. Specifically, we recommended that the Assistant to the President for National Security Affairs ensure that the federal government's strategy to address computer-based threats define

- specific roles and responsibilities of organizations involved in CIP and related information security activities;
- interim objectives and milestones for achieving CIP goals and a specific action plan for achieving these objectives, including implementing vulnerability assessments and related remedial plans; and
- performance measures for which entities can be held accountable.

In July 2002 we issued a report identifying at least 50 organizations that were involved in national or multinational cyber CIP efforts, including 5 advisory committees, 6 Executive Office of the President organizations, 38 executive branch organizations associated with departments, agencies, or intelligence organizations, and 3 other organizations.[19] Although our review did not cover organizations with national physical CIP responsibilities, the large number of organizations that we did identify as involved in CIP efforts presents a need to clarify how these entities coordinate their activities with each other. Our report also stated that PDD 63 did not specifically address other possible critical sectors and their respective federal agency counterparts. Accordingly, we recommended that the federal government's strategy also

- include all relevant sectors and define the key federal agencies' roles and responsibilities associated with each of these sectors, and
- define the relationships among the key CIP organizations.

In July 2002, the *National Strategy for Homeland Security* called for interim cyber and physical infrastructure protection plans that DHS would use to build a comprehensive national infrastructure plan. Implementing a well-developed plan is critical in effective coordination in times of crises. According to the strategy, the national plan is to provide a methodology for identifying and prioritizing critical assets, systems, and functions, and for sharing protection responsibility with state and local governments and the private sector. The plan is also to establish standards and benchmarks for infrastructure protection and provide a means to measure performance. The plan is expected to inform DHS on budgeting and planning for critical infrastructure protection activities and how to use policy instruments to coordinate between government and private entities to improve the security of our national infrastructures to appropriate levels. The strategy also states that the DHS is to unify the currently divided responsibilities for cyber and physical security. According to the department's November 2002 reorganization

[19]GAO-02-474.

plan, the Assistant Secretary for Infrastructure Protection is responsible for developing a comprehensive national infrastructure plan.

As discussed previously, in February 2003, the President issued the interim strategies—*The National Strategy to Secure Cyberspace* and *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (hereafter referred to in this testimony as the cyberspace security strategy and the physical protection strategy). These strategies identify priorities, actions, and responsibilities for the federal government, including federal lead departments and agencies and the DHS, as well as for state and local governments and the private sector. Both define strategic objectives for protecting our nation's critical assets. The physical protection strategy discusses the goals and objectives for protecting our nation's critical infrastructure and key assets from physical attack. The cyberspace security strategy provides a framework for organizing and prioritizing the individual and concerted responsibilities of all levels of government to secure cyberspace.

According to the physical protection strategy, across government, there are inconsistent methodologies to prioritize efforts to enhance critical infrastructure protection. This problem is compounded with ineffective communication among the federal, state, and local governments that has resulted in untimely, disparate, and at times conflicting communication between those who need it most. DHS has been given a primary role in providing cross-sector coordination to improve communication and planning efforts and serves as the single point of coordination for state and local governments on homeland security issues. To fulfill its role as the cross-sector coordinator, DHS will partner with state and local governments and the private sector to institute processes that are transparent, comprehensive, and results-oriented. This effort will include creating mechanisms for collaborative national planning efforts between the private and public sectors and for consolidating the individual sector plans into a comprehensive plan that will define their respective roles, responsibilities, and expectations.

The cyberspace security strategy is the counterpart to the physical protection strategy and provides the framework for organizing and prioritizing the individual and concerted responsibilities of all levels of government to secure cyberspace. DHS serves as the focal point for managing cybersecurity incidents that could impact the federal government or the national information infrastructure, and thus, plays a central role in executing the initiatives assigned in this strategy. While the cyberspace security strategy mentions the responsibility of DHS in creating a comprehensive national plan for securing resources and key infrastructures, much of the strategy's emphasis remains on coordinating and integrating various plans with the private sector.

Neither strategy (1) clearly indicates how the physical and cyber efforts will be coordinated; (2) defines the roles, responsibilities, and relationships among the key CIP organizations, including state and local governments and the private sector; (3) indicates time frames or milestones for their overall implementation or

for accomplishing specific actions or initiatives; nor (4) establishes performance measures for which entities can be held responsible. Until a comprehensive and coordinated plan is completed that unifies the responsibilities for cyber and physical infrastructures; identifies roles, responsibilities, and relationships for all CIP efforts; establishes time frames or milestones for implementation; and establishes performance measures, our nation risks not having a consistent and appropriate information sharing framework to deal with growing threats to its critical infrastructure.

Better Information Sharing on Threats and Vulnerabilities Must Be Implemented

Information sharing is a key element in developing comprehensive and practical approaches to defending against potential cyber and other attacks, which could threaten the national welfare. Information on threats, vulnerabilities, and incidents experienced by others can help identify trends, better understand the risks faced, and determine what preventive measures should be implemented. However, as we have reported in recent years, establishing the trusted relationships and information-sharing protocols necessary to support such coordination can be difficult. In addition, the private sector has expressed concerns about sharing information with the government and the difficulty of obtaining security clearances. Both Congress and the administration have taken steps to address information sharing issues in law and recent policy guidance, but their effectiveness will largely depend on how DHS implements its information sharing responsibilities.

A number of activities have been undertaken to build information-sharing relationships between the federal government and the private sector, such as InfraGard, the Partnership for Critical Infrastructure Security, efforts by the CIAO, and efforts by lead agencies to establish ISACs. For example, the InfraGard Program, which provides the FBI and NIPC with a means of securely sharing information with individual companies, has expanded substantially. By early January 2001, 518 entities were InfraGard members—up from 277 members in October 2000. Members include representatives from private industry, other government agencies, state and local law enforcement, and the academic community. As of February 2003, InfraGard members totaled over 6,700.

As stated above, PDD 63 encouraged the voluntary creation of ISACs to serve as the mechanism for gathering, analyzing, and appropriately sanitizing and disseminating information between the private sector and the federal government through NIPC. In April 2001, we reported that NIPC and other government entities had not developed fully productive information-sharing relationships but that NIPC had undertaken a range of initiatives to foster information sharing relationships with ISACs, as well as with government and international entities. We recommended that NIPC formalize relationships with ISACs and develop a plan to foster a two-way exchange of information between them.

In response to our recommendations, NIPC officials told us in July 2002 that an ISAC development and support unit had been created, whose mission was to enhance private-sector cooperation and trust so that it would result in a two-way sharing of information. As shown previously in table 3, as of April 8, 2003, DHS reported that there are 16 current ISACs, including ISACs established for sectors not identified as critical infrastructure sectors. DHS officials also stated that they have formal agreements with most of the current ISACs.

In spite of progress made in establishing ISACs, additional efforts are needed. All sectors do not have a fully established ISAC, and even for those sectors that do, our recent work showed that participation may be mixed and the amount of information being shared between the federal government and private-sector organizations also varies. Specifically, the five ISACs we recently reviewed[20] showed different levels of progress in implementing the PDD 63 suggested activities. For example, four of the five reported that efforts were still in progress to establish baseline statistics, which includes developing a database on the normal levels of computer security incidents that would be used for analysis purposes. Also, while all five reported that they serve as the clearinghouse of information (such as incident reports and warnings received from members) for their own sectors, only three of the five reported that they are also coordinating with other sectors. Only one of the five ISACs reported that it provides a library of incidents and historical data that is available to both the private sector and the federal government, and although three additional ISACs do maintain a library, it is available only to the private sector. Table 4 summarizes the reported status of the five ISACs in performing these and other activities suggested by PDD 63.

Table 4: ISACs' Progress in Performing Activities Suggested by PDD 63

	ISAC				
Activity	Telecommunications	Electricity	Information Technology	Energy	Water
Establish baseline statistics	In progress	In progress	Yes	In progress	In progress
Serve as clearinghouse within and among sectors	Yes	Yes	Yes	Only within own sector	Only within own sector
Provide library to private sector and government	In progress	Yes	Available only to private sector	Available only to private sector	Available only to private sector
Report incidents to NIPC	Yes	Yes	Yes	No	Yes

Source: ISACs.

Some in the private sector have expressed concerns about voluntarily sharing information with the government. Specifically, concerns have been raised that industry could potentially face antitrust violations for sharing information with other industry partners, have their information subject to the Freedom of Information Act (FOIA), or face potential liability concerns for information shared in good faith. For example, neither the IT nor the energy or the water ISACs share

[20] U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*, GAO-03-233 (Washington, D.C.: Feb. 28, 2003).

their libraries with the federal government because of concerns that information could be released under FOIA. And, officials of the energy ISAC stated that they have not reported incidents to NIPC because of FOIA and antitrust concerns.

There will be continuing debate as to whether adequate protection is being provided to the private sector as these entities are encouraged to disclose and exchange information on both physical and cyber security problems and solutions that are essential to protecting our nation's critical infrastructures. The *National Strategy for Homeland Security* includes "enabling critical infrastructure information sharing" in its 12 major legislative initiatives. It states that the nation must meet this need by narrowly limiting public disclosure of information relevant to protecting our physical and cyber critical infrastructures in order to facilitate the voluntary submission of information. It further states that the Attorney General will convene a panel to propose any legal changes necessary to enable sharing of essential homeland security related information between the federal government and the private sector.

Actions have already been taken by the Congress and the administration to strengthen information sharing. For example, the USA PATRIOT Act promotes information sharing among federal agencies, and numerous terrorism task forces have been established to coordinate investigations and improve communications among federal and local law enforcement.[21] Moreover, the Homeland Security Act of 2002 includes provisions that restrict federal, state, and local government use and disclosure of critical infrastructure information that has been voluntarily submitted to DHS. These restrictions include exemption from disclosure under FOIA, a general limitation on use to CIP purposes, and limitations on use in civil actions and by state or local governments. The act also provides penalties for any federal employee who improperly discloses any protected critical infrastructure information. Last month DHS issued for comment its proposed rules for how critical infrastructure information volunteered by the public will be protected. At this time, it is too early to tell what impact the act will have on the willingness of the private sector to share critical infrastructure information.

Information sharing within the government also remains a challenge. In April 2001, we reported that NIPC and other government entities had not developed fully productive information sharing and cooperative relationships.[22] For example, federal agencies had not routinely reported incident information to NIPC, at least in part because guidance provided by the federal Chief Information Officers Council, which is chaired by OMB, directs agencies to report such information to the Federal Computer Incident Response Center (FedCIRC).[23] Further, NIPC and Department of Defense officials agreed that their information-sharing procedures

[21]The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, Public Law No. 107-56, October 26, 2001.
[22]U.S. General Accounting Office, *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities*, GAO-01-323 (Washington, D.C.: April. 24, 2001).
[23]The Federal Computer Incident Response Center has been incorporated into the new Department of Homeland Security (DHS).

needed improvement, noting that protocols for reciprocal exchanges of information had not been established. In addition, the expertise of the U.S. Secret Service regarding computer crime had not been integrated into NIPC efforts. The NIPC director stated in July 2002 that the relationship between NIPC and other government entities had significantly improved since our review, and that quarterly meetings with senior government leaders were instrumental in improving information sharing. Also, in testimony in 2002, officials from the FedCIRC and the U.S. Secret Service discussed the collaborative and cooperative relationships that were subsequently formed between their agencies and NIPC.

Also, the private sector has expressed its concerns about the value of information being provided by the government. For example, in July 2002 the President for the Partnership for Critical Infrastructure Security stated in congressional testimony that information sharing between the government and private sector needs work, specifically, in the quality and timeliness of cyber security information coming from the government.[24] In March 2003 we also reported that the officials from the chemical industry noted that they need better threat information from law enforcement agencies, as well as better coordination among agencies providing threat information.[25] They stated that chemical companies do not receive enough specific threat information and that it frequently comes from multiple government agencies. Similarly, in developing a vulnerability assessment methodology to assess the security of chemical facilities against terrorist and criminal attacks, the Department of Justice observed that chemical facilities need more specific information about potential threats in order to design their security systems and protocols. Chemical industry officials also noted that efforts to share threat information among industry and federal agencies will be effective only if government agencies provide specific and accurate threat information. Threat information also forms the foundation for some of the tools available to industry for assessing facility vulnerabilities. The Justice vulnerability assessment methodology requires threat information as the foundation for hypothesizing about threat scenarios, which form the basis for determining site vulnerabilities.

The Homeland Security Act, *the President's National Strategy for Homeland Security, the National Strategy to Secure Cyberspace, and the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* all acknowledge the importance of information sharing and identify multiple responsibilities for DHS to share information on threats and vulnerabilities. In particular:

- The Homeland Security Act authorizes the IAIP Under Secretary to have access to all information in the federal government that concerns infrastructure or other vulnerabilities of the United States to terrorism and to use this information to

[24] Testimony of Kenneth C. Watson, President, Partnership for Critical Infrastructure Security, before the Subcommittee on Oversight and Investigation of the Energy and Commerce Committee, U.S. House of Representatives, July 9, 2002.
[25] U. S. General Accounting Office, *Homeland Security: Voluntary Initiatives Are Under Way at Chemical Facilities, but the Extent of Security Preparedness is Unknown*, GAO-03-439 (Washington D.C.: Mar. 14, 2003).

fulfill their responsibilities to provide appropriate analysis and warnings related to threats to and vulnerabilities of critical information systems, crisis management support in response to threats or attacks on critical information systems, and technical assistance upon request to private sector and government entities to respond to major failures of critical information systems.

- The *National Strategy for Homeland Security* specifies the need for DHS to work with state and local governments to achieve "seamless communication" among all responders. This responsibility includes developing a national emergency communication plan to establish policies and procedures to improve the exchange of information. Ensuring improved communications also involves developing systems that help prevent attacks and minimize damage. Such systems, which would be accessed and used by all levels of government, would detect hostile intents and help locate individual terrorists as well as monitor and detect outbreaks.

- The cyberspace security strategy encourages DHS to work with the National Infrastructure Advisory Council and the private sector to develop an optimal approach and mechanism to disclose vulnerabilities in order to expedite the development of solutions without creating opportunities for exploitation by hackers. DHS is also expected to raise awareness about removing obstacles to sharing information concerning cybersecurity and infrastructure vulnerabilities between the public and private sectors and is encouraged to work closely with ISACs to ensure that they receive timely and actionable threat and vulnerability data and to coordinate voluntary contingency planning efforts.

- The physical protection strategy describes DHS' need to collaborate with the intelligence community and the Department of Justice to develop comprehensive threat collection, assessment, and dissemination processes that are distributed to the appropriate entity in a timely manner. It also enumerates several initiatives directed to DHS to accomplish to create a more effective information-sharing environment among the key stakeholders, including establishing requirements for sharing information; supporting state and local participation with ISACs to more effectively communicate threat and vulnerability information; protecting secure and proprietary information deemed sensitive by the private sector; implementing processes for collecting, analyzing, and disseminating threat data to integrate information from all sources; and developing interoperable systems to share sensitive information among government entities to facilitate meaningful information exchange.

- The *National Strategy for Homeland Security* also describes DHS's need to engage its partners around the world in cooperative efforts to improve security. It states that DHS will increase information sharing between the international law enforcement, intelligence, and military communities.

Analysis and Warning Capabilities Need to Be Improved

Analysis and warning capabilities should be developed to detect precursors to attacks on the nation 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 analysis and warning capabilities to protect against strategic computer attacks against the nation's critical computer-dependent infrastructures. Such capabilities need to address both cyber and physical threats and involve (1) gathering and analyzing information for the purpose of detecting and reporting 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,[26] we reported on NIPC's progress and impediments in developing analysis and warning capabilities for computer-based attacks, which included the following:[27]

- Lack of a generally accepted methodology for analyzing strategic cyber-based threats. For example, there was no standard terminology, no standard set of factors to consider, and no established thresholds for determining the sophistication of attack techniques. According to officials in the intelligence and national security community, developing such a methodology would require an intense interagency effort and dedication of resources.
- Prolonged leadership vacancies and inadequate staff expertise, in part because other federal agencies had not provided the originally anticipated number of detailees. For example, at the close of our review in February 2001, the position of Chief of the Analysis and Warning Section, which was to be filled by the Central Intelligence Agency, had been vacant for about half of NIPC's 3-year existence. In addition, NIPC had been operating with only 13 of the 24 analysts that NIPC officials estimated were needed to develop analytical capabilities.
- Lack of industry-specific data on factors such as critical system components, known vulnerabilities, and interdependencies. Under PDD 63, such information is to be developed for each of eight industry segments by industry representatives and the designated federal lead agencies. However, at the close of our work, only three industry assessments had been partially completed, and none had been provided to NIPC. In September 2001, we reported that although outreach efforts had raised awareness and improved information sharing, substantive, comprehensive analysis of infrastructure sector interdependencies and vulnerabilities had been limited.

Another challenge confronting the analysis and warning capabilities of our nation is that, historically, our national CIP attention and efforts have been focused on

[26] GAO-01-323.
[27] Pursuant to the Homeland Security Act of 2002, the functions of NIPC (except for computer investigations and operations) were transferred over to DHS from the FBI.

cyber threats. As we also reported in April 2001, although PDD 63 covers both physical and cyber threats, federal efforts to meet the directive's requirements have pertained primarily to cyber threats, since this is an area that the leaders of the administration's CIP strategy view as needing attention. However, the terrorist attacks of September 11, 2001, have increased the emphasis of physical threats. In addition, in July 2002, NIPC reported that the potential for concurrent cyber and physical ("swarming") attacks is an emerging threat to the U.S. critical infrastructure. Further, in July 2002, the director of NIPC also told us that NIPC had begun to develop some capabilities for identifying physical CIP threats. For example, NIPC had developed thresholds with several ISACs for reporting physical incidents and, since January 2002, has issued several information bulletins concerning physical CIP threats. However, NIPC's director acknowledged that fully developing this capability would be a significant challenge. The physical protection strategy states that DHS will maintain a comprehensive, up-to-date assessment of vulnerabilities across sectors and improve processes for domestic threat data collection, analysis, and dissemination to state and local governments and private industry.

The administration and Congress continue to emphasize the need for these analysis and warning capabilities. The *National Strategy for Homeland Security* identified intelligence and warning as one of six critical mission areas and called for major initiatives to improve our nation's analysis and warning capabilities. The strategy also stated that no government entity was then responsible for analyzing terrorist threats to the homeland, mapping these threats to our vulnerabilities, and taking protective action. The Homeland Security Act gives such responsibility to the new DHS. For example, the IAIP Under Secretary is responsible for administering the Homeland Security Advisory System, and is to coordinate with other federal agencies to provide specific warning information and advice to state and local agencies, the private sector, the public, and other entities about appropriate protective measures and countermeasures to homeland security threats.

An important aspect of improving our nation's analysis and warning capabilities is having comprehensive vulnerability assessments. The President's *National Strategy for Homeland Security* also states that comprehensive vulnerability assessments of all of our nation's critical infrastructures are important from a planning perspective in that they enable authorities to evaluate the potential effects of an attack on a given sector and then invest accordingly to protect it. The strategy states that the U.S. government does not perform vulnerability assessments of the nation's entire critical infrastructure. The Homeland Security Act of 2002 states that the DHS's IAIP Under Secretary is to carry out comprehensive assessments of the vulnerabilities of key resources and critical infrastructures of the United States.

Another critical issue in developing effective analysis and warning capabilities is to ensure that appropriate intelligence and other threat information, both cyber and physical, is received from the intelligence and law enforcement communities.

For example, there has been considerable public debate regarding the quality and timeliness of intelligence data shared between and among relevant intelligence, law enforcement, and other agencies. Also, as the transfer of NIPC to DHS organizationally separated it from the FBI's law enforcement activities (including the Counterterrorism Division and NIPC field agents), it will be critical to establish mechanisms for continued communication to occur. Further, it will be important that the relationships between the law enforcement and intelligence communities and the new DHS are effective and that appropriate information is exchanged on a timely basis. The act gives DHS broad statutory authority to access intelligence information, as well as other information relevant to the terrorist threat and to turn this information into useful warnings. For example, DHS is to be a key participant in the multi-agency TTIC[28] that reportedly began operations on May 1, 2003. According to a White House fact sheet, DHS's IAIP is to receive and analyze terrorism-related information from the TTIC.[29] Although the purpose of TTIC and the authorities and responsibilities of the FBI and Central Intelligence Agency (CIA) counterterrorism organizations remain distinct, it has been reported that many details of the new center have not yet been finalized, including the types of reports that will be provided to other agencies.

In addition, according to NIPC's director, as of July 2002, a significant challenge in developing a robust analysis and warning function is the development of the technology and human capital capacities to collect and analyze substantial amounts of information. Similarly, the Director of the FBI testified in June 2002 that implementing a more proactive approach to preventing terrorist acts and denying terrorist groups the ability to operate and raise funds require a centralized and robust analytical capacity that did not exist in the FBI's Counterterrorism Division.[30] He also stated that processing and exploiting information gathered domestically and abroad during the course of investigations requires an enhanced analytical and data mining capacity that was not then available. According to DHS's reorganization plans, the IAIP Under Secretary and the CIO of the department are to fulfill their responsibilities as laid out by the act to establish and utilize a secure communications and IT infrastructure. This infrastructure is to include data-mining and other analytical tools in order to access, receive, analyze, and disseminate data and information.

Additional Incentives Are Needed to Encourage Increased Information Sharing Efforts

PDD 63 stated that sector liaisons should identify and assess economic incentives to encourage sector information sharing and other desired behavior. Consistent

[28] The center was formed from elements of the Department of Homeland Security, the FBI's Counterterrorism Division, the Director of Central Intelligence's Counterterrorist Center, and the Department of Defense.
[29] The White House, *Fact Sheet: Strengthening Intelligence to Better Protect America* (Washington, D.C.: Jan. 28, 2003).
[30] Testimony of Robert S. Mueller, III, Director Federal Bureau of Investigation, before the Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies, Committee on Appropriations, U.S. House of Representatives, June 21, 2002.

with the original intent of PDD 63, the *National Strategy for Homeland Security* states that, in many cases, sufficient incentives exist in the private market for addressing the problems of CIP. However, the strategy also discusses the need to use all available policy tools to protect the health, safety, or well-being of the American people. It mentions federal grant programs to assist state and local efforts, legislation to create incentives for the private sector, and, in some cases, regulation. The physical protection strategy reiterates that additional regulatory directives and mandates should only be necessary in instances where the market forces are insufficient to prompt the necessary investments to protect critical infrastructures and key assets. The cyberspace security strategy also states that the market is to provide the major impetus to improve cyber security and that regulation will not become a primary means of securing cyberspace.

Last year, the Comptroller General testified on the need for strong partnerships with those outside the federal government and that the new department would need to design and manage tools of public policy to engage and work constructively with third parties.[31] We have also previously testified on the choice and design of public policy tools that are available to governments.[32] These public policy tools include grants, regulations, tax incentives, and regional coordination and partnerships to motivate and mandate other levels of government or the private sector to address security concerns. Some of these tools are already being used, such as in the water and chemical sectors.

Without appropriate consideration of public policy tools, private sector participation in sector-related information sharing and other CIP efforts may not reach its full potential. For example, we reported in January 2003[33] on the efforts of the financial services sector to address cyber threats, including industry efforts to share information and to better foster and facilitate sectorwide efforts. We also reported on the efforts of federal entities and regulators to partner with the financial services industry to protect critical infrastructures and to address information security. We found that although federal entities had a number of efforts ongoing, Treasury, in its role as sector liaison, had not undertaken a comprehensive assessment of the potential public policy tools to encourage the financial services sector in implementing information sharing and other CIP-related efforts. Because of the importance of considering public policy tools to encourage private sector participation, we recommended that Treasury assess the need for public policy tools to assist the industry in meeting the sector's goals. In addition, in February 2003, we reported on the mixed progress five ISACs had made in accomplishing the activities suggested by PDD 63. We recommended that the responsible lead agencies assess the need for public policy tools to encourage

[31] U.S. General Accounting Office, *Homeland Security: Proposal for Cabinet Agency Has Merit, But Implementation Wil Pivotal to Success*, GAO-01-886T (Washington, D.C.: June 25, 2002).
[32] U.S. General Accounting Office, *Combating Terrorism: Enhancing Partnerships Through a National Preparedness Strategy*, GAO-02-549T (Washington, D.C.: Mar. 28, 2002).
[33] U.S. General Accounting Office, *Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats*, GAO-03-173 (Washington, DC,: Jan. 30, 2003).

increased private-sector CIP activities and greater sharing of intelligence and incident information between the sectors and the federal government.

The President's fiscal year 2004 budget request for the new DHS includes $829 million for information analysis and infrastructure protection, a significant increase from the estimated $177 million for fiscal year 2003. In particular, the requested funding for protection includes about $500 million to identify key critical infrastructure vulnerabilities and support the necessary steps to ensure that security is improved at these sites. Although it also includes almost $300 million for warning advisories, threat assessments, a communications system, and outreach efforts to state and local governments and the private sector, additional incentives may still be needed to encourage nonfederal entities to increase their CIP efforts.

Consolidating and Standardizing Watch List Structures and Policies

We recently reported on the terrorist and criminal watch list systems maintained by different federal agencies.[34] These watch lists are important information-sharing tools for securing our nation's borders against terrorists. Simply stated, watch lists can be viewed as automated databases that are supported by certain analytical capabilities. These lists contain various types of data, from biographical data–such as a person's name and date of birth–to biometric data such as fingerprints. Nine federal agencies,[35] which before the establishment of DHS spanned five different cabinet-level departments,[36] currently maintain 12 terrorist and criminal watch lists. These lists are also used by at least 50 federal, state, and local agencies.

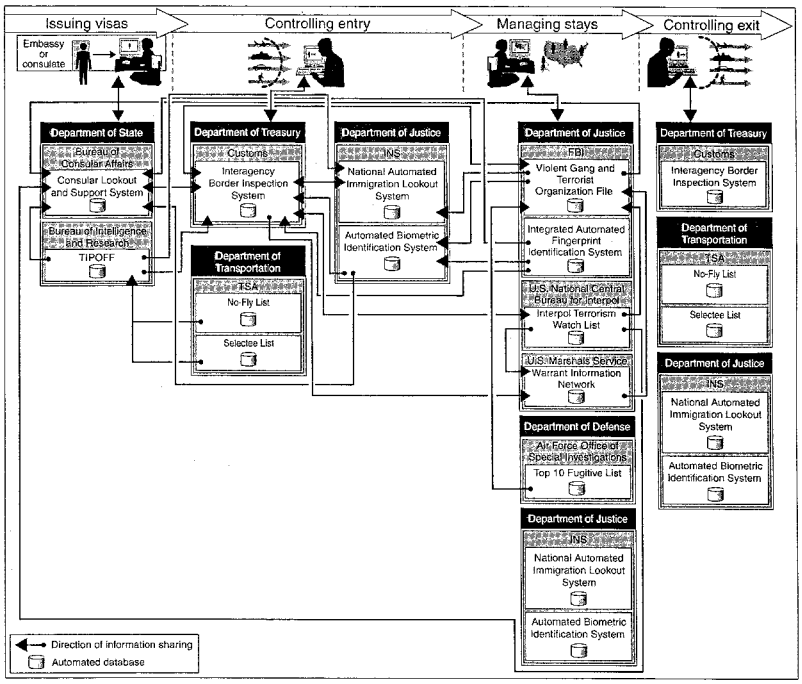
We found that the watch lists include overlapping but not identical sets of data, and that different policies and procedures govern whether and how these data are shared with others. As a general rule, we found that this information sharing is more likely to occur among federal agencies than between federal agencies and either state and local governments agencies or private entities. According to the *National Strategy for Homeland Security*, in the aftermath of the September 11th attacks, it became clear that vital watch list information stored in numerous and disparate databases was not available to the right people at the right time. In particular, federal agencies that maintained information about terrorists and other criminals had not consistently shared it. The strategy attributed these information-sharing limitations to legal, cultural, and technical barriers that resulted in the

[34] GAO-03-322.
[35] The nine agencies are the State Department's Bureau of Intelligence and Research and Bureau of Consular Affairs; the Justice Department's Federal Bureau of Investigation, Immigration and Naturalization Service, U.S. Marshals Service, and the U.S. National Central Bureau for Interpol; the Department of Defense's Air Force Office of Special Investigations; the Transportation Department's Transportation Security Administration; and the Treasury Department's U.S. Customs Service. Of these, the Immigration and Naturalization Service, the Transportation Security Administration, and the U.S. Customs Service have been incorporated into the new DHS.
[36] These departments are the Departments of State, Treasury, Transportation, Justice, and Defense.

watch lists being developed in different ways, for different purposes, and in isolation from one another. To address these limitations, the strategy provides for developing a consolidated watch list that would bring together the information on known or suspected terrorists contained in federal agencies' respective lists.

Further, we found that the extent to which such information sharing is accomplished electronically is constrained by fundamental differences in the watch lists' systems architecture. Agencies have developed their respective watch lists and managed their use in isolation from each other, in recognition of each agency's unique legal, cultural, and technological environments. The result is inconsistent and limited information sharing. We found that federal agencies that shared their watch list data with each other had developed and implemented their own interfaces with other federal agencies' watch lists. The consequence is the kind of overly complex, unnecessarily inefficient and potentially ineffective network that is associated with unstructured and nonstandard database environments. In particular, this environment consists of nine agencies–with 12 watch lists–that collectively maintain at least 17 interfaces. A simplified representation of the number of watch list interfaces and the complexity of the watch list environment is provided in figure 3.

Figure 3: Simplified Overview of the Border Security Process, Departments and Agencies Involved, Watch Lists Used, and Sharing Among Watch Lists



Sources: GAO (data), Nova Development Corp. (images).

As we recently reported, differences in agencies' cultures have been and remain one of the principal impediments to integrating and sharing information from watch lists and other information.

Finally, we found that not all of the nine agencies have policies and procedures governing the sharing of watch lists. In addition, each agency had different

policies and procedures on memorandums of understanding, ranging from one agency's not specifying any requirements to others' specifying in detail that such agreements should include how, when, and where information would be shared with other parties. We recommended that the Secretary of DHS, in collaboration with the heads of other departments and agencies that have or use watch lists, lead an effort to consolidate and standardize the federal government's watch list structures and policies to promote better integration and information sharing. DHS generally agreed with our findings and recommendations.

Effective Systems and Processes Need to Be Established to Facilitate Information Sharing

The success of homeland security relies on establishing effective systems and processes to facilitate information sharing among government entities and the private sector. In February 2003, the Chief Information Officer (CIO) of DHS stated that a key goal to protecting our nation is to put in place mechanisms that provide the right information to the right people all the time. He further stated that IT would provide homeland security officials throughout the United States with complete awareness of threats and vulnerabilities as well as knowledge of the personnel and resources available to conquer those threats. We have identified potential barriers and critical success factors to information sharing that DHS should consider. Also, in addition to the need to develop technological solutions, key management issues that DHS must overcome to achieve success include

- integrating existing IT resources of 22 different agencies,
- making new IT investments,
- ensuring that sensitive information is secured,
- developing secure communications networks,
- developing a performance focus,
- integrating staff from different organizations and ensuring that the department has properly skilled staff, and
- ensuring effective oversight.

Addressing these issues will be critical to establishing the effective systems and processes required to facilitate information sharing within the new department.

Potential Barriers to Information Sharing

GAO has previous reported numerous potential barriers to information sharing. that DHS faces, examples of which are summarized in table 5.[37] It will be important for the department to understand these barriers, consider any related provisions of the Homeland Security Act of 2002, and develop appropriate strategies to address them.

Table 5: Potential Barriers to Information Sharing

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 are 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. • Reluctance to disclose corporate information.
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. • Difficulty obtaining security clearances for nonfederal personnel. • Quality (specific, accurate, and actionable) and timeliness of information received from the federal government.
Coordinating law enforcement and intelligence activities	• Law enforcement and intelligence agencies may 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 between agencies.

[37]U.S. General Accounting Office, *National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy*, GAO-02-811T (Washington, D.C.: June 7, 2002), GAO-02-24, and GAO-03-233.

Where information sharing can potentially break down	Why
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.

Source: GAO.

Success Factors for Sharing Information

In October 2001, we reported on information sharing practices of organizations that successfully share sensitive or time-critical information.[38] We found that these practices include:

- establishing trust relationships with a wide variety of federal and nonfederal entities that may be in a position to provide potentially useful information and advice on vulnerabilities and incidents;
- developing standards and agreements on how shared information will be used and protected;
- establishing effective and appropriately secure communications mechanisms; and
- taking steps to ensure that sensitive information is not inappropriately disseminated.

Among the organizations we studied, we found some very good models to learn from and build on. For example, CERT/CC is charged with establishing a capability to quickly and effectively coordinate communication between experts in order to limit damage, responding to incidents, and building awareness of security issues across the Internet community. In this role, CERT/CC receives Internet security-related information from system and network administrators, technology managers, and policymakers and provides them with this information along with guidance and coordination to major security events. Further, the Agora is a Seattle-based regional network that at the time of our study had over 600 professionals representing various fields, including information systems security; law enforcement; local, state, and federal governments; engineering; IT; 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.

[38] U.S. General Accounting Office, *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*, GAO-02-24 (Washington, D.C.: Oct. 15, 2001).

In addition, we have previously reported on several other key considerations in establishing effective information sharing, including:

- identifying and agreeing on the types of information to be collected and shared between parties,
- developing standard terms and reporting thresholds,
- balancing varying interests and expectations, and
- determining the right format and standards for collecting data so that disparate agencies can aggregate and integrate data sets.

Some efforts have already taken place in these areas. For example, NIPC obtained information sharing agreements with most information sharing and analysis centers, which included specific reporting thresholds for physical and cyber incidents. Also, incident reporting thresholds have been publicly issued. It will be important for DHS to incorporate these considerations into its information sharing efforts.

Developing Technological Solutions

Developing and implementing appropriate technological solutions can improve the effectiveness and efficiency of information sharing. We have previously reported on the lack of connectivity and interoperability between databases and technologies important to the homeland security effort.[39] Databases belonging to federal law enforcement agencies and INS, for example, are not connected, and databases between state, local, and federal governments are not always connected. The technological constraints caused by different system architectures that impede the sharing of different agencies' watch lists illustrate the widespread lack of interoperability of many federal government information systems.

New technologies for data integration and interoperability could enable agencies to share information without the need for radical structural changes. This would allow the component agencies of DHS to work together yet retain a measure of autonomy, thus removing some barriers hindering agencies from embracing change. In August 2002,[40] we reported on various existing technologies that could be more widely implemented to facilitate information sharing. We reported that Extensible Markup Language (XML) is useful for better information sharing. XML is a flexible, nonproprietary set of standards for annotating or "tagging" information so that it can be transmitted over a network such as the Internet and readily interpreted by disparate computer systems. If implemented broadly with

[39] GAO-02-811T
[40] U.S. General Accounting Office, *National Preparedness: Technology and Information Sharing Challenges*, GAO-02-1048R (Washington, D.C.: Aug. 30, 2002).

consistent data definitions and structures, XML offers the promise of making it significantly easier for organizations and individuals to identify, integrate, and process information that may be widely dispersed among systems and organizations. For example, law enforcement agencies could potentially better identify and retrieve information about criminal suspects from any number of federal, state, and local databases.

We also reported that various technologies could be used to protect information in shared databases. For example, data could be protected through electronically secured entry technology (ESET). ESET would allow users of separate databases to cross check or "mine" data securely without directly disclosing their information to others, thus allowing agencies to collaborate as well as address their needs for confidentiality or privacy. Such technology could, for example, allow an airline to cross check a passenger or employee against data held by government agencies in a single-step process without actually disclosing the data to the airline. In checking an individual, the airline would not receive any data from the agencies' databases, rather it would receive a "yes or no" type response and/or a referral for further action. Additionally, appropriate authorities could automatically be notified.

We noted that intrusion detection systems could be used to prevent unauthorized users from accessing shared information. Intrusion detection uses normal system and network activity data as well as known attack patterns. Deviations from normal traffic patterns can help to identify potential intruders.

We also observed the need to simplify the process of analyzing information to more efficiently and effectively identify information of consequence that must be shared. Great emphasis has been placed upon data mining and data integration, but the third and perhaps most crucial component may be data visualization. The vast amount of information potentially available to be mined and integrated must be intelligently analyzed, and the results effectively presented, so that the right people have the right information necessary to act effectively upon such information. This may involve pinpointing the relevant anomalies.

Before DHS was established, OHS had already begun several technological initiatives to integrate terrorist-related information from databases from different agencies responsible for homeland security. These included (1) adopting meta-data standards for electronic information so that homeland security officials understood what information was available and where it could be found and (2) developing data-mining tools to assist in identifying patterns of criminal behavior so that suspected terrorists could be detained before they could act.

To address these technological challenges, the Homeland Security Act emphasized investments in new and emerging technologies to meet some of these challenges and established the Science and Technology Directorate, making it responsible for establishing and administering research and development efforts and priorities to support DHS missions.

Improving Information Technology Management

Improving IT management will be critical to transforming the new department. DHS should develop and implement an enterprise architecture, or corporate blueprint, to integrate the many existing systems and processes required to support its mission. This architecture will also guide the department's investments in new systems to effectively support homeland security in the coming years. Other key IT management capacities that DHS will need to establish include investment and acquisition management processes, effective IT security, and secure communications networks.

An Enterprise Architecture

Effectively managing a large and complex endeavor requires, among other things, a well-defined and enforced blueprint for operational and technological change, commonly referred to as an enterprise architecture. Developing, maintaining, and using enterprise architectures is a leading practice in engineering both individual systems and entire enterprises. Enterprise architectures include several components, including a (1) current or "as is" environment, (2) target or "to be" environment, and (3) transition plan or strategy to move from the current to the target environment. Governmentwide requirements for having and using architectures to guide and constrain IT investment decisionmaking are also addressed in federal law and guidance.[41] Our experience with federal agencies has shown that attempts to transform IT environments without enterprise architectures often result in unconstrained investment and systems that are duplicative and ineffective. Moreover, our February 2002 report on the federal agencies' use of enterprise architectures found that their use of enterprise architectures was a work in progress, with much to be accomplished.[42]

DHS faces tremendous IT challenges because programs and agencies have been brought together in the new department from throughout the government, each with their own information systems. It will be a major undertaking to integrate these diverse systems to enable effective information sharing among themselves, as well as with those outside the department.

The Office of Homeland Security has acknowledged that an enterprise 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. Furthermore, the President's homeland security strategy identifies, among other things, the lack of an enterprise architecture as an impediment to DHS's systems interoperating effectively and efficiently. Finally, the CIO of DHS has stated that the most

[41] U.S. General Accounting Office, *Business Systems Modernization: Longstanding Management and Oversight Weaknesses Continue to Put Investments at Risk*, GAO-03-553T (Washington, D.C.: Mar. 31, 2003).
[42] U.S. General Accounting Office, *Information Technology: Enterprise Architecture Use across the Federal Government Can Be Improved*, GAO-02-6 (Washington, D.C.: Feb.19, 2002).

important function of his office will be to design and help implement a national enterprise architecture that will guide the department's investment in and use of IT. As part of its enterprise development efforts, the department has established working groups comprising state and local CIOs to ensure that it understands and represents their business processes and strategies relevant to homeland security. In addition, OMB, in its current review of DHS's redundant IT for consolidation and integration, has taken an initial first step to evaluate DHS's component systems.[43] The CIO has set two milestones for developing the enterprise architecture. By June 2003, he intends to complete a baseline inventory of the department's current IT resources and business processes, and by August 2003 he intends to complete the future enterprise architecture. No target date has been provided for the transition plan to move from the current to the target environment.

In June 2002, we recommended that the federal government develop an architecture that defined the homeland security mission and the information, technologies, and approaches necessary to perform the mission in a way that was divorced from organizational parochialism and cultural differences.[44] Specifically, we recommended that the architecture 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. We observed that a particularly critical function of a homeland security architecture would be to establish protocols and standards for data collection to ensure that data being collected were usable and interoperable and to tell people what they needed to collect and monitor.

The CIO Council, OMB, and GAO have collaborated to produce guidance on the content, development, maintenance, and implementation of architectures that could be used in developing an architecture for DHS.[45] In April, we issued an executive guide on assessing and improving enterprise architecture management that extends this guidance.[46]

Investment and Acquisition Management Processes

The Clinger-Cohen Act, federal guidance, and recognized best practices provide a framework for organizations to follow to effectively manage their IT investments. This involves having a single, corporate approach governing how an organization's IT investment portfolio is selected, controlled, and evaluated across its various components, including assuring that each investment is aligned with the

[43] Office of Management and Budget, *Reducing Redundant IT Infrastructure Related to Homeland Security, Memorandum for the Heads of Selected Departments and Agencies*, July 19, 2002, M-02-12.
[44] GAO-02-811T.
[45] See Chief Information Officer Council, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0, (Washington, D.C.: Feb. 2001).
[46] U.S. General Accounting Office, *Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management (Version 1.1)*, GAO-03-584G (Washington, D.C.: April 2003).

organization's enterprise architecture. The lack of effective processes can lead to cost, schedule, and performance shortfalls, and in some cases, to failed system development efforts. GAO has issued numerous reports on agency investment and acquisition management challenges, including INS, which have been transferred into DHS.

INS has had long-standing difficulty developing and fielding information systems to support its program operations. Since 1990, we have reported that INS managers and field officials did not have adequate, reliable, and timely information to effectively carry out the agency's mission. For example, INS's benefit fraud investigations have been hampered by a lack of integrated information systems.[47] Also, INS's alien address information could not be fully relied on to locate many aliens who were believed to be in the country and who might have knowledge that would assist the nation in its antiterrorism efforts.[48] Contributing to this situation was INS's lack of written procedures and automated controls to help ensure that reported changes of address by aliens are recorded in all of INS's automated databases. Our work has identified weaknesses in INS's IT management capacities as the root cause of its system problems, and we have made recommendations to correct the weaknesses. INS has made progress in addressing our recommendations.

In a briefing to the House Appropriations Committee in February, the DHS CIO stated that his objective was to develop an IT investment review process by March 2003. Moreover, he set March as the milestone for finalizing the identification of all of DHS's mission-critical applications and February of next year as the milestone for having evaluated all major applications and investments in view of prioritizing actions to either renew or retire them.

Sound acquisition management is also central to accomplishing the department's mission. One of the largest federal departments, DHS will potentially have one of the most extensive acquisition requirements in government. The new department is expected to acquire a broad range of technologies and services from private-sector companies.

Moreover, DHS is faced with the challenge of integrating the procurement functions of many of its constituent programs and missions. Inherited challenges exist in several of the incoming agencies. For example, Customs has major procurement programs under way that must be closely managed to ensure that it achieves expectations. Despite some progress, we reported that Customs still lacks important acquisition management controls.[49] For its new import processing system, Customs has not begun to establish process controls for determining

[47] U.S. General Accounting Office, *Immigration Benefit Fraud: Focused Approach Is Needed to Address Problems*, GAO-02-66 (Washington, D.C.: Jan. 31, 2002).
[48] U.S. General Accounting Office, *Homeland Security: INS Cannot Locate Many Aliens Because It Lacks Reliable Address Information*, GAO-03-188 (Washington, D.C.: Nov. 21, 2002).
[49] U.S. General Accounting Office, *Customs Service Modernization: Management Improvements Needed on High-Risk Automated Commercial Environment Project*, GAO-02-545 (Washington, D.C.: May 13, 2002).

whether acquired software products and services satisfy contract requirements before acceptance, nor to establish related controls for effective and efficient transfer of acquired software products to the support organization responsible for software maintenance. Agreeing with one of our recommendations, Customs continues to make progress and plans to establish effective acquisition process controls.

Getting the most from its IT investment will depend on how well the department manages its acquisition activities. High-level attention to strong system and service acquisition management practices is critical to ensuring success.

Information Security Challenges

The Federal Information Security Management Act of 2002 requires federal agencies to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency, and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.[80] Further, the Homeland Security Act specifically requires DHS to establish procedures to ensure the authorized use and the security and confidentiality of information shared with the department, including information on threats of terrorism against the United States; infrastructure or other vulnerabilities to terrorism; and threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack. However, establishing an effective information security program may present significant challenges for DHS, which must bring together programs and agencies from throughout the government and integrate their diverse communications and information systems to enable effective communication and information sharing both within and outside the department.

Since 1996, we have reported that poor information security is a widespread problem for the federal government with potentially devastating consequences.[81] Further, we have identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2003.[82] Although agencies have taken steps to redesign and strengthen their information system security programs, our analyses of information security at major federal agencies have shown that federal systems were not being adequately protected

[80] *Title III—Federal Information Security Management Act of 2002, E-Government Act of 2002*, P.L. 107-347, December 17, 2002. This act superseded an earlier version of FISMA that was enacted as Title X of the Homeland Security Act of 2002.
[81] U.S. General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices*, GAO/AIMD-96-110 (Washington, D.C.: Sept. 24, 1996).
[82] U.S. General Accounting Office, *High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*, GAO-03-121 (Washington, D.C.: January 2003).

from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. For the past several years, we have analyzed audit results for 24 of the largest federal agencies,[53] and our latest analyses, of audit reports issued from October 2001 through October 2002, continued to show significant weaknesses in federal computer systems that put critical operations and assets at risk.[54] In particular, we found that all 24 agencies had weaknesses in security program management, which is fundamental to the appropriate selection and effectiveness of the other categories of controls and covers a range of activities related to understanding information security risks, selecting and implementing controls commensurate with risk, and ensuring that the controls implemented continue to operate effectively. In addition, we found that 22 of the 24 agencies had weaknesses in access controls—weaknesses that can make it possible for an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage, or in today's increasingly interconnected computing environment, can expose an agency's information and operations to attacks from remote locations all over the world by individuals with only minimal computer and telecommunications resources and expertise. In April 2003,[55] we also reported that many agencies still had not established information security programs consistent with requirements originally prescribed by government information security reform legislation[56] and now permanently authorized by the Federal Information Security Management Act.

Considering the sensitive and classified information to be maintained and shared by DHS, it is critical that the department implement federal information security requirements to ensure that its systems are appropriately assessed for risk and that adequate controls are implemented and working properly. Federal information security guidance, such as that issued by the National Institute of Standards and Technology (NIST), can aid DHS in this process. For example, NIST has issued guidance to help agencies perform self-assessments of their information security programs, conduct risk assessments, and use metrics to determine the adequacy of in-place security controls, policies, and procedures.[57] In addition, as we have previously reported, agencies need more specific guidance

[53]U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, GAO/AIMD-98-92 (Washington, D.C.: Sept. 23, 1998); *Information Security: Serious* and *Widespread Weaknesses Persist at Federal Agencies*, GAO/AIMD-00-295 (Washington, D.C.: Sept. 6, 2000); *Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets*, GAO-02-231T (Washington, D.C.: Nov. 9, 2001), and *Computer Security: Progress Made, but Critical Federal Operations and Assets Remain at Risk*, GAO-02-303T (Washington, D.C.: Nov. 19, 2002).
[54]GAO-03-303T.
[55] GAO-03-564T.
[56]Title X, Subtitle G—Government Information Security Reform, *Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001*, P.L.106-398, October 30, 2000.
[57]National Institute of Standards and Technology, Security Self-Assessment Guide for Information Technology Systems, NIST Special Publication 800-26, November 2001; Risk Management Guide for Information Technology Systems – Recommendations of the National Institute of Standards and Technology, Special Publication 800-30, January 2002; Security Metrics Guide for Information Technology Systems, NIST Draft Special Publication 800-55 (October 2002).

on the controls that they need to implement to help ensure adequate protection.[58] Currently, agencies have wide discretion in deciding which computer security controls to implement and the level of rigor with which to enforce these controls. One set of specific controls will not be appropriate for all types of systems and data, but our studies of best practices at leading organizations have shown that more specific guidance is important.[59] In particular, specific mandatory standards for varying risk levels can clarify expectations for information protection, including audit criteria; provide a standard framework for assessing information security risk; help ensure that shared data are appropriately protected; and reduce demands for limited resources to independently develop security controls. Responding to this need, the Federal Information Security Management Act (FISMA) requires NIST to develop, for systems other than national security systems, (1) standards to be used by all agencies to categorize all of their information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category.

DHS has identified implementing its information security program as a year one objective. In continuing these efforts, it is important that DHS consider establishing processes to annually review its information security program and to collect and report data on the program, as required by FISMA and OMB.

Secure Communications Networks

The "Homeland Security Information Sharing Act," included in the Homeland Security Act of 2002, provides for the President to prescribe and implement procedures for federal agencies to share homeland security and classified information with others, such as state and local governments, through information sharing systems. Provisions of the act depict the type of information to be shared as that which reveals a threat of actual or potential attack or other hostile acts. Grand jury information; electronic, wire, or oral information; and foreign intelligence information are all included in these provisions. The *National Strategy for Homeland Security* also refers to the need for a secure intranet to increase the flow of classified federal information to state and local entities. According to the strategy, this network would provide a more effective way to share information about terrorists. The strategy also refers to putting into place a secure communications network to allow agencies to share information in their existing databases.

[58]GAO-03-121.
[59]U.S. General Accounting Office, *Information Security Management: Learning From Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

To ensure the safe transmittal of sensitive, and, in some cases, classified, information vertically among everyone from intelligence entities, including the CIA, to local entities, such as those involved in emergency response and law enforcement, as well as horizontally across the same levels of government, requires developing and implementing communications networks with adequate security to protect the confidentiality, integrity, and availability of the transmitted information. Furthermore, these communications networks must be accessible to a variety of parties, from federal agencies to state and local government entities and some private entities.

There appear to be many efforts under way to implement secure networks. For example, according to the recently published the cyberspace security strategy, DHS intends to develop a national cyberspace security response system, the Cyber Warning Information Network (CWIN), to provide crisis management support to government and non-government network operation centers. CWIN is envisioned as providing private and secure network communications for both government and industry for the purpose of sharing cyber alert and warning information. Moreover, the National Communications System, one of the 22 entities that were merged into the DHS, has implemented a pilot system, the Global Early Warning Information System (GEWIS), which will measure how critical areas of the Internet are performing worldwide and then use that data to notify government, industry, and allies of impending cyberattacks or possible disturbances.

Other agencies are also engaged in efforts to provide homeland security networking and information management support for crisis management activities. Earlier, in 2001, the President's Advisor for Cyberspace Security outlined the high-level functional requirements for a private, secure network called GovNet. Department of Defense officials have also stated that the Army National Guard's network GuardNet, which was used to communicate among the states and the District of Columbia during the 9/11 terrorist attacks, is being considered for homeland security mission support.

It was also recently reported that the Justice Department and the FBI are expanding two existing sensitive but unclassified law enforcement networks to share homeland security information across all levels of government. When fully deployed, their Antiterrorism Information Exchange (ATIX) will provide law enforcement agencies at all levels access to information. Law enforcement agencies also can use ATIX to distribute security alerts to private-sector organizations and public officials who lack security clearances. Users, who will have different access levels on a need-to-know basis, will include a broad range of public safety and infrastructure organizations, including businesses that have homeland security concerns and duties. They will have access to a secure e-mail system via a secure Intranet, which the FBI and DHS will use to deliver alerts to ATIX users. The FBI and other federal agencies, including DHS, will link to ATIX via Law Enforcement Online, the bureau's system for sensitive-but-unclassified law enforcement data that provides an encrypted communications service for law

enforcement agencies on a virtual private network. The second Department of Justice and FBI network, the Multistate Antiterrorism Regional Information Exchange System, will enable crime analysts working on terrorism investigations to quickly check a broad range of criminal databases maintained by federal, state, and local agencies.

In March of this year, it was also reported that DHS's CIO had announced that DHS is opening up a network for secure videoconferencing to communicate with the nation's governors in the event of another terrorist attack. The CIO has also stated that a major initiative in implementing the department's IT strategy for providing the right information to the right people at all times is establishing the DHS Information Sharing Network Pilot project. Moreover, he sets 2005 as a milestone for DHS to build a "network of networks." However, no specifics on the latter two projects have been provided.

Managing Performance

As we have previously reported,[60] the new department has the challenge of developing a national homeland security performance focus, which relies on related national and agency strategic and performance planning efforts of the OHS, OMB, and the other departments and agencies. Indeed, the individual planning activities of the various component departments and agencies represent a good start in the development of this focus. However, our past work on implementation of the Government Performance and Results Act (GPRA) has highlighted ongoing difficulty with many federal departments and agencies setting adequate performance goals, objectives, and targets. Accordingly, attention is needed to developing and achieving appropriate performance expectations and measures for information sharing and in ensuring that there is linkage between DHS's plans, other agencies' plans, and the national strategies regarding information sharing. Ensuring these capabilities and linkages will be vital in establishing comprehensive planning and accountability mechanisms that will not only guide DHS's efforts but also help assess how well they are really working.

As we previously reported to this committee,[61] one of the barriers the new department faces in establishing effective homeland security is interagency cooperation, which is largely attributed to "turf" issues among the 22 component agencies subsumed by the new department. Strong and sustained commitment of agency leaders would provide performance incentives to managers and staff to break down cultural resistance and encourage more effective information sharing pertaining to homeland security. Moreover, agency leaders have a wide range of tools at their disposal for enforcing and rewarding cooperative efforts, including

[60] U.S. General Accounting Office, *Major Management Challenges and Program Risks: Department of Homeland Security*, GAO-03-102 (Washington, D.C.: January 2003).
[61] GAO-02-1048R.

performance bonuses for senior executives and incentive award programs for staff.

Our studies of other cross-cutting federal services with similar "turf" problems have also shown that agency performance plans, which are required by GPRA, offer a good avenue for developing incentives to cooperate. Specifically, agencies can set up goals in their performance plans for participation in cross-cutting programs and report on their progress in meeting these goals to Congress. Congress could also build similar incentives into budget resolutions.

Shared programmatic goals and metrics would also encourage cooperation and coordination. Agencies subsumed by DHS should all participate in the development of goals, milestones, and metrics to measure progress and success, and such indicators should be clearly articulated and endorsed by senior management. Such goals and metrics must be carefully chosen since how performance is measured greatly influences the nature of the performance itself; poorly chosen metrics may lead to unintended or counter-productive results. However, visible, clearly articulated and carefully chosen shared goals and metrics can effectively overcome "turf" issues. Developing metrics to measure the success of these activities is critical to ensuring a successful effort. Similar indicators more directly related to information sharing could be developed.

Emphasizing Human Capital

Human capital is another critical ingredient required for ensuring successful information sharing for homeland security. The cornerstones to effective human capital planning include leadership; strategic human capital planning; acquiring, developing, and retaining talent; and building results-oriented organizational cultures. The homeland security and intelligence communities must include these factors in their management approach in order to benefit from effective collaboration in this critical time.

As we have previously reported, the government-wide increase in homeland security activities has created a demand for personnel with skills in areas such as IT, foreign language proficiencies, and law enforcement, without whom critical information has less chance of being shared, analyzed, integrated, and disseminated in a timely, effective manner.[62] We specifically reported that shortages in staffing at some agencies had exacerbated backlogs in intelligence and other information, adversely affecting agency operations and hindering U.S. military, law enforcement, intelligence, counterterrorism, and diplomatic efforts.[63]

[62] GAO-02-1122T.
[63] U.S. General Accounting Office, *Foreign Languages: Human Capital Approach Needed to Correct Staffing and Proficiency Shortfalls*, GAO-02-375 (Washington, D.C.: January 2002).

We have also previously reported that some of the agencies that moved into DHS have long-standing human capital problems that will need to be addressed. One of these challenges has been the ability to hire and retain a talented and motivated staff. For example, we reported that INS has been unable to reach its program goals in large part because of such staffing problems as hiring shortfalls and agent attrition.[64] We also reported that several INS functions have been affected by the lack of a staff resource allocation model to identify staffing needs.[65] We concluded then that it was likely that increased attention to the enforcement of immigration laws and border control would test the capacity of DHS to hire large numbers of inspectors for work at our nation's border entry points. Moreover, we reported that other agencies being integrated into DHS were also expected to experience challenges in hiring security workers and inspectors. For example, we reported that the Agriculture Department, the Customs Service, INS, and other agencies were all seeking simultaneously to increase the size of their inspections staffs.[66]

To overcome its significant human capital shortfalls, DHS must develop a comprehensive strategy capable of ensuring that the new department can acquire, develop, and retain the skills and talents needed to prevent and protect against terrorism. This requires identifying skill needs; attracting people with scarce skills into government jobs; melding diverse compensation systems to support the new department's many needs; and establishing a performance-oriented, accountable culture that promotes employee involvement and empowerment. In February, the DHS CIO acknowledged the lack of properly skilled IT staff within the component agencies. Challenges facing DHS in this area, he stated, include overcoming political and cultural barriers, leveraging cultural beliefs and diversity to achieve collaborative change, and recruiting and retaining skilled IT workers. He acknowledged that the department would have to evaluate the talent and skills of its IT workforce to identify existing skill gaps. He further stated that a critical component of DHS's IT strategic plan would address the actions needed to train, reskill, or acquire the necessary skills to achieve a world-class workforce. He committed to working closely with the department's Chief Human Capital Officer and with the Office of Personnel Management to achieve this goal. He set July 2003 as a milestone for developing a current inventory of IT skills, resources, and positions and September 2003 as the targeted date for developing an action plan.

[64] U.S. General Accounting Office, *Immigration Enforcement: Challenges to Implementing the INS Interior Enforcement Strategy*, GAO-02-861T (Washington, D.C.: June 19, 2002).
[65] U.S. General Accounting Office, *Immigration and Naturalization Service: Overview of Recurring Management Challenges*, GAO-02-168T (Washington, D.C.: Oct. 17, 2001).
[66] GAO-03-260.

Ensuring Institutional Oversight

It is important to note that accountability is also a critical factor in ensuring the success of the new department. The oversight entities of the executive branch–including the Inspectors General, OMB and OHS–have a vital role to play in ensuring expected performance and accountability. Likewise, congressional committees and GAO, as the investigative arm of the legislative branch, with their long-term and broad institutional roles, also have roles to play in overseeing that the new department meets the demands of its homeland security mission.

In conclusion, our country is at a critical point in its history where information sharing with and between all levels of government and the private sector must become an integral part of everyday operations if we are to be able to identify terrorist threats and protect against attack. As such, information sharing is an essential part of DHS's responsibilities and is critical to achieving its mission. To implement these responsibilities, DHS will need to develop effective information sharing systems and other information sharing mechanisms, as well as develop strategies to address other challenges in establishing its organization and information architecture and in developing effective working relationships, cooperation, and trust with other federal agencies, state and local governments, and the private sector.

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

If you should have any questions about this testimony, please contact me at (202) 512-3317. I can also be reached by e-mail at daceyr@gao.gov.

310191

Chairman TOM DAVIS. Thank you very much.

Mr. Hite, are you there for questions?

Mr. HITE. Yes, sir, we have one combined oral statement.

Chairman TOM DAVIS. OK, that is great.

Welcome back before this committee, and thanks again for the job you did at IRS. We are happy to have you here.

Mr. ROSSOTTI. I am happy to share some observations based on my own experience at the IRS and previously at AMS. I would like to note that I have no special knowledge of the problems facing the Department of Homeland Security. Therefore, since every situation is unique, my observations are not intended or are not suggested as specific recommendations for DHS.

I do know that bringing together and transforming the work of large, fragmented organizations is a very difficult, costly, and in some ways a risky endeavor. I must say that Secretary Ridge and Mr. Cooper and their colleagues have taken on a very difficult job on behalf of the country. We need to give them all the support that we can.

When Congress passed the IRS reform bill, it directed major changes in the IRS, and there were a lot of questions raised at the time as to whether all the attention and time and money that was being focused on such a big transformation would really ever pay off as compared with just let's focus on some specific problems and get them fixed right away. A legitimate question, but I believe that the answer is, yes, it is possible to bring together previously fragmented organizations to share practices and systems, and the power of doing that is enormous, far greater than can be ever achieved by just short-term focus on specific issues. That is why major businesses are always merging and divesting and reinventing themselves.

In the case of the IRS, when the reform was passed in 1998, the IRS was still organized largely in the pattern of the 1950's with about 47 or so district service centers and regions that all operated semi-independently. There were, at least officially, 15 different information technology departments and very few standards across them. There was no single e-mail, voicemail system, no security standards, and taxpayer data was frequently very fragmented.

Today, it is almost 5 years later, and we certainly cannot claim that all of those problems have been solved, but many of them have been addressed and partially corrected through such things as a top-to-bottom reorganization, development of an enterprise architecture along the lines of what Mr. Cooper was talking about, standardization of much technology platforms and products, and beginning to replace legacy systems. Service to taxpayers, as GAO has reported, substantially improved.

Now there is still a great deal of work to be done. My successor, Mr. Everson, who was just confirmed, will have plenty to do during his 5-year term, but I think there is no question any longer that the payoff for doing this kind of an integration program really is great and, therefore, it is possible. So I just say that because that is the most basic question of all: Is this whole thing even worth it and can it work? My statement is, yes, it can, as long as we recognize the challenges involved.

Now I will just offer a few observations about some of the things, without, again, claiming that they are specific to DHS because I don't know. It is very important to address the organizational issues at every level. At one level Congress has addressed them by setting up the Department of Homeland Security, but within the department, I am sure, without knowing the specifics, there are many organizational issues in the department, and not the least those related to IT.

Within the IRS reorganization, we made the decision to bring together, to reorganize the entire agency, to reduce the number of operating units very substantially, the four major operating units, and one IT unit that serviced the entire agency under one CIO. This may not be right for DHS, but I am simply suggesting that I think that it is very important to think through at every level how the organization is going to work, because that is what controls in the long run the money; that is what controls the incentives; that is what controls people, people and the way that they work.

Second, I heard Mr. Cooper talking about his enterprise architecture. I would like to lend my support to that idea as being extremely important, and I will particularly note the importance of what I believe he called his business architecture. We had the same idea at the IRS. It was basically the idea of looking at how business is done, how work is done today, versus how it is going to be done in the future.

We developed those kind of designs for all the major functions, such as how returns would be processed, how collection would be done, how customer service would be done, and laid those out, not in extreme detail, but with enough meaningful information, so that people could see that it really was going to be different. Now it takes years to get to that point, but I think, just as he said in his testimony, it is extremely useful right at the beginning because it helps to screen out projects that are not contributing to the general direction you want to go and, on the other hand, to identify the opportunities for those that are. That essentially is one of the major kinds of decisions that need to be made.

I will say that doing that kind of high-level business architecture in a meaningful way is a big commitment of top management time, of the leadership. It is not an easy thing to do, but I think it is a step that is important.

I heard, Mr. Chairman, you giving encouragement to the idea of stepping back and thinking these things through before, in effect, just rolling right away, but to try to address specific things, and I could only lend my experience that is, in fact, wise counsel.

Within the IT field itself, there is considerable value, we found, to establishing standards for certain technologies as quickly as possible, such as, for example, basic desktop and laptop operating systems, office automation tools, messaging software, some of the mid-range servers. These kinds of platform softwares and basic softwares, to the extent that they can be established quickly, can just by themselves tend to increase the ability to share information and actually to reduce costs, recognizing that there is a one-time cost and investment that is required to get there. I think to the extent

that those opportunities are found by Mr. Cooper and his colleagues, they would be good things to try to move ahead on quickly.

With respect to stakeholders, the IRS, of course, has many. Just about everybody is a stakeholder of the IRS: taxpayers, employees, tax preparation agencies, government committees. Obviously, homeland security, as was noted in the testimony, has many State and local governments and other places; so does the IRS.

One of the lessons that I think we learned through all the change that we were implementing was that it worked a lot better for us when we actually got these stakeholders in right at the beginning of our process, when we were beginning to think through these things and shared with them, even though it wasn't complete, our thinking and got their input and continued to interact with them and engage with them rather intensively through the process, as compared with what we sometimes did, and it didn't work as well, which was to sit there, develop our plan, and then explain it to them and hope that they would react to it and buy it.

I think there are two reasons for it. One is it is just human nature: People react better to things that they are involved in, that they think they are involved in constructing. But, also, you just find out more. You know, no one is smart enough to know all these things, even if you have the best experts, and it just helps to get that input. It does make for some more complex management problems when you are managing all these stakeholders while you are trying to manage your internal changes, but we found that it worked better.

And, finally, just a word for those such as perhaps members of this committee that are going to be evaluating progress in these major programs, and I do have to say that it is very important to have realistic expectations. Clearly, you want to have accountability and you want to see progress, but I must say that it is important that be done in a realistic way in order to support the efforts as opposed to perhaps not supporting them.

Specifically, I think that it, frankly, is not realistic to really expect any major change program such as the IRS went through, DHS is going through, to lay out detailed plans, you know, here's what we are going to do every quarter for the next 3 or 4 years and schedules along that line. There just isn't any way to get enough information to do that accurately.

What it is realistic to do is to expect that you have this architecture, this vision of where you are going, and then to lay out some next steps that are immediate next steps that say these are the next steps we are going to take, and to see whether those steps are successfully executed and then how the plan is adjusted after that. I mean, I would recommend that way of thinking in how to evaluate this as compared with a vision that there is a 5-year plan and you check off everything that is going to happen for 5 years, because I don't believe it is possible to do that and it really is more misleading than it is helpful.

That concludes my testimony, Mr. Chairman.

Chairman TOM DAVIS. Thank you very much. I am going to start the questioning with Mrs. Blackburn.

Mrs. BLACKBURN. Thank you. Thank you, Mr. Chairman.

Mr. Rossotti, let's see, did I understand you correctly that you reorganized 40 different independent divisions? Would you restate that again?

Mr. ROSSOTTI. Yes. The reorganization, part of the transformation at the IRS, this was incorporated in the reform bill. It gave us the authority to do this.

The IRS, back since the fifties, was organized into what were called districts and service centers. These were, essentially, independent, relatively semi-independent units that ran the IRS, and then there was a regional and other headquarters that supported them.

When I got there, there were 33 districts, 10 service centers, 4 regions, and then some other units. As part of this reorganization, those were eliminated; those were abolished. In their place, what we ended up with was—and I am oversimplifying this a little—four major units that were organized around taxpayers, one for individual taxpayers, one for small business, one for large business, and one for tax exempt. Each of those four has nationwide responsibility to do everything to service those taxpayers, and in the process we eliminated several layers of management and streamlined things.

Then each of those units, or many of them, had their own information technology, and so on and so forth. That is part of what led to all the fragmentation. So all that was pulled out, and there is now two support organizations in the IRS, one agencywide information technology organization which has the responsibility of providing all information technology services to the other operating units. They are, in effect, customers, and there are service-level agreements that lay out what those standards are. There is another support organization that does all the other support services, such as personnel, procurement, facilities, equal employment opportunity, those kinds of services.

Mrs. BLACKBURN. OK, and you brought this into one major IT unit, correct?

Mr. ROSSOTTI. Yes, we did. We did that in phases.

Mrs. BLACKBURN. Yes.

Mr. ROSSOTTI. It was not done all at once, but it was done in phases.

Mrs. BLACKBURN. All right, over a period of how many years?

Mr. ROSSOTTI. About 5 years. It has basically been 5 years.

Mrs. BLACKBURN. Over a 5-year period of time that you got it down to one major IT unit?

Mr. ROSSOTTI. Right.

Mrs. BLACKBURN. Did you have a CIO——

Mr. ROSSOTTI. Yes.

Mrs. BLACKBURN [continuing]. Overseeing this unit?

Mr. ROSSOTTI. Yes.

Mrs. BLACKBURN. You did? OK.

Mr. ROSSOTTI. Now I want to say I am not suggesting that that is what ought to be done—I really have to be careful here because each situation is unique. I think that made sense for the IRS. I really can't say whether that is the right answer. I just don't know.

Mrs. BLACKBURN. Well, I will tell you, my hat is off to you if you could do it. I would have been pulling my hair out.

Mr. ROSSOTTI. Well, I did; I had more hair when I started. [Laughter.]

Mrs. BLACKBURN. Well, maybe I shouldn't have used that example. [Laughter.]

But, you know, it seems like quite a task——

Mr. ROSSOTTI. It was.

Mrs. BLACKBURN [continuing]. When you are looking at going through that.

Now let me ask you this, and this would be a question for both you and Mr. Dacey: What do you see as the vulnerability, for implementing a single enterprise architecture for homeland security? How would you respond to that?

Mr. ROSSOTTI. Oh, I'm sorry. Are you addressing me?

Mrs. BLACKBURN. Yes, either of you or for both of you. I would like to get your thought on that, in having just one major IT unit, and then what redundancies should be built into that in case of an attack? You know, what kind of safeguards would you put into that type of system?

Mr. ROSSOTTI. Well, let me not try to answer it with homeland security, because, in honesty, it really requires a great deal of specific knowledge to come to those answers, and I really don't know about homeland security.

I think in the case of the IRS, the issues that you get into—the redundancy issue, let me come back to that one—I don't think is actually that much of a concern, because one of the things that we did as part of this was to plan in what redundancy we needed. We didn't need 13 computing centers. We didn't need that much, but we needed three. So we ended up having three really good ones.

I believe, with that question, the business recovery at the IRS today is better than it was before, because we sat down and planned it, rather than just saying, "Here's how many we had because that is how many we had." So that problem can be solved.

The difficulty you have in trying to go, if you are talking about reorganizing into one unit, is that while you are reorganizing it is very costly; it takes time. There are balls that get dropped. There is a lot of friction that develops during the process of doing that. We had that. We had setbacks.

I would say that the committee ought to be prepared that, if the Homeland Security Department really does everything it says it is going to do, don't be surprised if there are some things that go one step back before they go two steps forward. I mean, you just really have to be prepared for that.

So that is the problem. I think if you can get to the endpoint, you have some very powerful benefits, but there are big transitional issues.

Mr. HITE. If I could add to that, I think your question has two parts. One deals with the challenges and the vulnerabilities as part of a single enterprise architecture, and then the other one deals with a single IT organization. They are actually two different things.

The enterprise architecture talks about the department as a whole, as a single entity. It takes a holistic view to how to optimize the mission and responsibilities of the department as a whole.

As part of architecting your enterprise and going through that process, it is done in a very structured, deliberate, thoughtful way. Part of that thought goes into, how do we secure the enterprise? Part of that would be, how do we build in the necessary redundancy into the systems and our processes to ensure that we are secure and our information is secure?

Regarding the other issue about whether or not there should be a single IT organization, I would agree with Charles that it depends on the situation. Based on the dialog that we have had thus far with the department, I am not sure if it is clear yet as to what model it intends to employ. That will be a major decision point and one we will want to stay abreast of and the committee will want to stay abreast of, because it has major implications for how you go about implementing IT management across the department.

Chairman TOM DAVIS. Thank you.

That is the bells. The gentlelady's time has expired. We have four votes, but we don't vote for 15 minutes. Why don't we go on for 10 minutes and try to get the panel through, if I can.

Mr. Ruppersberger.

Mr. RUPPERSBERGER. The first thing, Mr. Rossotti, I agree with you on the shareholders/stakeholders, whatever, from the beginning process.

You know, it is a very difficult issue we are dealing with. First, you have to resolve the Federal agency issues and communication. Then you have the State and local that we have referred to before.

One of the things that we haven't talked about here today, and especially because at the State and local level sometimes you might not have the sophisticated people in the communications area that will be working with law enforcement, the issue of training. Have we implemented anything as it relates to training both from a Federal or a State and local level to try to deal with some of the problems that we are talking about?

Mr. ROSSOTTI. I think I would have to ask GAO to answer. I really don't know.

Mr. HITE. Your question speaks to specifically, what has the department done?

Mr. RUPPERSBERGER. Well, I am just asking about training. Do we have it? Do we have any plans for it? And it relates to the stakeholder issue, too, but as part of the elements of resolving this issue, it seems to me, we need to have training.

Mr. HITE. Absolutely. I agree 100 percent.

Mr. RUPPERSBERGER. So, therefore, do we have that implementation? Do we have a plan for that? Is it happening now? Maybe it is not. That is why I am asking the question, but it is an issue that should be addressed.

Mr. DACEY. I don't think we are familiar with what the department's plans are in that area except for IT. We have some information with respect to their IT personnel. They are trying to assess what their skill sets are, indeed.

But, in terms of the broader issues with personnel and training, we are not familiar with what the department is doing. We will check back with our other resources in our office and get back to you.

Mr. RUPPERSBERGER. Well, I mean, it is an issue I think that hasn't been addressed.

Mr. DACEY. Right, but it is certainly important.

Mr. HITE. If I could just add one thing to that, I mean, we recognize in GAO as part of our responsibilities for evaluating the department's effort, the only way it is going to get things done is through people, process, and technology. Human capital is a major contributor to this. We do have ongoing evaluative work within GAO dealing with the human capital issue at the department.

Mr. RUPPERSBERGER. And you're right, the technology is extremely important, but technology integration, too, again, getting back to the Federal, State, and local issue that we have to deal with here. Then, again, also, if you are going to be dealing, getting back to the training, dealing with the issue not only in technology, but in investigation and law enforcement, there is another major issue that we all need to focus on, homeland security, whatever it be, FBI, CIA, and that is the analysis of information and, again, training.

Because I am sure that we don't have the individuals now that can be used for the analysis. Analyst is becoming a very important position, and it is something we need, again, to focus on. I hope we consider that.

Also, Mr. Rossotti, I think you talked about flexibility. This is an ongoing process. I agree with you that this is the United States of America; the only way we are going to solve a lot of these issues is teamwork. We have to learn from our mistakes. It is our job to point out the mistakes; hopefully, to educate and to fix those mistakes for the future. It is something that is extremely important.

So thank you.

Chairman TOM DAVIS. Thank you.

Mr. Dacey, let me ask you, are there any vulnerabilities in implementing a single enterprise architecture?

Mr. DACEY. Some of the issues, which I think Randy had spoken about a little earlier, are that it is important to have an enterprise architecture across the entire entity.

Chairman TOM DAVIS. Should redundancies be built in in case of an attack?

Mr. DACEY. In terms of attacks, I think security is an issue which certainly needs to be built into the enterprise architecture, but at the same time the department I think faces heightened risks for their information security in general which need to be dealt with also in the short term as it goes forward.

You are connecting 22 previously unconnected entities, some of which may have connections back to their old parent organization. You are connecting State and local organizations, the private sector. You are developing a massive network, and if it is not properly constructed and secure, you are going to have risk from the standpoint of the weakest link in there could cause security challenges to the entire network. That is certainly a challenge.

Also, it is going to handle classified and sensitive data. The users are going to have to really be identified and authenticated because they are going to be given only levels or certain levels of information, depending upon where they are and who they are. So you are going to have to discriminate between what access they have.

Also, actually, it could become a very likely target, or probably is, actually, in terms of hackers, terrorist groups, or others who might be trying to probe into it as we speak. So I think there are some big challenges in putting together this whole system from a security standpoint which need to be dealt with.

Chairman TOM DAVIS. GAO is continuing to monitor DHS's progress, aren't they? I mean in implementing the enterprise architecture and strategic, is that your current plan? Or do we need to give you further direction?

Mr. HITE. We have ongoing work, actually, for you, Mr. Chairman, looking at enterprise architecture management across the entire Federal Government. The department is part of that work.

Chairman TOM DAVIS. The department is so critical because, No. 1, of the nature of its business at this point. Second, it is late; it is a late start. Part of it is our fault. It took a long time passing its parts and, as we talked before, making sure you understand your requirements before you go at it.

But, I mean, we all agree it is a lot slower than we had hoped, given the nature of the threat. So we want to give it special emphasis as it gets started, and not get in the way, but we need to oversee and make sure it is being done appropriately.

Mr. HITE. Absolutely. Just prior to this hearing, when I was talking to Steve Cooper, he brought up again the offer that I had made to him earlier, that we sit down and talk to him about how he is going about this and be able to offer real-time reaction to it.

Chairman TOM DAVIS. Mr. Rossotti, thanks again for being with us. You had to bring back a lot of different cultures and blend them together, and the key here is they have some probably more diverse cultures than you did——

Mr. ROSSOTTI. Absolutely.

Chairman TOM DAVIS [continuing]. In terms of the groups. I mean, they are bringing in some agencies whose IT systems, some of them are pretty good stovepipes; some of them were bad even as stovepipes.

What are the keys to success in general in fostering and institutionalizing a behavior and practice, and how do you use IT to utilize that?

Mr. ROSSOTTI. Well, I think that in some ways it is actually simpler than sometimes people think. I mean, it is a little more tangible maybe than just the general notion of culture.

And I put down this way: Basically, I think you have to address two things from people's point of view. One, is how are they going to keep getting their job done? People in the Federal Government actually want to do the job. When somebody says, "I know how to do the job this way," now there is something different, a new system, a new way, it sounds great, but, you know, "This is what I know how to do." If they can become more comfortable with how they are actually going to get their job done, which means bringing them into the process or their representatives into the process as part of the design, I think their acceptance level is greater.

The second thing they want to know is, "What is going to happen to me? Am I still going to have a job?"

Chairman TOM DAVIS. That is sometimes the first thing they want to know.

Mr. ROSSOTTI. Well, it could be, but I will put the two on equal footing for the purpose of this hearing. But really both are important because, even if people know they are going to have a job, they get very, very worried if they feel, they really do, that I am going to be still out there trying to do whatever it is I am supposed to do and I am not going to know how to do it. You know, people are very worried about that, as well as their own personal job security.

Now, I mean, to the extent that people are going to be displaced, then there has to be a process to deal with that, but I think probably in most cases you are not really going to just actually displace most of the people. What you are going to do is maybe change the way they work.

So, to the extent that they can be brought in and it could be clear what is going to stay the same and what is going to change, so that people know what to expect, you know, you could break down a lot of barriers. I mean, that basically is what it boils down to, to me. You have to, in a practical, tangible way, not only in theory, bring people along to understand what is going to happen to me. If it is going to change, fine. OK, then I should know that. Second, how do I get comfort that I am still going to be able to do my job.

What they really are thinking is, you know, somebody up there has a great idea that is going to make it a lot better, and it is going to have a new system. It will be integrated. But, basically, they are going to be up there, and when things go wrong down here, I am going to be the guy that has to talk to the taxpayer or the person that is coming across the border, or whatever it is, and I am going to be the one that is going to end up holding the bag. That is what is going through their mind, in my experience, and not without some legitimacy, by the way, because they are still going to be out there talking to people when things go wrong.

So, to the extent that you can bring people involved and get them involved, and you can, in a concrete, tangible way, answer those two questions, I think you can make a lot of progress.

Chairman TOM DAVIS. Thank you. Panel, thank you very much. Any other questions?

[No response.]

Chairman TOM DAVIS. Thank you very much. We appreciate your being here. As I said, your entire statement is in the record. I will dismiss this panel, and you are free to go.

We are going to take a recess. It will probably be about a half an hour because we have four votes over on the House floor, and we will reconvene back here. Mr. Shays may chair the meeting at that point, depending on some other obligations I am trying to work through.

But we thank everybody for staying with us. Thank you very much.

[Recess.]

Mr. SHAYS [presiding]. Sorry to keep our third panel waiting.

At this time let me announce our third panel: Mr. Greg Baroni, president, global public sector, Unisys Corp.

Mr. Steven Perkins, senior vice president, public sector and homeland security, Oracle Corp., and Mr. Mark Bisnow, senior vice president, webMethods, Inc.

Gentlemen, at this time it is our policy to swear you in. If you would stand, I will swear you in.

[Witnesses sworn.]

Mr. SHAYS. Thank you. Note for the record our witnesses have all responded in the affirmative.

Mr. Perkins, you may start. Excuse me, I meant Mr. Baroni. I think we will do it as we called you.

Gentlemen, let me apologize for keeping you waiting. We had a little bit of a question as to who was supposed to be here. Thank you.

Go ahead.

STATEMENTS OF GREG BARONI, PRESIDENT, GLOBAL PUBLIC SECTOR, UNISYS CORP.; STEVEN PERKINS, SENIOR VICE PRESIDENT, PUBLIC SECTOR AND HOMELAND SECURITY, ORACLE CORP.; AND MARK BISNOW, SENIOR VICE PRESIDENT, WEBMETHODS, INC.

Mr. BARONI. Mr. Chairman and members of the committee here, thank you for the opportunity to appear before you to discuss Unisys' interaction with the Department of Homeland Security with regard to its information-gathering and-sharing functions.

Although Unisys is under contract to several of the agencies that make up the new department, our major effort to date is the management and implementation of the Transportation Security Administration's Information Technology Managed Services [ITMS], Program, a large-scale IT infrastructure and applications implementation.

My testimony today will focus on TSA's mission and vision as it pertains to transportation security, with its initial mission being aviation security; ITMS, as an example of best practices in both procurement and technology services; how Unisys, as a world-class IT partner supports TSA's mission and vision; the partnership between Unisys and TSA; the Unisys relationship to the department's development and implementation of an enterprise architecture, and, finally, some cost benefits and efficiencies.

The Transportation Security Administration officially became part of the Department of Homeland Security in March 2003. TSA is tasked with ensuring the safe transport of people and commerce throughout the Nation's transportation systems, beginning with air travel.

TSA's Chief Information Officer, Pat Schambach, has stated that, in order to accomplish its transportation security mission in the most efficient and effective fashion, TSA, and by extension DHS, must rely heavily on information-sharing in a solid technological platform on which to operate.

Fulfillment of TSA's transportation security mission and vision is based in part on the ability of the department and TSA to share information; establish and maintain communications between the Federal work force at transportation centers such as airports and seaports, and TSA command-and-control centers such as headquarters, the Office of National Risk Assessment, and data centers.

The department and TSA's ability to effectively share information and provide communications is dependent on its ability to deploy a state-of-the-art information technology infrastructure for

voice, data, and communication that connects all relevant activities and locations.

The first phase of this transportation security plan focuses on aviation. When complete, it connects the Nation's 429 commercial airports, the Office of Federal Security Directors, and TSA command-and-control organizations.

A little background on Unisys: Unisys is a world-class IT provider headquartered in Blue Bell, PA with 37,000 employees, $6 billion in revenue, and a presence in more than 100 countries; 1,400 of our employees are located in northern Virginia, which is the headquarters of our Global Public Sector Unit.

In August 2002, Unisys and its team of experienced partners, including IBM and DynCorp, were selected to implement TSA's ITMS program and immediately began work. Team Unisys is focused on helping TSA accomplish its mission and is dedicated to taking the steps necessary to understand TSA's critical business issues.

Let's talk about ITMS. TSA, as the sole, newly created component of the Department of Homeland Security, is in a unique position to adapt best practices in both IT implementation, such as a Web-based operational strategy that supports OMB's e-government principles, and a procurement strategy, such as the Managed Services Program under which Unisys and its world-class team of IT partners provide the full range of IT infrastructure services as well as application development, implementation, and management.

The ITMS program incorporates best practices in IT contracting, technology, and operations. It is performance-based, as it has a mission-oriented framework, embraces performance metrics, and provides for performance-oriented incentives and disincentives. It not only incorporates the concept of best value, but also provides a utility model which outlines the responsibilities of both contractor and the customer.

Capabilities of ITMS: Under this program, Team Unisys provides a full range of IT infrastructure services as well as application development and implementation to TSA headquarters employees, the Nation's 429 commercial airports, and the Federal Security Directorate sites, in addition to 21 Air Marshall field offices.

This includes providing equipment such as desktops, laptops, servers, voice-over-Internet phones, cell phones, pagers, land mobile radios, and hand-held devices. It also includes local area networks and wide area networking at TSA headquarters and airport locations, as well as the use of a hosting center to run specific and enterprise-wide applications.

Examples of applications Unisys and its team are hosting for TSA include the public-facing Web site, the internal employee Internet, e-mail, and a host of specialized applications to support mission functions.

The TSA strategy for IT deployment initially called for three phases referred to as "red," "white," and "blue," and I will just note here that my testimony, my written testimony, goes into much more detail with regard to these efforts. So, for the purposes of my testimony here orally, I am going to kind of summarize.

The initial or red phase focused on the deployment of initial infrastructure to headquarters and the hosting center, as well as deploying essential computing and communications equipment to

field airport locations. The red phase, as we describe it, is essentially complete.

The second or white phase consists of providing robust and secure LAN/WAN connectivity between field airport locations and the TSA hosting center. That effort is underway today, and we are in the early stages of it.

The blue phase represents a time at which TSA will be able to leverage deployed IT, or information technology, with both business model and process re-engineering to achieve new efficiencies and effectiveness for transportation security.

In addition to the services being provided directly to TSA, DHS has leveraged ITMS, the vehicle, by tasking Team Unisys to stand up the IT infrastructure at its headquarters locations, including desktop equipment and local area network support. Team Unisys also is hosting DHS's public-facing Web site in the same hosting center and using the same infrastructure, or leveraging that same infrastructure, that we established and are using for TSA.

Let me talk quickly about the relationship to DHS and the enterprise architecture. The Clinger/Cohen Act requires the use of a rigorous enterprise architecture blueprint to enable systems modernization. Recently, OMB provided guidance on EA through release of reference models that enable information-sharing and reduce IT stovepipes.

Additionally, GAO has indicated that the development and effective use of an enterprise architecture is crucial to successfully achieving an organization's mission and objectives. Absent such a blueprint, an organization may find a lack of integration among business operations and supporting information technology resources that could lead to burdensome inefficiencies and redundancies.

One of our major tasks is to develop TSA's enterprise architecture consistent with the department's overarching EA strategy. To do so, we have combined the best of OMB's reference models, GAO's maturity models, and the Federal CIO Council's Federal Enterprise Architecture Framework [FEAF], along with our own best practices that focus on business strategy and business drivers.

Additionally, we have implemented an enterprise architecture management system——

Mr. SHAYS. Mr. Baroni, let me just ask you, just give me a sense of how much longer you feel you need to be going.

Mr. BARONI. About a minute and a half.

Mr. SHAYS. OK. Let me just tell you the challenge. The challenge is we may not have another member to take my place, and about 4 minutes to 1 p.m., I have to leave. I want to make sure we do get into some key points.

Mr. BARONI. OK.

Mr. SHAYS. And I apologize to all three of you for that. There is just a little mixup as to how we were going to handle this. You are an important panel, but if we can try to deal with it—OK?

Mr. BARONI. OK, I will quickly go through here then.

Mr. SHAYS. Thank you.

Mr. BARONI. The department has established an Enterprise Architecture Working Committee comprised of representatives from its component agencies. Team Unisys works directly with TSA, the

TSA representative, and is sharing our best practices with that committee.

The department has also adopted that use that I referenced earlier as the repository for its enterprise architecture artifacts and has asked us to develop their IT investment portfolio system.

I will just move on to cost savings and efficiencies now. The concepts of IT integration and cost savings have been at the core of everything we are doing, and that has been assigned by TSA to Team Unisys. These concepts were initially driven by the Investment Review Board, established last fall by the then-Office of Homeland Security and the Office of Management and Budget.

For instance, TSA and Team Unisys have established a very deliberate process to review the capabilities and infrastructure in place at each airport that has a presence of both the Immigration and Naturalization Service [INS], and the U.S. Customs Service before we deploy any new infrastructure on behalf of TSA. The purpose of this process is to identify any potential opportunities to share space, equipment, and infrastructure that could drive down the cost for each agency.

In summary here, consistent with the President's Management Agenda, TSA's ITMS program is an end-to-end IT infrastructure contract for the application of IT life-cycle management. A major focus of ITMS implementation has been to design a blueprint of its technology requirements and establish a disciplined process for making IT investments.

TSA is focusing on real cost savings for the American taxpayer by ensuring the IT infrastructure investment decisions are coordinated among the co-located agencies in the field.

That concludes my testimony, and I will be happy to answer any questions you and/or any of the committee members may have.

[The prepared statement of Mr. Baroni follows:]

Testimony
of
Greg Baroni

President
Global Public Sector
Unisys Corporation

before the

House Government Reform Committee
on
Information Integration & Sharing Functions
of the
Department Homeland Security

May 8, 2003

Mr. Chairman and Members of the Committee, thank you for the opportunity to appear before you to discuss Unisys interaction with the Department of Homeland Security with regard to its information gathering and sharing functions. Although Unisys is under contract to several of the agencies that make up the new Department, our major effort to date is the management and implementation of the Transportation Security Administration's (TSA) Information Technology Managed Services (ITMS) program, a large-scale, IT infrastructure and applications implementation.

My testimony today will focus on the TSA's mission and vision as it pertains to air safety; ITMS as an example of best practices in procurement and technology; how Unisys, as a world-class IT partner, supports the TSA's mission and vision; the partnership between Unisys and TSA; Unisys relationship to DHS's development and implementation of an enterprise architecture; and finally, cost benefits and efficiencies.

AVIATION SECURITY MISSION AND VISION

The Transportation Security Administration, created by the Aviation and Transportation Security Act (PL-107-71), which passed Congress and was signed into law in November 2001, officially became part of DHS in March 2003. TSA is tasked with ensuring the safe transport of people and commerce throughout the nation's transportation systems, beginning with air travel.

TSA's Chief Information Officer Pat Schambach has stated that in order to accomplish its transportation security mission in the most efficient and effective fashion, TSA and, by extension, DHS must rely heavily on information sharing and a solid technological platform on which to operate.

Fulfillment of TSA's transportation security mission and vision is based in part on the ability of DHS/TSA to share information, establish and maintain communications between the federal workforce at transportation centers (e.g., airports and seaports) and TSA command and control centers (e.g., headquarters, the Office of National Risk Assessment, data centers, etc.). DHS/TSA's ability to effectively share information and provide

communications is dependent on its ability to deploy a state-of-the-art information technology (IT) infrastructure for voice, data and communications that connects all relevant activities and locations.

The first phase of this transportation security plan focuses on aviation; when complete, it will connect the nation's 429 commercial airports, the offices of Federal Security Directors (FSD) and TSA command and control organizations.

UNISYS

Unisys is a world-class IT provider headquartered in Blue Bell, Pa., with 37,000 employees, $6 billion in revenue and a presence in more than 100 countries. Fourteen hundred employees are located in Northern Virginia where our Global Public Sector is headquartered.

In August 2002, Unisys and its experienced team of partners, including IBM and DynCorp, were selected to implement TSA's ITMS program and immediately began work. Team Unisys is focused on helping TSA accomplish its mission and is dedicated to taking the steps necessary to understand TSA's critical business issues.

Unisys understands that government IT executives are faced with complex challenges as they consider how best to capitalize on information technology to realize that vision — challenges in human capital development, sourcing, management and measurement of the business impact that IT has on their mission. Successful transformation and management of the IT infrastructure to meet strategic business objectives is key in government – as it is in the private sector – not just to improving worker productivity, client satisfaction, operational efficiency and cost containment, but also to quantifying that improvement and its contribution to mission success. Unisys is cognizant of the need to develop practices that enhance end-to-end business process that support TSA in achieving its border aviation security objectives.

ITMS

TSA, as the sole newly structured component of DHS, is in a unique position to adapt "best-practices" in both IT implementation (such as a Web-based operational strategy, which supports OMB's e-Government principles) and procurement strategy, such as the managed services program under which Unisys and its world-class team of partners provide the full range of IT infrastructure services as well as application development, implementation and management. The ITMS program incorporates best practices in IT contracting, technology and operations. It is performance-based, as it has a mission-oriented framework, embraces performance metrics and provides for performance-oriented incentives and disincentives. It not only incorporates the concept of "best value" but also provides a utility model, which outlines the responsibilities of both the contractor and the customer.

For instance:

CONTRACTOR

- Provides level of service
- Builds infrastructure and retains ownership
- Incurs capital cost

CUSTOMER

- Orders services with service level agreements
- Leverages infrastructure and has flexibility in scaling up and down
- Predictable funding requirements

Operating guidelines that TSA's ITMS program have been following include investing in open architecture best-of-breed solutions as well as relying on commercially available off-the-shelf solutions driven by the business processes articulated in an enterprise architecture, in lieu of custom-built solutions. The ITMS contract vehicle also provides for ease of ordering, tech refresh and administration, and is an example of TSA's commitment to become a model of public-private partnership.

CAPABILITIES

Under this program, Team Unisys provides a full range of IT infrastructure services as well as application development and implementation to TSA's headquarters, employees, the nation's 429 commercial airports and Federal Security Director (FSD) sites in addition to 21 Federal Air Marshal (FAM) field offices. This includes providing equipment such as desktops, laptops, servers, voice-over-internet phones, cell phones, pagers, land mobile radios, and handheld devices. It also includes local area networks (LAN) and wide area networking (WAN) at TSA headquarters and airport locations, as well as the use of a hosting center to run specific and enterprise-wide applications. Examples of applications Unisys and its team are hosting for TSA include the public-facing web site, the internal employee intranet, e-mail, and a host of specialized applications to support mission functions.

The TSA strategy for IT deployment initially called for three phases referred to as Red, White and Blue. The initial, or Red phase, focused on the deployment of initial infrastructure to headquarters and the hosting center, as well as deploying essential computing and communications equipment to field airport locations. In addition, connectivity between field airports and the hosting center for services such as e-mail is provided via virtual private network (VPN) dial-up. The Red phase is essentially complete.

The second, or White phase, consists of providing robust and secure LAN and WAN connectivity between field airport locations and the TSA hosting center. It also provides additional applications to support workforce time and attendance monitoring, workforce scheduling and alert notification. Further, it provides the communications and computing infrastructure required to support secure data and information sharing between field locations and headquarters. We are in the early stages of the White phase and have initiated deployment to airport field locations.

The Blue phase represents a time at which TSA will be able to leverage deployed information technology with process re-engineering to achieve new efficiencies and

effectiveness for transportation security. In addition to the services being provided directly to TSA, DHS has leveraged the ITMS capability by tasking Team Unisys to stand up the IT infrastructure at its headquarters locations including desktop equipment and local area network support. Team Unisys also is hosting DHS's public-facing Web site in the same hosting center and using the same infrastructure that we established and are using for TSA.

RELATIONSHIP TO DHS/ENTERPRISE ARCHITECTURE

The Clinger-Cohen Act requires the use of a rigorous Enterprise Architecture blueprint to enable systems modernization. Recently, OMB provided guidance on EA through the release of reference models that enable information sharing and reduce IT stovepipes. Additionally, as GAO has indicated that the development and effective use of an enterprise architecture is crucial to successfully achieving an organization's mission or objectives. Absent such a blueprint, an organization may find a lack of integration among business operations and supporting information technology resources that could lead to burdensome inefficiencies and redundancies. One of our major tasks is to develop TSA's Enterprise Architecture consistent with DHS's overarching EA strategy. To do so we have combined the best of OMB's reference models, GAO's maturity models, and the Federal CIO Council's Federal Enterprise Architecture Framework along with our own best practices that focus on business strategy and business drivers. Additionally, we have implemented an Enterprise Architecture Management System (EAMS) as a repository for all TSA architecture artifacts.

DHS has established an Enterprise Architecture Working Committee comprised of representatives from its component agencies. Team Unisys works directly with the TSA representative and is sharing our best practices with that Committee. DHS has also adopted TSA's EAMS as the repository for its Enterprise Architecture and has asked us to develop their IT Investment Portfolio System (ITIPS). We will provide training, help desk and expert services as well as managing the hosting environment.

Unisys is also providing thought leadership in leveraging commercial best practices for Enterprise Architecture for federal agencies by acting as the chair for the Industry Advisory Council Enterprise Architecture Shared Interest Group. This Shared Interest Group is working closely to address information and data sharing architecture issues with DHS.

COST SAVINGS AND EFFICIENCIES

The concepts of IT integration and cost savings have been at the core of every task TSA has assigned to Team Unisys. These concepts were initially driven by the Investment Review Board established last fall by the then-Office of Homeland Security and the Office of Management and Budget. For instance, TSA and Team Unisys have established a very deliberate process to review the capabilities and infrastructure in place at each airport that has a presence of both the Immigration and Naturalization Service and the U.S. Customs Service before deploying any new infrastructure on behalf of TSA. The purpose of this process is to identify any potential opportunities to share space, equipment or infrastructure that could drive down cost for each agency.

When DHS stood up its new headquarters locations, they utilized Team Unisys under the ITMS contract to provide equipment, LAN, and WAN connectivity. To save time and money, they agreed to use essentially the same designs and capabilities already deployed to TSA. Likewise, DHS also leveraged the design and existing equipment in the TSA hosting center to establish their public-facing website which we host. This also provided a great time and cost savings for the Department.

SUMMARY

Consistent with the President's Management Agenda, TSA's ITMS program is an end-to-end IT infrastructure contract for the application of the IT life cycle management methodology. A major focus of the ITMS implementation is to design a blueprint of its technology requirements and establish a disciplined process for making IT investment decisions. As TSA is not wed to cumbersome legacy systems that complicate technology integration efforts, the ITMS program could serve as a model for a department-wide IT management process serving other operating components of DHS. TSA is focusing on real

cost savings for the American taxpayer by ensuring that IT infrastructure investment decisions are coordinated among co-located agencies in the field.

Mr. Chairman,

That concludes my testimony, and I will be happy to answer any questions you or any member of the committee might have.

Mr. SHAYS. Thank you.

The next two witnesses can use the same amount of time. With my interruption, it was 11 minutes. But it is important to put those things on the record. So you can decide whether you want to have statements or some questions and dialog. I will be here. So you can have 10 and 10, whatever.

Mr. Perkins, you are next.

Mr. PERKINS. Thank you, Mr. Vice Chairman. I will try to edit this on the fly.

Mr. SHAYS. But get it on the record.

Mr. PERKINS. Thank you very much.

Mr. SHAYS. Just as long as you realize what we have here.

Mr. PERKINS. And I would hope that the written testimony could be incorporated in the record as well.

Mr. SHAYS. It will be in the record.

Mr. PERKINS. Thank you very much.

Again, my name is Steve Perkins. I am senior vice president responsible for Oracle's public sector in the United States and our homeland security as well for Oracle Corp.

Just on a personal note, as a long-time Connecticut resident, it is delightful to appear before you.

Mr. SHAYS. Thank you. You may have 12 minutes. [Laughter.]

Mr. PERKINS. Thank you very much.

As you may know, Oracle was created 26 years ago to help the intelligence community manage its most sensitive information. Today, Oracle is the largest enterprise software company in the world, providing information management software and expertise to firms that include 98 of the Fortune 100 and hundreds of departments and agencies in Federal, State, and local governments.

Mr. SHAYS. The only thing I know is, had I invested stock with you that many years ago, I wouldn't be sitting here. [Laughter.]

Mr. PERKINS. Not part of my prepared remarks, but yes.

In addition to the corporate customers we work with, we are also very active with the Department of Homeland Security. In fact, all 22 of the agencies of the department use Oracle's technology.

So, given our market position, we are part of the Nation's critical information infrastructure, and since September 11 have spent a good bit of time working with them to better secure those systems.

Mr. Vice Chairman, I don't believe anyone could overstate the magnitude of the information-sharing challenge facing Secretary Ridge, Steve Cooper, and the entire Homeland Security team. Since the formal creation of the department last March, the department has been working very hard to stand itself up in the areas of personnel, administration, and technology, and to pull the 22 disparate organizations, and its 190,000 people, together. While this certainly isn't the largest of the commercial mergers, in a dollar sense it certainly is the most complex one I have ever seen in my experience.

Information we believe is one, if not the most, powerful weapon we have against terrorism. Strangely, when you watch the news shows, there seems to be a focus on a lack of information; we don't have enough information. I believe the problem is exactly the opposite; we have an abundance of information, and our challenge is to integrate that information, to make sense out of it, and make it ac-

tionable. Real data is found in these relationships, not in the data itself, and that certainly is one of the lessons that we learned, unfortunately, on September 11.

We are very pleased that Steve Cooper, the CIO for DHS, is looking to establish this enterprise architecture in accordance with OMB policy, and we are advocates of this approach. We believe the architecture can serve as a blueprint for information-sharing vertically with State and local and Federal organizations as well as horizontally within the 22 agencies and with the other groups at the Federal level as well.

That is one of the key challenges we are working on with the Transportation Security Administration and our partner, Unisys Corp. TSA is going to be in a position to receive a tremendous amount of information. Its challenge will be to assess that information and make it actionable.

They are using our technology in the areas of incident management and case tracking to better manage this. They are also using our technology to support a public portal, so the citizens can report concerns about public transportation. We think the architecture that they are using there can be an example for the application of enterprise architecture at the DHS level.

The most significant barrier to information-sharing, in our view, and an opportunity to apply standards, lies in the concerns raised by organizations, both public and private, about the potential of their data to be exposed to insecure systems. There are well-established standards for securing and auditing these data.

In the United States they are managed by NIAP, or National Information Assurance Partnership. Oracle is one of a few companies that actually builds security capability into the products as opposed to bolting it on after the fact. In fact, we go the extra step of having our software independently evaluated against standards like the Common Criteria.

I believe that Federal agencies, who represent the largest buying entities for commercial products, can play a significant role in the marketplace by making information assurance through independent evaluation ubiquitous.

In January 2000, a committee within the National Security Agency proposed standards which have been embodied in NSTISSP No. 11, a policy that calls for independent evaluations of information assurance products purchased by the Federal Government. This policy has been recently adopted by the Department of Defense in their evaluation and embodied in last year's defense authorization bill by Congress.

I bring it to the committee's attention because we believe DHS should adopt this policy for their procurements. We think, as a byproduct of the money that will be spent on homeland security, and without additional cost, we can lock down the entire information infrastructure.

In short, if DHS insists that that capability exists in commercial products, others like Oracle will build it in, and everyone who buys it anywhere in that vertical infrastructure will have it available. Whether it is information security enterprise architecture or industry standards, we think it is very important for DHS to continue

the outreach programs that they started. I enjoyed Mrs. Blackburn's question on that subject.

When Steve Cooper was part of the Office of Homeland Security at the White House, I thought he had a very effective outreach program. We encourage them to continue it. Obviously, the complexities of setting the department up are very time-consuming, but we think it is critical.

So, in conclusion, Mr. Vice Chairman, I believe the department is making sound, measurable progress on information engineering and integration. Congress, as policy leaders, can best assist DHS by defining appropriate policies to guide Federal, State, and local organizations down a common path for information-sharing.

Thank you again for the opportunity to testify, and we look forward to questions.

[The prepared statement of Mr. Perkins follows:]

ORACLE®

Statement of

Steven Perkins
Senior Vice President
Public Sector and Homeland Security
Oracle Corporation

Before the
Committee on Government Reform
United States House of Representatives

8 May 2003

Mr. Chairman, Ranking Member Waxman, and members of the Committee, thank you for the opportunity to appear before you today. My name is Steve Perkins and I am Senior Vice President of Public Sector and Homeland Security for Oracle Corporation.

It is only fitting that Oracle is represented today since the Ranking Member is from California – Oracle's home state -- and the Chairman is from Virginia -- the state where Oracle was founded and where our Government, Education, and Healthcare business are headquartered. In fact, many of my fellow Oracle team members who work in our Reston facility are proud to call the Chairman their Congressman. We are all very familiar with the Chairman's legislative accomplishments, such as the E-Gov Act, and the Critical Infrastructure Information Act; and we look forward to working with you in your new position of leadership in the Government Reform Committee.

Oracle was created twenty-six years ago to help the intelligence community manage its most sensitive information. Today, Oracle is the world's largest enterprise software company, providing information management software and expertise to firms that include 98 out of the Fortune 100, and to hundreds of departments and agencies in federal, state and local governments. Given our market penetration, we are an integral part of the nation's critical information infrastructure and, since September 11th, have worked with our customers, private and public, to better secure these vital networks. In fact Larry Ellison, our Chairman, led the first project, and remains actively engaged in innovations designed to improve the integrity and effectiveness of these systems. We at Oracle are proud to call the federal government a valued and strategic partner in these efforts

Mr. Chairman, I don't believe one can truly overstate the magnitude of the challenge facing Secretary Ridge, Steve Cooper and the entire Homeland Security team. Since the formal creation of the Department last March, the Department has been working very hard to stand itself up on a number of levels – personnel, administrative and technological – in order to have 22 federal entities and 190,000 federal employees work in a cohesive fashion. While not the largest of mergers on a commercial scale it is certainly one of the most complex I've seen in my career, and clearly one with the highest stakes for our nation.

Of course, Oracle monitors closely the investments made by Congress toward information technology, and how the Department, as well as other federal, state and local entities uses those investments to advance homeland security. Information is, after all, one of, if not the most powerful weapon that we have in the fight against terrorism. Just ask the brave men and women of our armed forces and intelligence agencies who served to liberate Iraq -- the more we know about the enemy, the more likely we are to be able to anticipate, prevent or effectively respond to his actions. A central concept of network centric warfare is making information available in near real time and pushing to the edges of the organization – a model to be emulated at DHS.

Strangely, when you watch the news shows, you get the sense that we don't have enough information. As someone who helps our customers manage information, I can say first

hand that information is all over the place. The real problem is the capability needed to establish relationships between various information sources. Real knowledge is found in these relationships, not in the data itself. That was one of the tough lessons of September 11th. There were lots of "facts" out there about individual terrorists – the federal government was unable to bring these facts together so that intelligence agencies and law enforcement could see the whole picture.

We are very pleased that DHS CIO Steve Cooper is looking to establish an enterprise architecture for his Department, consistent with OMB policy. We are advocates of this approach. By establishing clear business processes and business flows as part of this enterprise architecture model, the DHS is in a better position to drive technology toward these objectives. The architecture can serve as the blueprint for information sharing vertically with state and local institutions, as well as horizontally among federal components both within and outside the Department.

That's one of the key challenges we are working on with the Transportation Security Administration. TSA is positioned to receive vast amounts of information, but its success will be based on how well this information is processed and presented in order for TSA to take action. For example, we are working with TSA to provide incident management and case tracking capabilities in order for TSA to better manage its information flows. Further, we are working with TSA on a public portal so that citizens can report suspicious activities with public transportation systems. Just as important, these systems offer business continuity and scalability.

We hope that the efforts now underway at TSA will serve as a blueprint for the kind of information management architecture needed in other homeland security agencies. One of the fundamental, positive lessons that can be drawn from the TSA example is the utility of an enterprise architecture approach – an approach that builds its systems infrastructure in stages, and enables the agency to do more with less through common databases, tools and resources.

Accomplishing this requires a commitment to standards, but not standards exclusive to the DHS, or standards set by Congress. For example, integration standards define how a system exposes its data to other systems. Industry-generated 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.

Since federal, state, and local systems are all built independently, integration standards are necessary if they are going to be built or updated to effectively share information. We understand that Mr. Cooper is not going to insist on DHS exclusive standards, but work to integrate or reinforce existing standards, or leverage the DHS to push for industry

developed and supported standards. This approach in the long run is cost effective for both the public and private sectors.

Perhaps the most important form of information standard is geared toward security. The most significant barrier to information sharing will most likely be driven by concerns raised by organizations – private and public -- about exposing their data to potentially insecure systems. There are well-established standards for securing data and auditing its use. These standards 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 – an effective collaboration between the National Security Agency and the National Institute of Standards and Technology. Together, they manage the standards and independent evaluations processes required to ensure that technology providers like Oracle are implementing secure products.

Oracle is one of a number of software companies that build security into its software development process, rather than bolting it on through a constant barrage of patches. A build-in, as opposed to a bolt-on approach to security produces better products. We even go the extra step and invest in having our software tested against internationally recognized information assurance standards, such as the Common Criteria.

Federal agencies — collectively the single largest buyer of commercial off-the-shelf software products — can change the marketplace for the better by making information assurance, through independent evaluations, a factor in their buying decisions. In January of 2000, a committee within the National Security Agency proposed that federal agencies with information systems involved in national security can only purchase commercial information assurance software that has been independently evaluated to be secure. This policy went into affect last July, and the Defense Department has developed regulations consistent with this policy, which Congress endorsed last year in its Defense authorization bill. Also, the President's cybersecurity strategy called for a study on the potential effectiveness of applying similar policies throughout the federal government.

I bring this issue to the Committee's attention because we at Oracle believe DHS should adopt this acquisition strategy. After all, if the tragic terrorist attacks of September 11 proved anything, it is that our most sensitive information systems in federal information sharing and coordination of strategies will likely take place among those law enforcement agencies within and outside of the Homeland Security Department. Information sharing and analysis also is likely to occur between our law enforcement and intelligence agencies. All of this activity requires that the Department have strong information assurance strategies, including those involving the purchase of information assurance systems in the commercial market.

Whether it's information security, enterprise architecture, or industry standards, the approaches taken by DHS necessitate the need for continued outreach with the private sector. When the White House first created the Office of Homeland Security, it instituted a very open, accessible, and in our estimation, effective outreach program to private

sector innovators in the high tech community. Clearly, the challenges and demands of the newly created Department are far more complex and all consuming, particularly in the face of that complexity. It is essential that the Department, particularly Mr. Cooper, work hard to maintain that accessibility and visibility, and not just with vendors, but also with key customers in state and local governments, so they can better understand how they fit in the overall infrastructure. We believe the private sector can and must contribute quickly to solve the information and integration challenges.

As DHS moves forward with its proposed enterprise architecture, the need for continued openness is especially critical, particularly on the program side.

Finally, on a related topic, I wanted to touch on an issue that I know is important to the Chairman – a section in the Homeland Security Act called the Support Anti-terrorism by Fostering Effective Technologies Act – otherwise known as the SAFETY Act. This new law is designed to provide liability protections to private contractors that are producing qualified anti-terrorism technologies for federal, state or local governments. These protections are essential if we are to encourage innovative solutions to the numerous challenges that face both government and the private sector in securing our nation's homeland. The Chairman was instrumental in bringing this legislation to the attention of the Congress and in getting it included in the Homeland Security Act.

In order to receive this liability protection, a contractor's product has to meet several important criteria. The SAFETY Act will require regulations to further clarify product eligibility, but as of yet, draft regulations have not been issued. I am sure a number of our partners in the technology community would agree with me that the sooner we can get these regulations available to the public for comment and then finalized, the sooner we can encourage forward-thinking ideas to protect our critical infrastructures and most important, to best implement a homeland security strategy.

In conclusion, Mr. Chairman, I believe the Department is making sound, measurable progress on information integration. No doubt, individual entities that are part of our overall homeland security infrastructure are focusing on getting their own systems and capabilities up and running, and will press Congress to fund individual systems. What we risk in that kind of a situation is a thousand well-funded little systems, but no improved national capacity to deal with the threat of terrorism. This would amount to a failure of planning and protection. The DHS is working with the private sector, and state and local governments to make sure that doesn't happen. Congress, as policy leaders, can best assist the DHS by defining 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 for the opportunity to testify today. I look forward to answering any questions you may have.

Mr. SHAYS. Thank you, Mr. Perkins, and I appreciate your help here.

Mr. Bisnow.

Mr. BISNOW. Thank you, Mr. Chairman, and thanks for the opportunity to appear this morning on behalf of webMethods, which is a leading maker of integration software. I am really here to tell you about the experience of a small company dealing with the Department of Homeland Security.

My name is Mark Bisnow, and, yes, I am the one who does the corny radio commercials for webMethods, where I run our Government Operations Unit. We like to think there is a method to my madness, as I make fun of acronyms and techno-babble on the public airwaves. We have actually reached a point in American history where, for the first time, the word "integration," though that is still too arcane a term to use in polite company, can at least be understood conceptually, if you remove strange words like "back-end," "enterprise," "legacy," "scalability."

When I remind people that the September 11 terrorists went up to the counters at United and American, used their real names, but weren't recognized even though they were on government watch lists, a light bulb goes off and they realize the importance of integrating data bases. Or when I ask people if they ever called their bank and the voice menu says to punch in your account number, and you do so, and then you are transferred and a human being answers and they ask you for your account number again, and you say, "Didn't I just give you that?" And the person at the other end says, "Oh, that's another system in our company, and they're not connected." Well, let me put it this way: Even my mom now understands what we do at webMethods.

If we can harness the interest and understanding of ordinary Americans like my mom, we can create a powerful information-sharing revolution in America. Someday our grandchildren will think it is all very funny that computer systems didn't talk to each other. In fact, they probably just won't believe it.

But at the moment they don't talk to each other, and it is actually not very funny. Nowhere is the imperative for integration clearer than in homeland security, not just the mission of stopping terrorists, but how about just getting the daily functions of the department to work together and hum?

I have been around town a long time, and when you talk about merging 170,000 people and 22 agencies, you are talking about a lot of B-H-A-Sy. That is the acronym for "big, hairy accounting systems," not to mention "big, hairy financial systems," "human resources systems," and the like.

Of course, it just so happens that is what webMethods does. We are a company of nearly 1,000 people, based in Fairfax, with 50 offices in 18 countries throughout the world. We make commercial, off-the-shelf software that, in our view, is cheaper, faster, more reliable, and more secure than the old-fashioned way of hiring lots of human beings to come in and write software code to connect different systems.

Instead, we provide a single software platform that all the different systems and data bases plug into. We do this for FedEx, Dell, 3M, Office Depot, Apple, Verizon, Best Buy, Freddie Mac, the

Army, EPA, and about 1,000 other household-name companies and government organizations.

So how does a relatively small company like ours, no matter how great its product, get into a big agency like the Department of Homeland Security? Well, I wish it were like going to Carnegie Hall and all it takes is practice, but, no, that is not enough. If it were a matter of having vast, world-class practice and experience, DHS would be ringing our phone off the hook. The fact is it is not easy, and here are some reasons why.

First, those heroic people at DHS have a million other things to do. Thank heavens, they don't stop every moment to listen to every vendor, but we would like to think that integration is about as high a priority as you can get and that they will be looking for the best technology. So I keep hoping that, when I check my voicemail each day, there will be an urgent message waiting from Steve Cooper.

Second, relatively small companies like ours depend on relationships with giant prime contractors who agencies, first and foremost, deal with, not with small companies like ours. We depend on those big companies.

So have I forgotten to mention how wonderful a company Unisys is? [Laughter.]

I think Oracle is a good company, but Unisys is a great company. [Laughter.]

Third, the government is a bit of an IBM shop on the civilian side. Even though top analysts may say that our software is superior in our particular niche, never underestimate the bureaucratic appeal of the deniability you get if there is ever a problem and you can say, "Hey, man, I bought IBM," but we're stubborn and know that someday they will also say that about webMethods.

Fourth, there is still something called architecture being established, and, of course, you wouldn't start building a house and buying components without a blueprint.

Finally, there isn't a lot of money sloshing around yet. That is where this fine committee and Congress come in, but that is above my pay grade to comment.

But, on the bright side, there are now some pilot programs, and we do hope to participate in those. We are lucky that, in general, when our software is evaluated, people love it and we get contracts. So if I had one thing to suggest to DHS, it would be that there should be more proactive evaluation of specific technology like ours. I suspect that DHS actually agrees, and when the dust settles from the merger, maybe there will be.

Mr. Chairman, integration is not just a subject for techies. It has huge implications for our economy, foreign policy, and homeland security. This committee will leave an extraordinary legacy if it gets ordinary Americans to understand the power for good that information-sharing, AKA "integration," can have in our daily lives, making government run more efficiently and helping to prevent terrorism.

The Department of Homeland Security is the best imaginable laboratory and showcase for this revolution. As an integration company, we at webMethods are excitedly hoping that the example it sets will be a great one.

We are deeply indebted to this committee for trying to make that happen, and we stand ready to help. Thank you again for the invitation.

[The prepared statement of Mr. Bisnow follows:]

Remarks of Mark Bisnow
Senior Vice President
webMethods, Inc.

House Committee on Government Reform
May 8, 2003

Mr. Chairman and Members of the Committee,

Thank you for the opportunity to appear this morning on behalf of webMethods, a leading maker of integration software. My name is Mark Bisnow, and yes, I am the one who does the corny radio commercials for webMethods, where I run our government operations unit.

We like to think there's a method to my madness as I make fun of acronyms and technobabble on the public airwaves. We've reached a moment in American history where for the first time the word "integration"—though that's still too arcane a term to use in normal conversation—can at least be understood conceptually…if you remove strange words like "back end," "enterprise class," and "scalability."

When I remind people that the 9/11 terrorists went up to the counters at United and American, used their real names, but weren't recognized even though they were on government watch lists, a light bulb goes off and they realize the importance of integrating databases. Or when I ask people if they've ever called their bank, and the voice menu says to punch in your account number, and you do so, and then you're transferred, and a human being answers, and they ask you for your account number again, and you say, "Didn't I just give you that?" And the person at the other end says, "Oh, that's another system in our company, and they're not connected." Well, let me put it this way: even my mom now understands what we do at webMethods.

Someday our grandchildren will think it's all very funny that computer systems didn't talk to each other; in fact, they probably just won't believe it. But at the moment, they don't talk to each other, and it's actually not very funny.

Nowhere is the imperative for integration clearer than in homeland security. Not just the mission of stopping terrorists, but how about just getting the daily functions of the department to work together and hum? I've been around town a long time and when you talk about merging 170,000 people and 22 agencies, you are talking about a lot of BHAS's—that's the acronym for Big Hairy Accounting Systems, not to mention big hairy financial management systems, human resource systems, and the like.

Of course, it just so happens that's WebMethods' bread and butter. We are a company of nearly 1000 people, based in Fairfax, with 50 offices in 18 countries throughout the world. We make commercial, off-the-shelf software that, in our view, is cheaper, faster,

more reliable, and more secure than the old fashioned way of hiring lots of human beings to write software code to connect different systems. Instead, we provide a single software platform that all the different systems and databases plug into.

We do this for Fed Ex, Dell, 3M, Office Depot, Apple, Verizon, Best Buy, Freddie Mac, the Army, NSA, EPA, and about 1000 other household name companies and government organizations. For Bank of America, we are the standard integration platform for their retail banking arm, all their ATMs, branch tellers, web access, and every voice response you get when you call them. For Motorola, we connect all their countless facilities around the planet. So the commercial world knows us well.

But how does a relatively small company like ours, no matter how great its product, get into a big agency like DHS? Well, I wish it were like getting to Carnegie Hall and all it takes is practice, but no, that's not enough. If it were a matter of vast world-class experience, DHS would be ringing our phone off the hook.

The fact is, it's not easy, and here's some reasons why:

First, those heroic people at DHS have a million other things to do. Thank heavens they don't stop every moment to listen to every vendor. But we'd like to think that integration is about as high a priority as you can get, and that they will be looking for the best technology, so I keep hoping that when I check my voice mail each day there will be an urgent message waiting from Steve Cooper.

Second, relatively small companies like ours depend on relationships with giant prime contractors, who agencies deal with first and foremost. Have I forgotten to mention how wonderful a company Unisys is?

Third, the government is a bit of an IBM shop on the civilian side. Even though top analysts may say our software is superior in our particular niche, never underestimate the bureaucratic appeal of the deniability you get if there's ever a problem and you can say, "Hey, man, I bought IBM." But we're stubborn and know someday they'll say that about webMethods.

Fourth, there is still something called architecture being established, and of course you wouldn't start building a house and buying components without a blueprint.

Finally, there ain't a lot of money sloshing around—yet. That's where this fine Committee and Congress come in, so that's above my pay grade to comment.

But on the bright side, there are now some pilot programs, and we do hope to participate in those. We are lucky that, in general when our software is evaluated, people love it and we get contracts. If I had one thing to suggest to DHS, it would be that there should be more proactive evaluation of specific technology like ours. I suspect DHS agrees, and when the dust settles from the merger, there may be.

Mr. Chairman, integration is not just a subject for techies. It has huge implications for our economy, foreign policy, and homeland security. This committee will leave an extraordinary legacy if it gets ordinary Americans to understand the power for good that information-sharing, a/k/a integration, can have in our daily lives—making government run more efficiently, and helping to prevent terrorism.

The Department of Homeland Security is the best imaginable laboratory and showcase for this revolution, and as an integration company, we at webMethods are excitedly hoping that the example it sets will be a great one. We are deeply indebted to this Committee for trying to make that happen, and we stand ready to help.

Thank you again for your invitation.

Mr. SHAYS. Thank you. You all are a wonderful panel. Let me just try to understand a few things, first off.

Mr. Perkins, you have a contract, your company has a contract with DHS as we stand right now. A number of them or one?

Mr. PERKINS. We have many contracts. We worked with most of the 22 agencies prior to their becoming part of the department. So we do now.

Mr. SHAYS. OK, I want to come back to that because this is a wonderful opportunity to see how the system is going to work.

How about you, Mr. Baroni.

Mr. BARONI. We have several contracts with the various agencies, but the main contract we have is the one I referenced in my testimony, ITMS.

Mr. SHAYS. And that was a contract established before DHS or after?

Mr. BARONI. Established, technically, before DHS, yes.

Mr. SHAYS. OK. And, Mr. Bisnow.

Mr. BISNOW. None.

Mr. SHAYS. None. Now it is interesting to think of a company with 1,000 employees as being relatively small, but, you know, I thought you were going to be telling me about how you work in the kitchen, and so on. I mean you are a pretty established company here.

Mr. BISNOW. We are one-thirty-seventh of their size.

Mr. SHAYS. Right. So it means you are more nimble, more flexible, and so on. I don't feel sorry for you.

Bottom line: What I would love to know, but I am intrigued by it, Mr. Perkins, walk me through—you are in a wonderful position to describe the benefits or the challenges of bringing 22 into 1, because you have worked with different parts. And, Mr. Baroni, are you in some cases—I am getting the sense that you are interacting, your two companies are interacting and sharing certain responsibilities.

Let me just throw these questions out now. Have we in some cases made some of these contracts moot in the sense that one supersedes another or it doesn't make sense anymore now that we are integrated, and so on? So who wants to begin?

Mr. PERKINS. Let me start with your first question about the integration of the departments. I do think we are in a unique position because we have been working on the information technology problems of the agencies, and now of the department, and they come in two classes. I think it is important to differentiate those as we think about making progress.

The set of problems on the business side, if you will, are around programs. That deals with threat lists and managing those threat lists and responding to them. There is another set on the back office side, if you will, or kind of the operational side. And we participate in both.

On the operational side, we see a tremendous opportunity for synergy, integration and consolidation. How many financial systems do you need, etc? And there is an opportunity to do that. I would encourage us to proceed with all energy on that side.

Mr. SHAYS. Let me just interrupt you. So in the case of your having a number of contracts now with just one department, are you

going through and recommending that you don't need to pursue this contract? Are you coming back and suggesting that, instead of doing this with three different parts, that you do one, one thing, with many parts?

Mr. PERKINS. Yes, we have been working with the individual CIOs since the formation of the department was proposed on how they might integrate systems that they have running on Oracle technology, either business systems or program systems that run our data base technology, how they can integrate those, how they can communicate, how they can consolidate for more efficient business operations, and better information. We work with those regularly. Those CIOs participate at a CIO Council level with Steve Cooper. We think we have an ability to communicate and participate in that discussion.

Mr. SHAYS. Do you want to jump in?

Mr. BARONI. Sure. As it relates to the question you asked about the contract and the contract vehicles, our belief is that the one that we established with TSA is a best practices contract vehicle. So our preference is to see as many of the folks use that, meaning vendors and contractors, use that vehicle in order to do business with the Department of Homeland Security.

Now take, for example, the work we are doing with Oracle, where we actually negotiated a license agreement with them, with extensibility to all of the departments of Homeland Security. So that there would be just one vehicle for acquiring that. So that is just one example of how you could actually get away or reduce the number of contract vehicles out there.

Mr. SHAYS. I am coming to you in a second, Mr. Bisnow, but let me just ask you this. This may seem a little off the subject, but very much an interest of mine.

You were working with these different agencies with people that technically could be consolidated under one department, information folks in different agencies now coming to one. Are you starting to see that happen, and do you see some benefits here?

Mr. BARONI. What we are seeing right now is that the agency, or I should say the department, is putting the plans together around that. We heard that in Steve Cooper's testimony. But the plan is to look for opportunities, as driven by re-engineered business processes, by rethought-through business models, where they can optimize resource-sharing and the leverage of information technology investments.

So those are the goals: The improvement of Federal—I should say the optimization of the use of Federal resources.

Mr. SHAYS. Mr. Bisnow, given that you are a candid person, as you are hearing this dialog, what is going through your mind?

Mr. BISNOW. I guess you can't repeal the laws of human nature. People want contracts, and they——

Mr. SHAYS. So am I to infer in that we should be starting over again, saying, you know, new department; let's cancel all the old stuff and let's start fresh?

Mr. BISNOW. Probably not, because, my experience is usually that causes a whole set of unexpected problems, but I am no expert on that.

Mr. SHAYS. OK. I have a feeling you are.

Mr. PERKINS. If I might——

Mr. SHAYS. Sure.

Mr. PERKINS. May I just comment on that?

Mr. SHAYS. Yes.

Mr. PERKINS. I think one of the things that I have been very impressed with in the department is the openness and the persistence of their outreach, not just to companies like Oracle or Unisys or others who have an institutional position that can help them accelerate the transformation, but out to smaller companies who have component technologies that can play a role either in integration or have biometric technologies or those kinds of things. I think there has been a decided outreach, and I think there is a real need for us to reinforce that outreach and the openness of that outreach, because there are terrific technologies out there that need to be incorporated into the solutions.

Mr. SHAYS. My committee, the National Security Subcommittee, oversees Defense and the State Department. We have added in now Homeland Security. But we had a real giant of a gentleman from California. He used to do the management in information systems. So we kind of all deferred to him over the last few years, no longer, Congressman Horn.

What has been a gigantic disappointment for us, as we have looked at information systems in DOD, has been that one after another have not succeeded. Then we have new management folks, and so on.

One of the questions I would love to ask you is: Is the Government at somewhat a disadvantage because it has folks that, one, come in and out, and, two, frankly, are not paid all that much? In other words, are they up against—is the pay structure of Government such that we are disadvantaged at getting people with the latest skills, etc?

Mr. PERKINS. I think, if I might, there certainly is an expectation gap, if we think about the Department of Defense and the uniformed person coming in, with their ability to go home and buy things over the Web and their ability to go on the base and do the same thing are dramatically different. So that expectation differs.

I don't think it is a capability issue, though, in transformation. There clearly is an issue of persistence of senior leadership, particularly on the defense side, as you have rotations in administrations and forced rotation in command structure as well.

I think the only thing that will make that be successful, in my view, is a transformation of business process to lead technology. We heard Steve Cooper talk about that today and Mark Forman talked about it also.

If all we see is the systems change and the process stay the same, and the organization to support them stay the same, we know we have made no progress. We probably spent a lot of money, but we have made no progress.

I think that kind of business transformation has to be led. I have been around the government marketplace for 26 years. I see a real interest and persistence in doing that. It is going to take a while to do. Oracle has gone through a transformation on our own. We are in about our third year of it, and we saved $1 billion in our operating base, but it is hard, even for a company of Oracle's scale,

to do that. So I think there is an opportunity to do it, but we have to start with business change first.

Mr. BARONI. Can I pick up on his comment there?

Mr. SHAYS. Yes, sir.

Mr. BARONI. To your direct question, I would say, as I look at the government systems and compensation structures, I would say they are completely arcane and they lack competitiveness with the private sector. That is why I think that the government has to have a marriage with the private sector in order to accomplish their mission.

Mr. SHAYS. Well, they clearly need that, and I understand that, but I guess what I am wondering is, in that negotiation process and the oversight process that the government is doing, we hire out; you do the job. Are we able to match the skill with the private sector to be able to bring out the best in the private sector, etc? And that is kind of what I am wondering. I am getting the sense that we are somewhat, but the turnover is the big challenge.

Mr. BARONI. I think, yes, you definitely face turnover issues. But I think, from what I have seen—and, obviously, my experience has been focused in on TSA and their ITMS efforts, and I have actually had a hands-on perspective there. My perspective is that, if you look at the aging work force, you don't need allegiance. The government doesn't need to have allegiance of folks out there any longer trying to do all these different functions.

But by hiring strong folks that can stay within the Federal Government and carry out the program management and oversight responsibilities of these efforts, then they are going to be able to—and you need fewer of them—then you are going to be more successful in overseeing these contractor efforts.

Mr. SHAYS. Thank you.

Mr. Bisnow, I want to ask you this: you really started out—and, obviously, speaking to someone with my minimal level of technical skills here——

Mr. BISNOW. From one to another.

Mr. SHAYS. No, I don't believe that. Otherwise, I don't want to ask you the question. [Laughter.]

OK. No, but the point that you were basically making is that our systems need to be able to talk with each other. Implicit in your comment to me was, it is not going to take a rocket scientist to do that, and why aren't we doing it? So, one, am I right in assuming that is what you are saying? Then my second question is, why aren't we doing it?

Mr. BISNOW. You bet it is easy. You bet, it is technologically easy.

Mr. SHAYS. OK.

Mr. BISNOW. And it is a red herring when people say, "Oh, that's just so complicated." We do it every day on the commercial side for lots of big companies.

The problem is—I hate to throw it back into your court—policy and politics. You know, do people want to share information? Do they want to change? There is lots of vested interest in the status quo. It is human nature.

But, you know, to try to connect that with your last question about, do we pay people enough, you know, sometimes people can

be paid in psychic income. One thing that on occasion is very exciting about working in government—and I have worked in government—is if you think you are sitting on top of a really cool revolution and that what you are doing really matters.

Mr. SHAYS. Right.

Mr. BISNOW. I think that if people began to see that this has a practical impact, and everybody, instead of hating the government, says, "Oh, wow, this is great. We taxpayers are getting our money's worth," and "Oh, wow, there haven't been any terrorist acts and it's because we've gotten good information and nabbed people," I think if I were a part of a CIO's office, I would take great pride in that. I would be telling people at dinner, "Wow, you know, I worked on this and that's why you guys are happy out there."

So I would think about paying, you know, really focusing on the excitement of the revolution that is in front of us, and not getting caught up in all the trees.

Mr. SHAYS. Well, I have an exciting activity. I am supposed to have a press conference with McCain and Feingold at 1 p.m., in the Russell Building on campaign finance reform, something we have worked on a long time. There would be many things that would keep me here, but that is one thing that is going to move me away.

Is there any last thing that we need to put on the record? Mr. Perkins, anything that you just want to make sure——

Mr. PERKINS. I would just refer back to my remarks. I think there is opportunity to encourage, through the money that is already being spent for homeland security, the adoption of a policy like NSTISSP No. 11, an independent evaluation of a security capability of products you are going to buy anyway. If you do that, you will encourage companies, and require companies like Oracle already does and others, to build that into the core of their products, and that becomes available when it is bought by a utility company or a financial services company or a municipal police department.

And as a byproduct of all this money spent, we will lock down the critical infrastructure not just for homeland security, but for cyber terrorism. I think we should think of peacetime dividends for some of these investments as well.

Mr. SHAYS. Thank you.

Mr. Baroni.

Mr. BARONI. My comments are concluded, and I just want to respect your desire to get over to vote.

Mr. BISNOW. Thank you.

Mr. SHAYS. Thank you. I don't usually miss something for a press conference, but this is somewhat exceptional.

Let me thank you all and say the record will be open for 2 weeks. There may be some questions our staff needs to ask you to respond to and that you may want to put on the record.

With that, I am going to adjourn this hearing and run out. Thank you.

[Whereupon, at 1:02 p.m., the committee was adjourned, to reconvene at the call of the Chair.]

[Additional information submitted for the hearing record follows:]

Question from Rep. Turner to Mr. Cooper:

Your agency recently released a report on the sharing of terrorist watch lists between federal, state and local agencies (GAO-03-322). The report discussed the importance of an enterprise architecture that served all agencies needs. The report went on to discuss the role of database architectures as an integral component of the overall enterprise architecture. Specifically, the report pointed out the problems encountered unless data is consolidated as opposed to relying on decentralized databases. The report recommends that the agencies move to consolidate these watch lists.

Can you tell me what steps the Department is taking to centralize terrorist watch lists? When do you anticipate that all agencies will be using a common, centralized watch list database? Are you working to consolidate other data sources in the department to enable the correlation of relationships that can point to developing threats?

Question from Rep. Turner to Mr. Dacey:

The GAO recently released a report on the sharing of terrorist watch lists between federal, state and local agencies (GAO-03-322). The report discussed the importance of an enterprise architecture that served all agencies needs. The report went on to discuss the role of database architectures as an integral component of the overall enterprise architecture. Specifically, the report pointed out the problems encountered unless data is consolidated as opposed to relying on decentralized databases. The report recommends that the agencies move to consolidate these watch lists.

While your report is specific to terrorist watch lists, I am interested in whether you believe that the Department of Homeland Security should be also be consolidating other "stovepiped" databases in order to enable the correlation of relationships in that data that can point to developing threats. Can you comment on this?

Questions from Rep. Turner, Government Reform Committee
To Steve Cooper
"Out of Many, One: Assessing Barriers to Information Sharing in the Department of Homeland Security"
May 8, 2003

Question from Rep. Turner to Mr. Cooper:

The GAO recently released a report on the sharing of terrorist watch lists between federal, state and local agencies (GAO-O3-322). The report discussed the importance of an enterprise architecture that served all agencies needs. The report went on to discuss the role of database architectures as an integral component of the overall enterprise architecture. Specifically, the report pointed out the problems encountered unless data is consolidated as opposed to relying on decentralized databases. The report recommends that the agencies move to consolidate these watch lists.

Can you tell me what steps the Department is taking to centralize terrorist watch lists? When do you anticipate that all agencies will be using a common, centralized watch list database? Are you working to consolidate other data sources in the department to enable the correlation of relationships that can point to developing threats?

"Watch lists" contain information on terrorists; they support a variety of homeland security missions. A distinction should be made between the terms "database" and "watch list." A database is the storehouse of a large amount of data, while a watch list is an extracted portion of the database.

The GAO is correct in its assessment that the Government's approach to using watch lists has been decentralized, because the lists were developed in response to individual agencies' unique missions. Those historical missions include the duties of the law enforcement and intelligence communities, and now include the mission to defend the homeland. The effort to share more quickly and broadly all the information we have on terrorists, from which watch lists may be generated, requires close coordination among DHS, Intelligence agencies, Department of State, Department of Justice, the new Terrorism Threat Integration Center (TTIC), and the White House. We also need to share information with State and local government partners and even private-sector operators of critical infrastructure facilities.

Eleven lists were identified by the recent GAO report in the "as is" inventory. Most of the information on all these lists derive from one database – the Department of State TIPOFF database – which itself is fed from a variety of Intelligence Community sources. Plans to make significant improvements in the speed and scope of dissemination of information from this database are being developed. Also, a plan to improve the

dissemination of information from the database a three levels of classification has been developed, including a concept of operations, phasing, and technical approach.

Re-engineering the entire process is a major effort, and the technology issues are less difficult than the legal and operational questions that must be worked through. Meanwhile, some immediate improvements are being made in how watch lists are used, and in information sharing generally among homeland-security partners.

United States General Accounting Office
Washington, DC 20548

July 7, 2003

The Honorable Tom Davis
Chairman, Committee on Government Reform
House of Representatives

Subject: *Post-hearing Question From the May 8, 2003, Hearing on Barriers to Information Sharing at the Department of Homeland Security*

Dear Mr. Chairman:

As requested, this letter provides our response for the record to the question posed by Representative Michael Turner to GAO, in your letter of June 13, 2003.

> *The GAO recently released a report on the sharing of terrorist watch lists between federal, state, and local agencies (GAO-03-322).*[1] *The report discussed the importance of an enterprise architecture that served all agencies' needs. The report went on to discuss the role of database architectures as an integral component of the overall enterprise architecture. Specifically, the report pointed out the problems encountered unless data is consolidated as opposed to relying on decentralized databases. The report recommends that the agencies move to consolidate these watch lists.*
>
> *While your report is specific to terrorist watch lists, I am interested in whether you believe that the Department of Homeland Security should also be consolidating other "stovepiped" databases in order to enable the correlation of relationships in that data that can point to developing threats. Can you comment on this?*

Standardizing and consolidating stovepiped databases can offer significant benefits. In particular, it can help reduce or eliminate duplicative data capture and storage and enable faster data access and better data consistency, which can reduce costs as well as improve data reliability and sharing. Analyzing these benefits in relation to associated costs and risks, such as security and privacy, provides a basis for informed decisions about not only consolidation but also the appropriate level of consolidation. Effective development of enterprise architectures provides for performing such analysis.

---

[1]U.S. General Accounting Office, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, GAO-03-322 (Washington, D.C.: April 15, 2003).

In the case of federal watch lists, we identified indicators (such as the number and variability of the lists and the commonality of their purposes) of opportunities to consolidate and standardize. Consequently, we recommended that the Department of Homeland Security determine the extent of watch list consolidation needed to accomplish its mission and that such consolidation be done as part of the department's efforts to develop an enterprise architecture.

We believe this approach—analyzing information and data needs and solutions within the context of an enterprise architecture—is also necessary to determine the extent to which all existing systems of the department's 22 component agencies should be standardized and consolidated. In fact, during the subject hearing, the department's chief information officer testified that it plans to develop and use an enterprise architecture to guide its systems consolidation and integration. He stated that the department plans to issue the enterprise architecture by the fall of 2003.

If you have any questions concerning this information, please contact me at (202) 512-3439 or hiter@gao.gov, or Gary Mountjoy, Assistant Director, at (202) 512-6367 or mountjoyg@gao.gov.

Sincerely yours,

Randolph C. Hite
Director, Information Technology Architecture
and Systems Issues

(310264)

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:	Voice:	(202) 512-6000
	TDD:	(202) 512-2537
	Fax:	(202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON RECYCLED PAPER