THE IT ROADMAP: AN OVERVIEW OF HOMELAND SECURITY'S ENTERPRISE ARCHITECTURE

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

FIRST SESSION

OCTOBER 8, 2003

Serial No. 108–129

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
92–900 PDF WASHINGTON : 2004

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*

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

ADAM H. PUTNAM, Florida, *Chairman*

CANDICE S. MILLER, Michigan
DOUG OSE, California
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio

WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts

EX OFFICIO

TOM DAVIS, Virginia

HENRY A. WAXMAN, California

BOB DIX, *Staff Director*
SCOTT KLEIN, *Professional Staff Member*
URSULA WOJCIECHOWSKI, *Clerk*
DAVID MCMILLEN, *Minority Professional Staff Member*

CONTENTS

THE IT ROADMAP: AN OVERVIEW OF HOMELAND SECURITY'S ENTERPRISE ARCHITECTURE

WEDNESDAY, OCTOBER 8, 2003

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:40 a.m., in room 2247, Rayburn House Office Building, Hon. Adam Putnam (chairman of the subcommittee) presiding.

Present: Representatives Putnam, Murphy, and Clay.

Staff present: Scott Klein, professional staff member; Bob Dix, staff director; Ursula Wojciechowski, clerk; John Hambel, counsel; David McMillen, minority professional staff member; and Teresa Coufal, minority assistant clerk.

Mr. MURPHY [presiding]. Good morning. As you can tell, I'm not Mr. Putnam. His flight is delayed. He'll be here soon and I'll be starting off for him. A quorum being present, this hearing of the Subcommittee on Technology, Information Policy, Intergovernment Relations and the Census will come to order.

Good morning and welcome to today's hearing on a very important information technology initiative: The Department of Homeland Security's Enterprise Architecture. This morning the subcommittee will be examining the Department's release of its first enterprise architecture as well as how it aligns with the overall Federal Enterprise Architecture and E-Government strategy.

Less than a year ago, on November 25, 2002, President Bush launched this enterprise architecture development process by signing into law the bill that combined part or all of 22 Federal agencies into one Cabinet-level umbrella known as the Department of Homeland Security. As you may be aware, this consolidation is the largest reorganization of the Federal bureaucracy since our Defense Department and intelligence agencies were restructured over a half century ago.

In addition to the challenges of consolidating and integrating the masses of disparate information technology systems to allow 22 agencies to function as a cohesive organization, the Department quickly discovered it had a critical and enhanced role to secure, analyze, and share important information across traditional agency boundary lines, including intergovernmentally.

To achieve the Department's core mission, the need to interface and become interoperable with systems internally and externally quickly became a top priority. The Department inherited a collection of legacy systems for a variety of missions, from securing our borders to providing intelligence data identifying subjects of interest. Clearly the challenge was, and continues to be, an enormous exercise in collaboration that requires cooperation throughout the entire organization.

In assessing the huge task it faced, the Department of Homeland Security discovered it operated more than 1,000 servers and approximately 700 different applications, including more than 300 applications performing some variety of back-office operations. Nearly 50 of those disparate applications have been functioning to prevent and respond to terrorist events.

As we have seen during congressional debate and at hearings, the Department has faced tremendous challenges to become interoperable in unifying multiple field structures; blending the cultures of each agency and some 180,000 employees; standardizing data to improve information sharing; and integrating both existing applications and IT. Needless to say, building an effective Department from 22 separate entities will require sustained leadership from both IT and other top managers to ensure the transformation of a diverse collection of agencies, programs, and missions into an integrated organization. Quite frankly, some have expected this transformation to simply occur overnight and fail to fully appreciate the magnitude of the effort required to achieve the integrated functionality necessary to operate in a collaborative manner. The IT challenge is only part of the equation, however; the success of that component is critical to the ultimate success of the transformation itself.

The challenges that face the Department are both real and difficult, in fact, leading the General Accounting Office to designate the administration of the Department as a high-risk area. Foremost among those challenges is the Department's development and implementation of a coherent enterprise architecture to support its mission. Even the President's own homeland security strategy identifies, among other things, the need for an enterprise architecture as a necessary component to achieving the goal of the Department's systems interoperating effectively and efficiently.

As I am confident our witnesses will convey today, an enterprise architecture is a very important step because it will help identify shortcomings and opportunities in current homeland security-related operations and systems, such as duplicative, inconsistent, or missing information.

I also understand that 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, I understand that OMB, in its examination of DHS's overall IT program, an effort to identify redundant activities that might be candidates for consolidation and integration through the IT budget submission process, has taken an initial first step to evaluate DHS's component systems.

Given the climate that exists in our world today and the eminent danger that confronts our Nation, there are justifiably huge expectations for the Department of Homeland Security. Many folks are insisting upon results, and today we will examine a significant step forward in producing those results. Truthfully, it is a remarkable achievement that we are here today, in such a short period of time by virtually anyone's measure, to unveil this critical information technology milestone at the Department of Homeland Security.

This subcommittee has held 15 hearings during the 108th Congress focused on e-government, integration and consolidation of governmentwide functional IT systems, information privacy and cyber security. Development of an effective enterprise architecture at the Department will provide a detailed roadmap to address nearly all of the important IT issues examined this year by the subcommittee, including how DHS will configure its IT in such functions as grants management, geospatial information, HR and financial management systems, smart cards and biometrics, records management and the handling of personally identifiable information by government.

In addition, this subcommittee's oversight activities on cyber security have made it abundantly clear that developing and adhering to an enterprise architecture is the most effective method of integrating information security solutions over the long term. Congress recognized the importance of EA in assessing risk and achieving secure systems through passage of the Federal Information Security Management Act, which requires agencies to consider security throughout the life cycle of a system. Consistent with today's architecture release, we will continue to press for cyber security solutions at the initial stages of systems development versus attempting to attach expensive, disparate solutions to the old processes and systems as an afterthought.

Finally, on a broader scope, the subcommittee will review how this initial Department of Homeland Security roadmap aligns with the overall Federal Enterprise Architecture and E-Government Strategy managed by the Office of Management and Budget. Accordingly, we are very pleased to be joined today by the distinguished CIO from DHS, Mr. Steve Cooper, and we welcome the brand new administrator for Information Technology and E-Government, Karen Evans, for her very first appearance at a congressional oversight hearing in her new position.

I now yield to the gentleman from Missouri, the ranking member, Mr. Clay, for any opening remarks that he may wish to make.

[The prepared statement of Hon. Adam H. Putnam follows:]

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

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

Congressman Adam Putnam, Chairman

OVERSIGHT HEARING
STATEMENT BY ADAM PUTNAM, CHAIRMAN

Hearing topic: *"The IT Roadmap: An Overview of Homeland Security's Enterprise Architecture."*

Wednesday, October 8, 2003
10:00 a.m.
Room 2247 Rayburn House Office Building

OPENING STATEMENT

Good morning and welcome to today's hearing on a very important information technology initiative… the Department of Homeland Security's Enterprise Architecture. This morning, the Subcommittee will be examining the Department's release of its first enterprise architecture, as well as how it aligns with the overall Federal Enterprise Architecture and E-Government strategy.

Less than a year ago, on November 25th, 2002, President Bush launched this enterprise architecture development process by signing into law the bill that combined part or all of 22 federal agencies into one cabinet-level umbrella known as the Department of Homeland Security. As may of you are aware, this consolidation is the largest reorganization of the federal bureaucracy since our defense department and intelligence agencies were restructured over a half-century ago.

In addition to the challenges of consolidating and integrating the masses of disparate information technology systems to allow 22 agencies to function as a cohesive organization, the Department quickly discovered it had a critical and enhanced role to secure, analyze, and share important information across traditional agency boundary lines, including inter-governmentally.

To achieve the Department's core mission, the need to interface and become interoperable with systems internally and externally quickly became a top priority. The Department inherited a collection of legacy systems for a variety of missions, from securing our borders to providing intelligence data and identifying subjects of interest. Clearly, the challenge was...and continues to be...an enormous exercise in collaboration that requires cooperation throughout the entire organization.

In assessing the huge task it faced, the Department of Homeland Security discovered it operated more than 1,000 servers and approximately 700 different applications, including more than 300 applications performing some variety of back-office operations. Nearly 50 of those disparate applications have been functioning to prevent and respond to terrorist events.

As we have seen during Congressional debate and at hearings, the Department has faced tremendous challenges to become interoperable in unifying multiple field structures; blending the cultures of each agency and some 180,000 employees; standardizing data to improve information sharing; and integrating both existing applications and IT. Needless to say, building an effective department from 22 separate entities will require sustained leadership from both IT and other top managers to ensure the transformation of a diverse collection of agencies, programs, and missions into an integrated organization. Quite frankly, some have expected this transformation to simply occur overnight, and fail to fully appreciate the magnitude of the effort required to achieve the integrated functionality necessary to operate in a collaborative manner. The IT challenge is only part of the equation, however, the success of that component is critical to the ultimate success of the transformation itself.

The challenges that face the Department are both real and difficult . . . in fact, leading the General Accounting Office to designate the administration of the Department as a high-risk area. Foremost among those challenges is the Department's development and implementation of a coherent enterprise architecture to support its mission. Even the President's own homeland security strategy identifies, among other things, the need for an enterprise architecture as a necessary component to achieving the goal of the Department's systems interoperating effectively and efficiently.

As I am confident our witnesses will convey today, an enterprise architecture is a very important step because it will help identify shortcomings and opportunities in current homeland-security-related operations and systems -- such as duplicative, inconsistent, or missing information.

I also understand that as part of its enterprise development efforts, the department has established working groups comprising state and local CIO's to ensure that it understands and represents their business processes and strategies relevant to homeland security. In addition, I understand that OMB, in its examination of DHS's overall IT program, and effort to identify redundant activities that might be candidates for consolidation and integration through the IT budget submission process, has taken an initial first step to evaluate DHS's component systems.

Given the climate that exists in our world today, and the eminent danger that confronts our nation, there are justifiably huge expectations for the Department of Homeland Security. Many folks are insisting upon results and today we will examine a significant step forward in producing those results. Truthfully, it is a remarkable achievement that we are here today, in such a short period of time by virtually anyone's measure, to unveil this critical information technology milestone at the Department of Homeland Security.

The Subcommittee has held 15 hearings during the 108th Congress focused on E-Government; integration and consolidation of government-wide functional IT systems; information privacy; and cybersecurity. Development of an effective enterprise architecture at the Department will provide a detailed roadmap to address nearly all of the important IT issues examined this year by the Subcommittee, including how DHS will configure its IT in such functions as: grants management; geospatial information; HR and financial management systems; smart cards and biometrics; records management; and the handling of personally identifiable information by government.

In addition, the Subcommittee's oversight activities on cybersecurity have made it abundantly clear that developing and adhering to an enterprise architecture is the most effective method of integrating information security solutions over the long-term. Congress recognized the importance of EA in assessing risk and achieving secure systems through passage of the Federal Information Security Management Act (FISMA), which requires agencies to consider security throughout the lifecycle of a system. Consistent with today's architecture release, we will continue to press for cybersecurity solutions at the initial stages of systems development versus attempting to attach expensive, disparate solutions to the old processes and systems as an afterthought.

Finally, on a broader scope, the Subcommittee will review how this initial Department of Homeland Security "roadmap" aligns with the overall Federal Enterprise Architecture and the E-Government strategy managed by the Office of Management and Budget. Accordingly, we are very pleased to be joined today by the distinguished CIO from DHS, Mr. Steve Cooper, and we welcome the brand new Administrator for Information Technology and E-Government, Karen Evans, for her very first appearance at a congressional oversight hearing in her new position.

Mr. CLAY. Thank you, Mr. Chairman, and thank you for calling this hearing. I also thank the witnesses for appearing before us today. Unfortunately, this morning is full of competing opportunities. The full Committee on Government Reform is downstairs holding a hearing on rebuilding Iraq, and I apologize for not being able to give this hearing my undivided attention.

It wasn't that long ago that information policy in the Federal Government was about buying computers. People talked about information resource management, but what they really meant was buying computers and computer software. Congress believed that information policy was about getting the right information to decisionmakers at the time they had to make a decision. That concept was a part of the last rewrite of the Paperwork Reduction Act which was written in the early 1990's. These competing concepts have come together and been named enterprise architecture.

Unfortunately, it took a few billion dollar mistakes at the IRS and the FAA before the executive agencies got it. When you strip away all of the jargon, the process of developing an enterprise architecture is about mapping the way an organization communicates and making sure those communications are timely and effective.

Congress put together 22 agencies from nearly every Department in the government to create the Department of Homeland Security. The managers of the Department now have the task of making those agencies work together as a cohesive whole.

The enterprise architecture is designed to be a roadmap for how that will happen. Like most maps, there are a variety of ways of getting from A to B. Some routes are more direct than others. Some are more expensive and some more educational. What really matters is how the Department chooses the route it will take. Implementing this transformation is about communication and cooperation. If the individuals and agencies within the Department lose sight of those goals, the process will fail and the Department will fail in its mission to protect the American public.

If this transformation becomes bogged down in selecting which personnel system will be used or which payroll system or whether it runs on PCs or Sun Microstations, the process will fail.

I look forward to our discussion today, and I hope our witnesses will proceed with a minimum of jargon. Thank you, Mr. Chairman.

Mr. MURPHY. Thank you, Mr. Clay.

[The prepared statement of Hon. Wm. Lacy Clay follows:]

STATEMENT OF THE HONORABLE WM. LACY CLAY AT THE HEARING ON ENTERPRISE ARCHITECTURE AT THE DEPARTMENT OF HOMELAND SECURITY

OCTOBER 8, 2003

Thank you Mr. Chairman for calling this hearing, and I thank the witnesses for appearing before us today. Unfortunately, this morning is full of competing opportunities. I have a mark-up proceeding in the Financial Services Committee, and the full committee is down stairs holding a hearing on rebuilding Iraq. I apologize for not being able to give this hearing my undivided attention.

It wasn't that long ago that information policy in the federal government was about buying computers. People talked about information resource management, but what they really meant was buying computers and computer software.

Congress believed that information policy was about getting the right information to decision makers at the time they had to make a decision. That concept was a part of the last rewrite of the Paperwork Reduction Act, which was written in the early 1990s. These competing concepts have come together and been named enterprise architecture. Unfortunately, it took a few billion-dollar mistakes at the IRS and FAA before the executive agencies got it.

When you strip away all of the jargon, the process of developing an enterprise architecture is about mapping the way an organization communicates, and making sure those communications are timely and effective.

Congress put together 22 agencies from nearly every department in the government to create the Department of Homeland Security. The managers of the Department now have the task of making those agencies work together as a cohesive whole. The enterprise architecture is designed to be a road map for how that will happen. Like most maps, there are a variety of ways of getting from A to B. Some routes are more direct than others. Some are more expensive, and some more educational. What really matters is how the Department chooses the route it will take.

Implementing this transformation is about communication and cooperation. If the individuals and agencies within the Department loose sight of those goals, the process will fail, and the Department will fail in its mission to protect the American public. If this transformation becomes bogged down in selecting which personnel system will be used, or which payroll system, or whether it runs on PCs or Sun micro-stations, the process will fail.

I look forward to our discussion today, and I hope our witnesses will proceed with a minimum of jargon.

Mr. MURPHY. I too hopefully will understand half of what is said. I will rely on you to understand the other half. Thank you for your leadership in this subcommittee.

I ask now that the witnesses rise to be sworn in.

[Witnesses sworn.]

Mr. MURPHY. Let the record show that both witnesses responded in the affirmative.

I'd like to start by introducing our first witness for her 5-minute opening statement, Karen Evans. On September 3, 2003, Karen S. Evans was appointed by President Bush to be Administrator of the Office of Electronic Government and Information Technology at the Office of Management and Budget. Ms. Evans replaces our good friend Mark Forman, and I understand she began as Administrator on Monday; and to her great fortune, 48 hours later she's testifying before Congress. I hope you've had time to prepare.

Prior to joining OMB this week, Ms. Evans was Chief Information Officer at the Department of Energy and served as a vice chairman at the CIO Council, the principal forum for agency CIOs to develop IT recommendations. Previously she served at the Department of Justice as Assistant and Division Director for Information Systems Management.

Ms. Evans, thank you for agreeing to serve in this important post. We are grateful for the work you're going to be doing, and we look forward to working closely with you and your staff. Welcome, and I yield 5 minutes for your opening statement.

STATEMENT OF KAREN S. EVANS, ADMINISTRATOR OF E-GOVERNMENT AND INFORMATION TECHNOLOGY, OFFICE OF MANAGEMENT AND BUDGET

Ms. EVANS. Good morning, Mr. Chairman, Ranking Member Clay, and members of the committee. It is my pleasure to be here during my first week as the new administrator of the Office of Electronic Government and Information Technology at OMB. Thank you for the opportunity to discuss with the committee the steps the administration has undertaken and will continue to take to improve Federal IT management, particularly as it relates to our homeland security mission.

Mr. Chairman, I know that under your leadership, this committee has been a forerunner in Congress on a number of critical IT issues such as enterprise architecture, e-government and IT security. I look forward to working with you and the committee to make progress on our shared priorities. My remarks will focus primarily on the administration's Federal Enterprise Architecture [FEA] efforts as well as OMB's role in assisting the Department of Homeland Security in their enterprise architecture [EA] work.

The development and implementation of the FEA is a key step toward achieving significant governmentwide improvement in the management of Federal IT resources. The FEA gives agencies a new way to describe, analyze, and improve how the Federal Government serves its citizens. By looking at the government's many lines of business, the citizen groups it serves, and the underlying tools and technologies, agencies will be better able to leverage resources while improving service delivery.

We will be able to identify opportunities to eliminate redundant investments while improving integration of resources and information sharing across Federal agencies with State and local governments.

This business focus framework will assist Federal agencies, OMB, and the Congress in improving the performance of the government. The outcome of our FEA efforts will be more citizen-centered, customer-focused government that maximizes technology investments to better achieve mission outcomes.

The FEA also directly supports the development of individual agency's EAs by providing a framework for agencies to align their performance, business, data application and technology layers to the FEA.

OMB has leveraged both traditional management and budget processes to ensure that the FEA is directly linked to and informed by each agency's EA and agency's IT investments. Each agency's EA must describe how they meet their missions through the use of people, business processes, data and technology, while each major IT investment request must detail how the investment is aligned with and supports the FEA and the agency EA.

While it is essential for each agency to develop and implement an EA, nowhere is this more critical than for the Department of Homeland Security. Achieving effective homeland security will require IT investments that guarantee realtime information sharing to improve response time and decisionmaking. To meet these goals and assist in overcoming information sharing barriers, we require wise IT investments that support homeland security missions, enhance productivity and improve information sharing while providing for security and privacy.

In his proposal for creating the Department over a year ago, the President highlighted the use of EA techniques. The President stated that the development of a single EA for the Department would result in elimination of duplicative and poorly coordinated systems that are prevalent in government today, and that we must fund homeland security missions based on an overall assessment of requirements rather than a tendency to find all good ideas beneficial to a separate unit's individual needs even if similar systems are already in place elsewhere.

The merging of 22 previously separate agencies has resulted in DHS inheriting many redundant and overlapping IT systems and processes, nearly all designed to address individual programs. Both the FEA and the Department's EA will be instrumental in identifying opportunities for both reducing existing duplication and preventing new redundant investments.

Throughout the fiscal year 2005 budget process, OMB will work with the Department to eliminate redundant and nonintegrated operations systems and processes for both IT infrastructure and mission areas. DHS's EA is indispensable to achieving these results.

However, to be an effective tool, the EA must reflect organizational decisions made by the Department's leaderships and be used by the entire Department and particular senior officials in mission and management in making all resource decisions.

Tough but necessary investment decisions must be made on which systems and processes remain, which will be consolidated and which are eliminated.

OMB will continue to oversee DHS's efforts to implement their EA, consolidate their IT investments and support and shepherd E-gov initiatives through both management and budget processes. Through the budget process OMB will assess all DHS major IT investments with a strong focus on planned integration and consolidation of overlapping systems.

Additionally, through the President's Management Agenda, under the expanding electronic government score card, OMB will assess on a quarterly basis the Department's progress in their EA development and implementation as well as their IT consolidation activities.

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. Both the FEA and DHS's EA are vital tools necessary to improve the management and performance of our homeland security missions. While we recognize the significant challenges facing DHS in consolidating the cultural and resource legacies of 22 component agencies, we fully expect that DHS leadership will continue to build an integrated and interoperable structure.

To ensure we successfully meet this goal, OMB will work with DHS leadership to ensure that their EA efforts, their integration of business processes and consolidation and elimination of redundant IT investments remains a top priority and is addressed in a timely manner.

I look forward to working with the committee on our shared goals of improving the Federal Government's management of all its IT resources, including those related to homeland security. Thank you.

Mr. MURPHY. Thank you, Ms. Evans.

[The prepared statement of Ms. Evans follows:]

STATEMENT OF
THE HONORABLE KAREN EVANS
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND
INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS, AND THE CENSUS
U.S. HOUSE OF REPRESENTATIVES

October 8, 2003

Good morning, Mr. Chairman, Ranking Member Clay, and Members of the Committee. It is a pleasure to be here during my first week as the new Administrator of the Office of Electronic Government and Information Technology at the Office of Management and Budget. Thank you for the opportunity to discuss with the Committee the steps the Administration has undertaken and will continue to take to improve Federal IT management, particularly as it relates to our homeland security mission. My remarks will provide an update on both the Administration's Federal Enterprise Architecture (FEA) efforts as well as address OMB's role in assisting the Department of Homeland Security (DHS) with their EA work.

Federal Enterprise Architecture – Update and Next Steps

The development and implementation of the FEA is a key step toward achieving significant government-wide improvement in the management of Federal IT resources. The purpose of the FEA is to identify opportunities to simplify processes and unify work across Federal agencies and within the lines of business of the government. It is a business-focused framework developed for Federal agencies, OMB, and the Congress to use in improving the performance of government through improved coordination and wiser investments. Specifically, the FEA will enable the Federal government to:

- Identify opportunities to leverage technology and alleviate redundancy, or to highlight where agency overlap limits the value of IT investments;
- Facilitate horizontal (cross-Federal) and vertical (Federal, State and Local) integration of IT resources;
- Establish a clear view of IT support to mission and program performance; and
- Support a more citizen-centered, customer-focused government that maximizes IT investments to better achieve mission outcomes, while eliminating duplicative and wasteful investments.

The development of individual agency EAs is critical to the success of the FEA. Each agency's EA will describe how they meet their missions through the use of people, business processes, data, and technology. Both agency EA efforts and their IT budget documents directly inform and help to build the FEA. In turn the FEA, as described in OMB guidance, serves as a framework for agencies to align their performance, business, data, application, and technology layers to the FEA. The work of the Federal Chief Information Officers Council's Architecture and Infrastructure Committee is instrumental in linking agency EA's and the FEA. This is the key linkage to allow comparisons across agency, and even governmental, boundaries to identify sharing, collaboration and consolidation opportunities.

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 identify 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 was released on June 12 of this year and was required for use by all agencies 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 by business line and set baselines and targets. This allows effective comparisons of the relative performance of like investments. The PRM was released on September 17 of this year, but a final draft was available in June for agencies use in the FY 2005 budget formulation process.
- The *Service Component Reference Model (SRM)* provides the foundation for the re-use and sharing of IT components across Federal agencies, and potentially across Federal, state and local governments. The SRM was released on June 12 of this year for use by agencies in the FY 2005 budget formulation process.
- The *Technical Reference Model (TRM)* provides a set of technology standards and specifications that support the assembly and use of service components. The TRM will facilitate the transition to e-government by supporting interoperability and standardization across Federal agency systems. This will encourage the sharing of infrastructures across agencies and levels of government. The TRM was released on June 12 of this year for agencies use in the FY 2005 budget formulation process.
- 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 sharing of information across Federal agencies and with state and local governments. 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.

Enterprise Architecture and Homeland Security

While it is essential for each agency to develop and implement an EA, no where is this more critical than for the Department of Homeland Security. Achieving effective homeland security will require IT investments that both guarantee real-time information sharing, to 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, and improve information sharing while ensuring security and privacy.

In his proposal for creating the Department over a year ago the President highlighted the use of EA techniques to improve both the sharing and use of information. The President stated that the "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."

The merging of twenty-two previously separate agencies has resulted in DHS inheriting a number of redundant and overlapping IT systems and processes, nearly all designed to address individual programs. Throughout the FY 2005 budget process, OMB will work with the Department to eliminate redundant and non-integrated operations, systems, and processes for IT infrastructure and mission areas. Through consolidated business cases, the relevant systems for consolidation will be listed, plans for migration and elimination will be reported, and an integrated business process identified. 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. DHS' current state and target architectures as well as their transition strategy to move from their current state to their target architecture are indispensable to achieving these real results.

However, to be an effective tool, the EA has to reflect organizational decisions made by the Department's leadership and be owned and used by the entire Department in making all resource decisions. Tough but necessary investment decisions must be made on which systems and processes remain, which will be consolidated, and which are eliminated. This serves to underscore the point that the EA is not and should not be simply viewed as an IT exercise. Information technology is not the driver; it is the enabler to assist the Department in meeting its missions.

The benefits to our nation will of successful implementation of these efforts are significant and far-reaching. For example, more efficient information sharing between all levels of government and law-enforcement will result in improved capabilities to safeguard our nation at our borders and points of entry. Additionally, through the use of the FEA and DHS' use of their EA, we will be able to prevent unnecessary and wasteful investments, saving taxpayer dollars.

Additional Government-wide Efforts to Improve Homeland Security

As you know, the Administration has been aggressively working over the last two years 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.

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 manager's 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.

OMB Assistance and Oversight

In addition to continuing our efforts in the development and implementation of the FEA, OMB will also continue to work with DHS on their efforts to execute a comprehensive EA that optimizes the existing investments inherited from the legacy agencies, and eliminates redundant investments.

Specifically, OMB will monitor, assess, and enforce IT management policies and requirements through both budget and management processes. Through the budget process, OMB will assess all DHS major IT investments, with a strong focus on planned integration and consolidation of overlapping systems. OMB will also review the Department's recently completed EA.

Additionally, through the President's Management Agenda, under the Expanding Electronic Government Scorecard, OMB will assess on a quarterly basis, the Department's progress in their EA development and implementation.

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. Both the FEA and DHS' EA are vital tools necessary to improve the management and performance of our homeland security missions. While we recognize the significant challenges facing DHS in consolidating the cultural and resource 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-optimized, duplicative, and poorly coordinated systems."

To ensure we successfully meet this goal, OMB will work with DHS leadership, in particular with the Department's CIO who is responsible for leading DHS' EA, to ensure that their EA efforts, their integration of business processes, and consolidation and elimination of redundant IT investments remains a top priority and is addressed in a timely manner. I look forward to working with the Committee on our shared goals of improving the Federal government's management of all of its IT resources, including those related to homeland security.

Mr. MURPHY. Our second witness this morning is Steven I. Cooper, Chief Information Officer of the U.S. Department of Homeland Security. Prior to being appointed by the President to be the first CIO at the Department, Mr. Cooper served at the White House as a Special Assistant to the President for Homeland Security.

Prior to Federal service, Mr. Cooper spent 20 years in the private sector, most recently as a CIO at Corning in New York. Previously he served as Director of IT for Eli Lilly & Co. in Indianapolis. He also held key IT management positions with CSC, Maxima, and CACI.

Mr. Cooper, you certainly have been given a monumental task, and I know Members of Congress are looking forward to your candid views on this subject and the Department of Homeland Security. You may proceed.

STATEMENT OF STEVEN I. COOPER, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. COOPER. Thank you. Mr. Murphy and members of the subcommittee, I'm very pleased to appear before the subcommittee today. I want to thank the chairman and members of the subcommittee for giving me the opportunity to talk about the Department of Homeland Security's enterprise architecture efforts and initiative. I'm very pleased to announce to you that we have completed the first version of our target enterprise architecture and are already beginning to implement the objectives of our enterprise architecture transition strategy.

The enterprise architecture will help DHS align information technology investments with its mission and business needs, help us improve data sharing and interoperability with its many information sharing partners and stakeholders that include other Federal agencies, State and local tribal governments and particularly the private sector responsible for our critical infrastructure.

In my previous testimony, I discussed the vision and strategy of DHS and how that strategy must be supported by a disciplined capital planning and investment control process that is guided by a business-driven enterprise architecture.

Our strategy identified major initiatives, such as information integration across the Federal, State and local government, private industries and citizens, common standards for electronic information sharing and integration, improved communications capability and interoperability and reliable public health information capability and sharing.

The enterprise architecture captures this strategy and describes a target information management infrastructure that will be dramatically different from the one we have today, one that will provide timely, accurate, useful, and actionable information to all individuals who require it all the time.

We have accomplished something we believe to be truly unique in the Federal Government. We have designed and delivered a comprehensive and immediately useful target enterprise architecture in less than 4 months. Our enterprise architecture is enabling us to make decisions now about our information technology investments, even as we continue the hard work of developing greater detail, reaching deeper to find more opportunities for consolidation and are beginning to develop new and improved mission support capabilities enabled by information technology.

Now I'd like to kind of take everything we've done and see if I can summarize it in easy to understand jargon in less than a couple minutes.

Mr. MURPHY. Please.

Mr. COOPER. First let me share some of the things that we found. First of all, we have inherited a ton of stuff. Most of it is categorized in some manner within the legacy organization that developed it.

At that time everything was developed for the mission and capability of that specific legacy entity. For example, legacy Customs, legacy Immigration and Naturalization Service, Federal Emergency Management Administration and so forth.

What we have to do and what we have already begun doing—and we have our first release—is to basically step back and now take a look in the context of the Department of Homeland Security, how do all the parts and pieces fit together.

The diagram that you have on your left, which isn't quite the eye test that you have on the right—and we'll get copies of these to the committee members—but on the left you effectively have a diagrammatic representation of the strategies, goals and objectives of the Department. We refer to it as our value chain, the same as you would find in any private sector corporation. It represents what we have to accomplish to secure the homeland and protect the lives and secure 286 million Americans. It's that simple.

On the right, that single diagram which we labeled a sequencing diagram effectively represents all the work that we've done in this first release. Let me try to verbally describe what you see up there. First and foremost, the value chain in that left-hand diagram is represented across the center—the rough center of the diagram left to right. So those kind of blue-turning-to-gray rectangles are the mission, goals, and objectives of the Department. I'll give you an easy example. We talk about preventing incidents, disseminating information, preparing for incidents. God forbid something should happen, we have to respond to that incident and we have to recover from that incident. At the highest level, that's the goal of the Department related to terrorism.

If we then begin to break that down, what we find is a lower-level category that aligns with that mission that we've labeled threat identification and management, to give you one example for illustrative purposes here.

Below that horizontal grouping of rectangles the little teeny tiny print that none of us can read are basically all of the projects and initiatives that we found underway in the Department at this time.

Now, what you can visually see is some of the columns have a whole bunch of projects, and some of them have very few or none. The first thing that that tells us is where we've got a whole bunch of them, they're basically in the same mission area and may provide an opportunity for integration and consolidation.

Collectively, those projects represent somewhere on the order of about $2 billion in fiscal year 2004. So we're talking a pretty sizable capital investment.

Our work then, if I continue the example of threat identification and management, I'm going to read these quickly, but you'll get the idea, OK, and some of these names you will recognize. CAPS 2, U.S. VISIT, SEVS, which is the Student Exchange and Visitor System, electronic surveillance system, FORCE, IDENT consolidated intelligence system, numerical integer intelligence system, cyber warning information, national warning system. You get the idea.

There are about 16 major initiatives in this threat identification and management column, and one of our first orders of business is to understand how do they integrate, how do they overlap, if they overlap, and what can we do to both successfully deliver the mission capability represented by these applications but at the same time be respectful of the fact they represent a huge investment of taxpayer dollars. We don't want to be wasteful. We want to ensure homeland security, and we may have opportunities to both consolidate, deliver mission-capable, deliver accurate, useful and timely information and save money. That's our objective. We repeat that across every one of those columns. There's a significant amount of work to do.

The pink stars or the lavender stars represent what we believe to be quick hits. Those are things we believe we could do very quickly, meaning within about a 6-month timeframe, to accomplish delivering mission capability, doing no harm to current mission capability in each of our inherited legacy environments, and at the same time begin some of the consolidation activity, integration activity.

At this point in time let me stop, and I think Karen and I would both be delighted to answer questions of the committee.

[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
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census

October 8, 2003

Mr. Chairman and Members of the Subcommittee:

I am pleased to appear before the Subcommittee today, and want to thank the Chairman and members of the Subcommittee for giving me the opportunity to talk about the Department of Homeland Security (DHS) Enterprise Architecture (EA) planning project. I am very pleased to announce to you that in September of this year, we completed the first version of our target EA and are already beginning to implement the objectives of our EA Transition Strategy. The EA will help DHS align Information Technology (IT) investments with its mission and business needs, and improve data sharing and interoperability with its many information sharing partners, such as other Federal agencies and State, Local, and Tribal governments.

In my previous testimony I discussed the vision and strategy of DHS and how that strategy must be supported by a disciplined capital planning and investment control process that is guided by a business-driven EA. DHS' strategy identified major initiatives such as information integration across the federal, state, and local governments, private industries, and citizens; common standards for electronic information; improved communications; and reliable public health information. The EA captures this strategy and describes a target information management infrastructure that will be dramatically different from the one we have today—one that will provide timely, accurate, useful, and actionable information to all individuals who require it.

We have accomplished something unique in Federal government: We designed and delivered a comprehensive—and immediately useful—target EA in under four months. Our EA is enabling us to make decisions about our IT investments now, even as we continue the hard work of developing greater detail, reaching deeper to find more opportunities for consolidation, and beginning to develop new and improved mission support capabilities. I would like to now provide an overview of the DHS EA and discuss how we are using our EA today, as well as how it is aligned to the Federal EA reference models and E-government initiatives.

Introduction to EA

Mission performance depends on providing operational decision makers with appropriate, accurate, and timely information upon which to base their decisions. IT is a significant contributor to providing such information. The challenge is putting in place a modern, adaptable, and interoperable set of applications to aid in improving mission performance.

Although IT cannot address all the challenges faced by DHS and its homeland security partners, alignment to business activities will improve the Department's overall ability to execute its mission.

DHS embarked on its EA planning project as a beginning point for integrating its business processes, data, application systems, and IT—to transform from an organization composed of 22 formerly separate agencies and their various assets, to an organization with a unified, interoperable infrastructure and a modern, adaptable, and interoperable set of IT applications based on the business needs of DHS.

Documenting our business and information needs through EA planning enabled us to highlight overlapping and duplicative initiatives. For example, we have identified at least eight existing initiatives supporting Port of Entry management that can be unified, leading to cost savings. We have begun identifying areas where we can leverage and reuse legacy systems. In the same Port of Entry management example, we have identified at least three existing systems that have capabilities that can be reused to meet that business need. And we have begun identifying mechanisms for sharing information not only within DHS, or even within the federal government, but also with the first responder community, and state, local, and tribal governments to support the broader homeland security enterprise.

Our EA provides the vision, concepts, and structure to enable, enhance, and increase the efficiency of DHS. I believe that it is unique in many respects. First and foremost, it is business driven; that is, it is based on the mission needs of DHS that, in turn, drive the target IT architecture. Also, the Target EA has been constructed to provide the necessary agility to enable rapid changes in response to new threats through flexible component- and service-based applications. It is based on the reuse of components to reduce the costs of IT development, and business and technology patterns to ensure repeatability of common processes.

Our DHS EA Team has produced a conceptual-level EA. It provides a high-level view—a critical beginning as our initial EA requirement was to identify and drive opportunities for consolidation and interoperability. I want to point out that even though it is conceptual, it is actionable. In fact, we are using our EA transition strategy to focus on early quick hits and development of initial component capability in FY04. The first components that we will create (whether we build new or modify existing investments) are those which are reused most frequently, and serve as foundational capabilities. We are also using our EA plan to inform our FY05 budget process and it will be even more instrumental in making IT investment decisions in the FY06 budget process.

Support for Federal Initiatives

EA is one of the means by which visibility into IT assets can enable the federal government to find business and financial efficiencies. Our alignment to the Office of Management and Budget's Federal Enterprise Architecture and our transition to e-government initiatives are discussed below.

Support for the Federal Enterprise Architecture

The Office of Management and Budget (OMB) Federal Enterprise Architecture (FEA) is an approach and framework that provides guidance to federal agencies in developing their EAs. It provides a common structure and vocabulary for federal EAs, so that they may be analyzed and compared to identify commonality and duplication across agencies. Our EA planning project was driven by the concepts and products of the OMB FEA Reference Models. We have aligned the various EA artifacts with the five FEA Reference Models: the Business Reference Model, the Data and Information Reference Model, the Service/Component Reference Model, the Technical Reference Model, and the Performance Reference Model. And, more importantly, we have embraced the two FEA foundation concepts: Line of Sight for program effectiveness and Component and Service Based Architectures for effective reuse and repeatability.

Business Reference Model. The FEA Business Reference Model drove the development of our business model. Several of the Business Reference Model Lines of Business are directly applicable to DHS (in particular, Homeland Security and Disaster Management). For all other business activities within the DHS business value chain level, there is a one-to-one link to the Business Reference Model Lines of Business. The EA Business Model includes a matrix that shows the relationship between our business activities and the Business Reference Model Sub-functions. It is important to note that every business activity in the EA Business Model is mapped to a Business Reference Model Sub-function. As a result of this alignment, OMB should be able to readily identify functional commonality of DHS with other federal agencies.

Data and Information Reference Model. The Data Reference Model consists of a layered model for decomposing collections of information, from Subject Areas down to Data Objects and their properties. We adopted this approach and classified the information required to support the homeland security business activities at the Subject Area and Data Object levels. Further decomposition and description of the data objects will be performed in the next phase of the EA process. Our Data Architecture aligns with the Data Reference Model concepts by providing a common, consistent way of categorizing and describing data to facilitate data sharing and integration.

Service Component Reference Model. The DHS EA project has fully embraced the FEA Service/Component Reference Model's component-based approach to the reuse of applications, application capabilities, components, and business services across the federal government. OMB created the Service/Component Reference Model specifically to identify service components and their relationship to the technology architectures of federal agencies. We leveraged the Service/Component Reference Model in two important manners: (1) the structure of our Application Architecture is a set of interworking components that has direct ties to the Service/Component Reference Model, and (2) our Technology Architecture applies a set of technology patterns that is derived directly from the technology aspects of the reference model.

The Application Architecture has been constructed to leverage reusable components that can be acquired once and used to provide services to many applications. It shows the structure of this component reuse. From the set of component architecture diagrams, it can be seen that there is a significant opportunity to apply this reuse concept throughout DHS (and across other government agencies). The result should be considerable cost savings, as well as greatly improved interoperability and flexibility of applications.

The Technology Patterns of our EA are repeatable solutions to recurring technical challenges. These patterns employ technologies described in the DHS Technical Reference Model (discussed below) and provide capabilities as described in the FEA Service/Component Reference Model. For example, the Business Intelligence/Data Warehouse technology pattern of our EA aligns with the Business Intelligence Service Type of the FEA reference model.

Technical Reference Model. The initial formulation of the DHS Technical Reference Model began with the taxonomy as well as the technical services, protocols, and interfaces specified in the FEA Technical Reference Model. The DHS model extends and refines the FEA model where necessary to reflect the additional functional and technology requirements of DHS. In deriving the DHS model from the FEA model, we have also made adjustments to better align the technology categories with the physical layering of services that exist in vendor and open source products. The Domain level (Tier 3) categories of the DHS model have all been mapped to the FEA model, so that comparisons can be directly made with the technical reference models from other agencies.

Performance Reference Model. Although this FEA reference model was still under development during our EA planning project, an initial attempt was made to align our Business Model with the intent of the Performance Reference Model, based on draft materials provided by OMB. Specifically, the Business Model includes a table that defines the outcomes or measurement categories and corresponding indicators (metrics) for each cross-cutting, corporate activity defined in the Homeland Security Value Chain. Measurement categories are defined for each activity in six areas: Mission and Business Results, Customer Results, and Process and Activities, People, Technology, and Other Fixed Assets. This guidance within the DHS EA will provide specific DHS IT programs with a starting point for applying the Performance Reference Model within their Exhibit 300 submissions to OMB.

Support of E-Government Initiatives

The Target EA and Transition Strategy identified several opportunities to leverage on-going e-Government initiatives. As you may be aware, the Department is currently the managing partner for the Disaster Management and Safecom e-Gov initiatives. The Department is also actively participating in six additional e-gov initiatives. For example, there are three major organizations within the department that provide grants to state, local, private industry, academia, and individuals for a variety of reasons that participate in the e-Grants effort. We will be looking more closely at this mode of delivery and how it may leveraged into the EA program.

Finally, the target EA identifies a concept for homeland security information sharing and knowledge flow - the Homeland Security Information Sharing Architecture - based on a concept of Communities of Interest adopted from the intelligence community. Information sharing with state, local, tribal, and other federal government entities is a critical function of DHS, both as a source of information and as the "first responders" to an incident. Implementation of this information sharing architecture will provide value to homeland security community by driving results and productivity through effective information sharing.

In addition to the initiatives for which DHS has the lead responsibility, we expect to be a major contributing player or user of several others. We are committed to transitioning to projects such as e-Authentication, e-Clearance, e-Payroll, e-Travel, and HR Integration. We are actively gaining more knowledge about these initiatives so that our role in supporting them and their particular timelines and capabilities can be integrated seamlessly into our target and transition strategy.

Overview of The EA Plan

Our EA consists of four parts: an "As-Is" architecture characterization, a Business Model, a Target Architecture, and a Transition Strategy for migrating from the As-Is to the Target state.

As-Is Architectural Characterization

The As-Is or baseline architectural characterization describes the DHS enterprise from an IT perspective, and provides a reference point for the development of the target EA and transition planning. The scope of the work was intended to present a high-level assessment of readily available EA-oriented information. It is neither an operational audit, nor is it intended to be a detailed inventory of activities, data entities, applications, locations, or IT elements. Further analysis and refinement is required to provide that level of detail.

The baseline characterization looked at the business activities, data, applications, and IT currently in use by legacy agencies. Also included within the characterization is a view of the DHS FY 2004 major O Ma B exhibits 300. Some high-level observations:

- The current state of DHS architectural artifacts does not lend itself to a full operational audit. Current EA artifacts were developed while organizations were part of their legacy agencies, prior to DHS' operational start in March 2003. As a result, there are inconsistencies in structure across the legacy EA artifacts that require further definition.
- Considerable overlap exists in business activities among the legacy agencies. Legacy agencies were found to have redundancies in several business activities (e.g., human resources, financial management, procurement, and some mission-specific areas).
- A standard definition of the types of high-level entities (data objects) required to support missions was not uniformly available from all legacy agencies. Data entities (such as "person") may be defined as a "baggage screener" or a "passenger screener" entering the country, whereas a "document" category may be defined as a "manifest," "permit," or "certificate."
- DHS has over 300 IT applications that are back-office in nature and perform functions such as budgeting, financial management, recruiting, and human resource management.
- DHS has in excess of 1,000 servers and 1,000 various telecommunications circuits clustered throughout the United States and international countries.
- DHS initiatives (OMB Exhibits 300) have significant overlap. Fourteen initiatives were identified, for example, that have a primary emphasis on supporting various credentialing activities.

- Thirty-four initiatives are aligned to at least one e-Government initiative or could use the new General Services Administration (GSA) Smart Buy program.
- The existing DHS Technical Reference Model (TRM) document was incomplete in that it did not adequately address how to provide a common DHS IT standards profile. It also did not give sufficient detail to allow the mapping required to respond to future OMB requirements.

Business Model

The Business Model is the foundation of the EA. It serves as the "business view" of the activities performed by the homeland security enterprise. The homeland security enterprise is defined as DHS, as well as the homeland security functions performed by other entities (state, local, and other Federal) related to securing the homeland.

The business model lists activities and describes these activities to a level of detail that permits an understanding of the data necessary to perform each activity, the system capabilities needed to perform the activities, and the IT to support the capabilities. Hence, the business model "bridges the gap" between the mission and the information systems and underlying infrastructure that support that mission. It was the foundation for the development of a business-driven target EA. The Business Model also provides a framework to identify business outcomes and performance measures and the resources necessary to achieve desired outcomes.

Our Business Model describes the mission, organizational structures, business activities, user classes, and work locations. Documenting our business activities enabled us to identify common activities that can be automated in the optimal target EA and subsequently provided to many users. It comprises several different elements:

- Value Chain. A holistic view of business activities across the enterprise, showing high-level business functions that are core to mission fulfillment and that add value to the services provided by the enterprise. The value chain cuts across organizational boundaries.
- Business Activities. Decompositions of the high-level business functions independent of the performing organization. Business activities are identified by an appropriate name, which is descriptive and conveys the meaning of the activity, and a textual definition.
- Performing Organization. The organizational entities responsible for performing business activities.
- Workplace Environments. Descriptions of the actual physical environments where activities are performed. This characterization aids in determining the potential technologies needed to support the automation of the business activity.
- Workzones. Physical, geographic locations at which an activity is performed. The four workzones are:
  - Pushed-back Border – Activities performed outside the traditional borders of the U.S. This could include activities such as pre-screening passengers or refugee processing.
  - International Space – Activities performed in traditional "international" space, also known as international waters or international air space.

  - At the Border – Activities performed at traditional U.S. borders. This would include activities such as patrolling the borders (both land and sea), performing inspections on people and goods, etc.
  - In the Interior – Activities performed within the traditional U.S. borders.
- Business Scenarios. Key value streams of activities (with clear outcomes) that demonstrate and validate the relationship between activities, the value chain, programmatic and national strategies, and performance outcomes.

Target Enterprise Architecture

The target EA comprises the data, applications, and technology architectures. Although the target will evolve over time, it has been constructed to enable quick and efficient business change by leveraging current best practices in service-oriented and component-based architectures.

To reduce cost and risk, this EA relies on state-of-the-art IT concepts focused on reusable common IT assets, repeatable patterns, and modularity. By designing reuse into the architecture, the cost of meeting new requirements will be reduced. By utilizing repeatable patterns, the risk in developing new IT assets will be minimized. This will, in turn, reduce the schedule and performance risk for IT projects. The modular concepts embedded in the architecture will allow the enterprise to be more agile in responding to change. IT applications can be assembled from a set of existing "building blocks" rather than having to be built as new large-scale IT development efforts.

Data Architecture. DHS requires an efficient means of handling data across the Department, both for normal business purposes, and to enable DHS and other entities to share timely, accurate, accessible, and reusable information. The data architecture was driven by and developed in conjunction with the Business Model, using a parallel decomposition approach. The data architecture identifies the enterprise-wide data necessary to support business activities, without regard to organizational or procedural boundaries. It focuses on answering the question: "What information is needed to accomplish this activity?" The data architecture was designed to satisfy two main objectives: to provide common vocabulary across the enterprise and to provide understanding of the fundamental (data) structure of the enterprise. It consists of a list of subject areas (with definitions), data objects (with definitions, key characteristics, and important relationships), a high-level Entity Relationship Diagram, and a data-usage matrix, referred to as the CURE Matrix.

Application Architecture. The purpose of the target application architecture was to develop an easily understood picture of the type of application systems that would satisfy the Department's business needs. The target application architecture defines the "to be built" applications and components, describing the required functions and capabilities to support business needs. It is based on commercial best practices and a new paradigm promoted by the Office of Management and Budget (OMB) and the Federal Chief Information Officer Council: Service/Component-Based Architecture.

Service/Component-Based Architecture divides the functionality of the applications into the services provided. Services, in turn, are implemented by reusable software components. Construction of applications consists of assembling components into a meaningful whole that satisfies a set of business needs. The concept of monolithic applications that provide all functionality in a particular area (of which each individual might use only a small portion) is dispensed with in favor of a flexible "virtual application" that brings together the services provided by the components that are applicable to the individual's task. An application thus becomes the software to manage the workflow associated with the particular task. This paradigm has many advantages. Among these advantages are reduced user training, easily modified applications (plug and play), reuse of components in multiple applications, and better interoperability of applications.

The target application architecture lays the foundation for defining the IT software to be built, assembled, reused, mined, and acquired to provide the tools to conduct normal business operations. It was based upon the activities defined in the business model and data objects defined in the data architecture. It is a notional architecture, meaning it does not attempt to define in detail each application that will be required by the enterprise. Instead, it defines the types of application groups that will be required and the types of software components that each application group will consume.

Technology Architecture. The target technology architecture assists those responsible for delivering and maintaining business systems. It defines the platform upon which all DHS assets will operate. Providing a common platform is critical to achieving the objectives that caused the Department to be created (e.g., information sharing, interoperability, effective communication, etc.). The target technology architecture consists of technology principles; a set of technology patterns; a technical reference model (TRM); and a Standards Profile. The technology patterns are implemented using technology categories that are defined in the TRM. The Standards Profile identifies the acceptable standards, protocols, and products for the categories in the TRM.

Patterns represent industry-accepted solutions to repetitive problems or issues facing IT. The focus of the EA is on architecture-level patterns. A set of drivers (requirements or features) is applied to the applications to allow a mapping of the applications and components to appropriate technology patterns. Technology categories are then applied to the patterns. This provides the basis for developing the Standards Profile for those categories implied by the patterns.

The DHS TRM describes the technology platform upon which the application and other architectures rest. It provides a common conceptual framework that assists in coordinating the acquisition, development, operation, and capitalization of IT assets. It provides a common structure and vocabulary for describing DHS IT at all organizational levels and in all environments. The TRM establishes the basic guidance necessary to ensure that proposed IT solutions are compliant with the intent of the EA. Finally, the TRM includes communication and interoperability categories that provide the technical basis for interfacing with state, local, and other government agencies. The goals of the TRM and DHS standards profile are as follows:

- Promote vendor independence through the use of standards-based products and interchangeable services and components.

- Improve interoperability, reuse, and information sharing across operational entities.
- Improve operational effectiveness and efficiency through the use of common concepts and tools.
- Improve security through the identification of common security services and standards.
- Improve development and integration efficiency and responsiveness through the identification of a common infrastructure for applications.
- Improve development and integration quality through implementation of a Department-wide systems assurance program.

Information Sharing Architecture. One of the fundamental drivers in the establishment of DHS was the need to share information in a timely manner among the intelligence, law enforcement, emergency management, responder, and other communities. DHS has requirements to share and access information at many different levels. Above all, it needs the capability to provide data to all users that have a need for it—to exchange that data with other Federal agencies (horizontal sharing), and with state, local, private sector, and tribal governments (vertical sharing), as well as with foreign governments. Information sharing, whether horizontal or vertical, generally refers to the ability to access and share critical information with key business partners. The information sharing architectural description within the target describes the most common models for information sharing: push, pull, query/response, and publish/subscribe. Depending on the type of information, its urgency, the consumer, and the available technology, DHS may rely on any or all of these models.

Transition Strategy

While our first step in meeting the challenges that face IT in helping the Department meet its mission and objectives has been accomplished—producing a business-driven Target EA—the second step is actually implementing that target. Our Transition Strategy guides us as we make decisions about our current environment so that we can, project by project, realize the target. The strategy identifies objectives that will be met through the implementation of conceptual projects. Those objectives are to unify the DHS infrastructure, address immediate critical mission needs, address mandated project dates, optimize corporate solutions, and provide new and improved mission capabilities.

Taken together, the target EA and transition strategy describe an IT environment that is vastly different from the one that exists today, an IT environment that:

- Captures data at its source, avoiding costly multiple data capture.
- Allows data access by multiple applications, so that data once collected is available to all decision makers.
- Leverages information sources that decision makers might not normally have had access to.

The EA also contributes to improved data sharing capabilities. It helps us identify the data requirements of each business activity and for each relevant stakeholder. Through the EA planning process it is possible to identify where data actually resides, who uses the data, where the data is used, and when the data must be available. The result is enhanced sharing capabilities by virtue of developing IT systems that collect data necessary to support business activities only once, but make the data available many times over to support other homeland security business activities.

The relevance of the our Transition Strategy is that we are using it today, right now, to make decisions about our IT investments. The strategy guides us as we decide to initiate new projects, modify existing applications, consolidate many investments into fewer, build new capabilities, then field improved information systems, or deploy enabling technology infrastructure to better support mission performance. The most immediate impact of the Transition Strategy is its use in deciding what projects to initiate or continue in FY04, most significantly which existing investments must be considered for consolidation to better align existing resources to new mission requirements, and save significant resources—financial and human—with the elimination of redundant investments. Each conceptual project in our Strategy identifies existing investments that are consuming financial and human resources today that will be considered for consolidation or elimination as the capability to meet that business need is designed, built, and fielded.

Our Transition Strategy is the foundation of a more detailed transition plan that will identify more concrete steps for moving to the target EA. As we refine our target and the transition strategy itself, we will have a more significant impact on the budget formulation processes and the requests we make for IT investments for FY06 and beyond.

Challenges

It would be easy to rest on the laurels of what we've accomplished in such a short period of time. It was a Herculean effort accomplished in a very short period of time and has resulted in an actionable strategy for moving forward. In reality, however, we have only just begun the journey to get from where we are today to where we need to be tomorrow and into the future.

DHS faces a number of challenges in building upon the success of our initial EA effort. First, we need to move DHS culture closer to a "One DHS / One Enterprise Architecture" culture and further away from "stove piped" legacy thinking by further engaging our business units in the maturation of this EA. Second, as we begin to implement the target EA, we need to re-orient and potentially redirect some current IT investments. This will be a challenge as we move from a culture of "ownership" to one of "stewardship" that requires business users to share and re-use IT assets to the maximum extent practicable. Third, as we re-engineer our business processes, we need to better align our capital assets (human, real, IT) to meet the needs of those improved processes. Finally, we need to implement and embrace a disciplined, enterprise-wide architecture governance process. This process will lead to optimal IT investment decisions across the DHS enterprise and successful IT implementations. I am confidant that as we move forward, and with your guidance and assistance, we can overcome these challenges, and in the process, become a model organization for business and IT transformation.

Finally, EA planning is being performed at the Department level. This approach will facilitate the optimal use of IT resources by applying common architecture principles and establishing a common architectural framework to ensure uniformity and standardization when migrating and integrating IT investments. A collaborative approach will ensure that overlapping business processes and data needs are identified, and that applications and IT supporting those applications will not duplicate each other. It will also ensure that the EA addresses the unique aspects and business missions of each of those organizations. Our challenge is that it requires significant input, dedication of resources, and the close collaboration of the DHS Directorates and organizational elements to develop a single DHS-wide EA. Concurrently, many of the legacy agencies now within DHS have conducted EA planning projects and are maintaining mature EA support structures. We must find the right balance between leveraging what we have, and creating a new, single, DHS-wide framework.

Next Steps

While the development of our EA plan is an important first step, it is just that, a first step. The value of an EA is in its ability to improve IT investments and resources management in a manner that advances DHS mission performance in both the short and long term. In the near term:

- **We are using the results of our EA effort today to support our immediate investment decisions.** We are doing this by aligning and integrating our current investments to leverage our investment review process to ensure solid enterprise architecture-based justifications for our investments.
- We will begin implementing **"quick hit"** items – beneficial modest scale investments that will quickly deliver needed capabilities consistent with the target architecture.
- We are evaluating existing programs against the EA and consolidating investments where there are **areas of overlap and duplication**.

As we start the hard work of evolving our EA architecture beyond the conceptual level, we will begin to make direct links between specific detailed target architecture elements and specific IT projects. This will also allow us to mature the transition strategy into a detailed, specific project plan for evolving to the target architecture. In addition, we will begin to put in place the necessary processes to ensure that business and technology strategies and investments remain aligned over time to meet DHS' mission priorities. These specific next steps will ensure that we continue along our EA based roadmap and that we are ultimately successful in transforming DHS to optimally meet our critical mission.

Thank you, Mr. Chairman, for this opportunity to discuss the DHS EA.

Attachment A
DHS Enterprise Architecture Participants and Support Contractors

DHS Headquarters
George Brundage, Catherine Santana, Charles Thomas, Amy Wheelock, Ron Williams

Border and Transportation Security Directorate
Bureau of Immigration and Customs Enforcement
Glenn Norton, Paul Rosenberg Mike Nicholson

Bureau of Customs and Border Protection
Rick Alcocer, Phil Cullens, James Jeffers, Shenell Jennings, Brian Nicholas, Will Peters, Brenda Stealing, William Tyree

Federal Law Enforcement Training Center
Robert Crouch, William Dooley, Ned Futoran, Sandra Peavy

Transportation Security Administration
Mark Emery, Jonathan Houk

Bureau of Citizenship and Immigration Services
Patty Cogswell

Emergency Preparedness and Response Directorate
Tom Brace, Jack Fox

Information Assurance and Infrastructure Production Directorate
Tim Daniel, Keith Herrington

Science and Technology Directorate
Parney Albright, David Boyd, Maureen McCarthy, Robert Shepherd

United States Coast Guard
Bradford Eyre, Jack Green, Ron Hewitt, David McLeish

United States Secret Service
William Cachinero, Ken Gunderson, John Gutsmiedi, Gregg James, Damian Kokinda, Greg Lydon, Doug Schraeder

DHS Enterprise Architecture Support Team
Science Applications International Corporation (SAIC)
High Performance Technologies, Inc. (HPTi)
Everware

Mr. MURPHY. Thank you both for your testimony. This shows a very complex system that needs to be smoothly integrated, because where there's all that complexity, there's also a lot of places that there are chinks in the armor, so to speak, that we make sure we resolve so no one sees those as vulnerable positions.

Mr. Cooper, let me begin by questioning you at the bottom line. How will the enterprise architecture that you discuss contribute to the achievement of the overall mission of the Department of Homeland Security?

Mr. COOPER. First and foremost, as I mentioned, the enterprise architecture captures and represents all of our mission capability. One of the first things that we recognize is that we have to basically understand what we have today before we can add new mission capability from an information technology enablement perspective.

So the first immediate value is we know what we have, we know what we need to rationalize and stabilize from an infrastructure perspective, meaning we've got to have a stable platform before we can launch new capability. From that stable platform, which we anticipate will probably take us about 12 to 24 months, the good news is that we deliver value along the way, so it's not an all-or-nothing proposition, but it will take us about 12 to 24 months to completely stabilize our infrastructure.

We then can launch new mission capability along the way, but we can rapidly speed up, we can make wiser investments of how we want to achieve new capability. We can understand where we are lacking support for some of our mission capability. We can identify that immediately, as I mentioned, by showing basically the white space in our enterprise architecture.

Mr. MURPHY. As a followup there, when you talk about things you can do within the first 6 months, are those things you can do within the first 6 months because they are relatively more simple to change or because those are high priorities?

Mr. COOPER. Both.

Mr. MURPHY. Let me followup by asking you to describe for this subcommittee how a comprehensive architecture will produce a Department that is more efficient, productive and cost effective. I think you're talking about $2 billion worth of programs here.

Mr. COOPER. Exactly. You had already mentioned in fact in your opening remarks that we've identified, for example, over 300 information technology solutions and applications that are what we call back-office in nature. They represent the functions around human resources, finance, budgeting, procurement acquisition capability.

While I can't argue that necessarily one or two is the right answer, I can tell you 300 is not the right answer. All right.

So one of the things that we can immediately do, and we have now identified these, we can immediately begin to stop or not continue some of the redundant applications, guided by the principle of doing no harm. We need to make informed decisions about where we stop, and we will do that. We'll do it conjoint with OMB. We'll do it with this committee and with Congress as appropriate. But we can begin to move from many, in this case 300, down to some sizable, manageable number. That enables us to take the savings that we will achieve in this integration and consolidation and apply that to other areas of need. The idea would be hopefully that our efforts do not cost additional money, but rather we are able to redirect where we invest.

Mr. MURPHY. Let me followup with that. You're going to integrate 22 agencies through all this. So I mean, what is the real effect going to be on DHS in accomplishing its overall mission of utilizing your enterprise architecture here, getting these 22 agencies together?

Mr. COOPER. Let me give a couple more specific examples in the mission area. The principle that we're after is basically to simplify our environment. OK. We want to make things less complex, but at the same time deliver mission capability.

In the mission space we've already identified areas of opportunity. One I shared with you around threat identification and management. Another one that we've begun to do work in is identity credentialing. We have several applications underway that deal with the identification of people and how they are documented, how that documentation is then authenticated.

By first identifying all these different initiatives, we can take a look at where they overlap, we can begin to bring multiple project teams that began in their legacy environments, meaning the Coast Guard had different initiatives underway, the Secret Service had different initiatives underway, legacy Customs, legacy INS, all had appropriate to their mission initiatives underway. By bringing those teams together and by having them work with one another, we accomplish a couple very important things.

First of all, we rapidly integrate the actual functionality to deliver mission capability of the Department. We now have people with expert skills in this area or other areas working so that we speed up the process by which 190,000 people begin to know who to talk to and who to collaborate with inside the Department. Extremely important and extremely valuable for us to do that as quickly as we can.

The second thing, we begin to leverage that expertise. Each one of those experts brings their expertise and their perspective from the objective that they previously operated in, their previous operating environment. By sharing we benefit as a Department because now we have a broader perspective.

The United States benefits because we now are bringing many experts to bear on common problems, and we can do it faster. Hopefully we can do it less expensively, and we can achieve a result that is basically greater than the sum of the parts.

Collaboration, knowledge management, identity credentialing, intelligence information, integrated case management are all other examples of areas of activity that we're bringing collective project teams and initiatives together.

Mr. MURPHY. You were talking about the legacy and what appears to be redundancy, but are these functions that different from one another, or are they going to want to preserve some of their turf on how they handle this?

Mr. COOPER. Well, let me answer in two parts. First of all, from a process and functionality standpoint, there is overlap. Let's take something like the identification of people who might be a threat to the United States. We can do the same thing with the identification of cargo, in tracking cargo before it reaches our ports of entry. Secretary Ridge has announced that is our Smart Border Initiative.

In both of those cases there clearly are aspects of each of those processes that we want to retain within the inherited legacy environment, but there are also aspects that we absolutely want to share.

Now, the second part of the question about are there cultural objectives to overcome, candidly I would tell you, yes, there are. We have some parts of the Department that have a 200-year-plus very rich history and legacy of tradition and honor and service to America. We don't want to do away with that. We don't want it to disappear. This is about change. This is about organizational change. This is about people understanding how do I continue to have a valued role in a new working environment, which is now the Department of Homeland Security. That's tough. It requires each of the individuals involved to understand how they have to contribute in a new role. It does require some very hard work with regard to organizational entities and how those entities cooperate and work together.

Mr. MURPHY. So how confident are you that the content of this whole EA program has sufficient depth and scope to address the intended purposes here?

Mr. COOPER. At the moment it does not have sufficient depth. What we explained and what I shared in my testimony back in the April timeframe was that we will continue—this is a living, breathing type of initiative. It's dynamic. We will continue, and have already begun on effective release of two of our enterprise architecture. That is, to continue the work that has begun and now push it both down in level of detail and fill in some of the gaps, some of the white space that you see that we weren't able to address adequately in our initial 4 months.

I am very confident that the process of enterprise architecture as defined by OMB and as now applied by DHS will deliver all of the level of detail granularity, understanding, business goals, business-driven linkage that we will need. It will take us a little bit more time to fully populate the enterprise architecture, but the important message is we are using our enterprise architecture now to make decisions about IT investment. We will continue to do that, as it becomes more robust.

Mr. MURPHY. Ms. Evans, I know it's Wednesday and you pretty much have to grasp the entire program you've inherited Monday, but actually I wonder if you could also comment on OMB's perception of this. How and when do you think you'll have a grasp of the sufficient scope and depth of this EA program from OMB's perspective?

Ms. EVANS. Well, the only perspective—and a preliminary review of the Department of Homeland Security's EA efforts, we believe is really very encouraging. We are pleased that they have identified a current state enterprise architecture as well as a target state and a transition plan. We are also very encouraged with the clear linkage that they have to the Federal Enterprise Architecture efforts as well as their commitment to a component-based approach for application and integration.

What we will be evaluating as we go forward are the investment decisions that they are now making, and it will be reflected in the President's budget for the fiscal year 2005 budget.

Mr. MURPHY. One thing that certainly struck us with this new Department is it's not the same kind of discussions held back in the 1790's when forming departments to begin with, but part of where we are now is we're looking at evaluation metrics and how one will put some things in place to evaluate what is going on.

Mr. Cooper, what is being put in place?

Mr. COOPER. We use two high-level metrics, kind of from the startup of the Department, because obviously we hadn't had a chance to get together. We hadn't had a chance to get guidance from the Secretary and business leadership yet, but we immediately put two metrics in place. One was speed to market or cycle time. OK. We set that as a metric, because we felt that it held value almost across every business process of the Department. If there are activities that we can do, if we can take out nonvalue-added work in our business processes to reduce the time, for example, that critical information, homeland security-sensitive information gets from its source to sworn law enforcement officers as an example, then in fact we are moving to increase the security of the United States.

The second metric that we have applied thus far is the quality of the information that's used wherever it's used throughout the Department. By focusing on cycle time, speed, and quality of information——

Mr. MURPHY. Those are the metrics you're using?

Mr. COOPER. Those are the two metrics that we're using right now, OK. We felt that immediately added value. What we intend to do and what we've begun now, as we now continue the in-depth work and based upon the data that we've gathered thus far, we now can begin to actually attach specific performance metrics to each of the mission areas of the Department.

So, for example, if we look at the cargo area, we can actually now begin to use the information gathered to determine an easy one: how many containers that we believe might hold risk are inspected. OK. Today that percentage is not very high. It isn't that we want to move to 100 percent inspection, but we want to move to 100 percent of those where we believe there is sufficient risk or the informed information we have leads us to believe that we ought to inspect that container.

Mr. MURPHY. Are you talking about imported containers?

Mr. COOPER. Yes. In that example, imported containers.

Mr. MURPHY. But what about packages shipped within this country as well?

Mr. COOPER. Again, as appropriate, what we would want to do is use the enterprise architecture information that we gather—remember, the information is gathered from subject matter experts in all of our business areas. This isn't an IT activity, an information technology activity. It's a business-driven activity. So by participation of the business experts in each of the component areas, they are the folks who then in a facilitated manner can determine here are the performance metrics that we want to use.

One of the questions that we have in the Department that we're working toward is how do you measure the success of the Department—is it as simple as no terrorist incidents, or is it more complex—so that we understand kind of the correlation and cause effect of the activities taken by the Department to prevent any type of incident. We believe it's the latter.

Mr. MURPHY. Are you working with private business in the same aspect too? Are we talking about just intragovernment agencies here? You talked about 22 agencies. Let's look at packaging from the shipping companies from the Postal Service, UPS, FedEx, coordinating with those efforts as well.

Mr. COOPER. Absolutely. Now, in that particular example that you gave, we have a major initiative underway that you may be aware of called ACE. If I translate the acronym, it's basically the former Customs modernization effort which is now Customs and Border Protection. That initiative we are working directly with private industry. In fact, there is a supporting network, the trade support network, that is comprised—I believe its membership at any given point in time represents about 150 private sector entities and associations. They actually work directly with Customs and Border Protection to determine requirements, and those requirements then move through a release management process. They are vetted both internally by the Department and with our industry partners to determine the priority, the sequencing, cost, business advantage, that type of thing, such that they then drive additional capability that appear in subsequent releases in our modernization effort.

We are doing a similar type of thing in many areas of the Department. We recognize the responsibility that the Department has to both partner with and draw upon the private sector, for we view them as stakeholders, we view them as customers, we also view them as important suppliers of a lot of the solution sets that we need to put in place.

Mr. MURPHY. For both of you, can you give some immediate uses, benefits? And when can we expect to see some concrete results as a result of this whole transition?

Ms. EVANS. As it relates to DHS, this particular effort?

Mr. COOPER. Oh, I shouldn't have put you on the spot, should I?

Ms. EVANS. That's OK. I would like to say that as I move forward, given that this is my 3rd day, the way that we're moving forward with this so that you can—and I'd like to come and really speak more specifically to this—is that we intend to evaluate DHS going forward through the budget process and ensure that they continue on that progress through the score card initiative that OMB has, the President's management agenda score card. But we're working with DHS, just as we work with all the agencies, so that they really can realize the potentials and the results of their efforts as they move forward and make those decisions using the enterprise architecture.

Mr. COOPER. Let me give you one example that's not quite as glamorous, that's not quite as sexy as some of the things that we get involved in, but it's critically important, and it deals with records management and document management. OK. One of the things that we have recognized—and with headquarters when we stood up a new headquarters, there was nothing, there was no legacy anything that we inherited. Our enterprise architecture helped us identify existing records management capability, existing document capability that we could immediately draw upon and begin to apply at the headquarters level. So while not very glamorous, it's a very real example where rather than going out and reinventing the wheel and rather than reaching out and saying, oh, we have this need in a vacuum, we'll just go ahead and move forward in this direction, we actually use the enterprise architecture to draw upon expertise and understanding what we already had available inside the Department.

Mr. MURPHY. I yield to Mr. Clay for some questions.

Mr. CLAY. Thank you, Mr. Chairman.

Mr. Cooper, this enterprise architecture document is quite lengthy. At the same time it does not address what many experts say is the most important variable in any merger: agency culture. The culture at the Secret Service and in the former Federal Emergency Management Agency could hardly be more different. How will you address these cultural differences in implementing this enterprise architecture plan?

Mr. COOPER. One of the things the Secretary has clearly stated is that we want to respect and retain the cultures and the traditions of the entities that now comprise the Department of Homeland Security. The value of our enterprise architecture in one sense is that it actually is an objective way to take some of the emotion out of some of the cultural aspects of how we come at things. Each of us brings our own perspective to bear on any type of problem or any type of challenge that all of us face in our professional careers or within our roles and responsibilities.

The enterprise architecture being devoid of a motion actually can objectively document here's the process that we are trying to deal with or trying to automate or trying to improve. Everybody can see it. Everybody can see themselves and their perspective in our documentation of that process.

Second, we clearly document this is the information that is needed, both as input to that process and perhaps produced by any particular process within the Department. All right. We can agree factually on what information is needed, what information comes out, what information flows through the process, who needs to receive that information, when do they need to receive it, in what form do they need to receive it. All right.

By kind of breaking this down step by step, we don't eliminate or negate culture, but we allow all of us to have a common frame of reference with which we can bring the best that all of us have to bear on the appropriate problem.

We then can step back and again in the same objective manner collectively reach consensus around, now, how do we want to automate the process and the delivery of information.

Mr. CLAY. All right. And in practice that's working.

Mr. COOPER. In practice we're underway.

Mr. CLAY. Let me ask you, it's my understanding that this is just version 1 of the architecture and that you expect to develop subsequent versions in the future. What does this version represent, and what will it allow you to do?

Mr. COOPER. OK. This version represents—think of it this way. We're starting top down, meaning we started with the National Strategy for Homeland Security. It's pretty high level. It's a pretty macrotype of strategy. We're trying now to push the level of detail down in terms of functional responsibility, in terms of business processes that carry out the mission, in terms of the information that supports all of these business processes; but I've given some very real examples that we have begun to identify even in this first release. So there are things that we can do, documentation management being one. OK. Those little pink stars, which even I admit I can't read from here at the table, but if I got up and ran around there, so those pink stars represent about a dozen very real opportunities that we can act on right now.

Now, the banding which most of you can see, the darker blue at the bottom, represents about a 6 to 12-month timeframe. That lighter green as you move up the chart represents about a year to 2 years, and then that lightest color at the very top represents about a 2-plus-year timeframe. OK. And you'll see those little colored boxes out there.

So even in this first pass, even in just the 4 months of work, we actually have begun a roadmap that says here are the things that we can do in each of these timeframes to add real value in the respective timeframes.

Mr. CLAY. What will—that takes me to the next question. What will version 2 add to this architecture? When will we see it, and what will version 2 allow you to do that cannot be done within this version?

Mr. COOPER. OK. What we don't have here is all of the level of detail about how the processes actually operate and some of the lower level details, meaning some of the activities and tasks of how the processes are actually carried out. That will come in subsequent releases, meaning we'll continue to populate, we'll add more detail.

That work becomes more tedious, it's a little bit more time-consuming, so we don't—the first 4 months we kind of—think of it this way. We went kind of about an inch deep and a mile wide. All right. Now subsequent releases, we start going deeper and deeper and deeper. So the breadth of each release may be less, but it's greater detail. That enables us to actually understand in more detail and make more definitive decisions about how information actually fits together; where, for example, might we source once in the entire Department information about employees for human resources purposes, information about cargo for use by all business processes that must use cargo information. OK. Visa information, for example, we might with this additional detail—we could determine how do we source it once, meaning capture it once, reuse it many times across the Department.

Mr. CLAY. Thank you for your response.

Ms. Evans, one of your stellar achievements at the Department of Energy was the contract with Oracle that incorporated security into the software contract. I'm interested to learn of your plans to expand this program. Do you expect this to become a feature of the Smart Buy Program?

Ms. EVANS. First, I'm very proud to speak about that particular effort at energy. What we really did was leverage our business requirements and work that into the contract so that we could ensure that what we needed to do at the Department really move forward to ensure our cyber posture. It is my intention to bring that feature where it is applicable to the smart buy activities. It was applicable in this particular case given this type of software and the applications that the Department was doing to incorporate that into the contract. Not necessarily all efforts that will be going through the smart buy would necessarily need to have that type of feature, but it is my intention to ensure that feature in support of the national cyber security strategy is incorporated into the smart buy activity.

Mr. CLAY. Wonderful. Wonderful. Let me also ask you, as the Federal CIO you face many of the same problems that Mr. Cooper faces, but your job of defining a common mission is even greater than that faced by Mr. Cooper. Creating common enterprise architectures across the Federal Government is a formidable task.

Do you have any recommendation for Mr. Cooper as he tackles this task at the Homeland Security Department?

Ms. EVANS. And that is the big question.

Mr. CLAY. I realize you're new here but——

Ms. EVANS. That's OK, and actually I really believe that as my esteemed colleague moves forward and as I move forward with my role changing, that the enterprise architecture—and you really did hit on the issue, which is it really does facilitate communications on all levels throughout all management in government, and that this effort really is about leadership with partnership. And so I really am approaching this going forward as it's a partnership between the agencies, with Congress, with private industry, State and local government, and so that we can provide that so that the result of the architecture efforts and the resulting investment decisions will really benefit the country as a whole. And I make that recommendation to Mr. Cooper as I do all my fellow CIOs.

Mr. CLAY. Thank you for that response.

And thank you, Mr. Chairman, and so good to see you.

Mr. PUTNAM [presiding]. Thank you, sir. It is good to be here. The airline gods have been working against me all day. Got a baby due at home and fog at National Airport. So between that I have been to Richmond and back and refueled and all that fun stuff.

And I want to apologize to the two of you for being late. I am glad we are able to move forward.

Ms. Evans, I want to take the opportunity to welcome you to your new position and thank you for your time and attention to this subcommittee. Your predecessor, Mr. Forman, was a frequent flyer with our subcommittee, and we have reason to believe that you will be as open and accessible and available as he was; and we are delighted to see you in that role and look forward to working with you in the future.

And, Mr. Cooper, we don't envy the position you have of assimilating all of the different systems and agencies and cultures that you face. And we look forward to being partners in that effort to bring about the change that I think everyone in Congress envisioned when supporting the creation of the new department, and work together to make that a seamless transition for the best interests of homeland security and the taxpayer.

If I may, I will continue with some of the questioning that Mr. Clay and Mr. Murphy have begun. Ms. Evans, I am curious how OMB, how aggressively you intend to enforce compliance with the Federal Enterprise Architecture. That is an area that certainly is a responsibility that is on your shoulders. And some is on Congress' shoulders to stand by this and be tough, but I would like to hear your thoughts on your ways to enforce compliance.

Ms. EVANS. Well, it is the intention of OMB and through the budget guidance that was issued this year to the agencies to align their architecture efforts with the FEA. That is our intention through the management processes and the budget processes that exist that we will assist the departments in ensuring that alignment is there and that the architecture is used for business investment decisions.

Mr. PUTNAM. Have any discussions taken place within the agency about holding up spending and working with the appropriators to make sure that is not bypassed?

Ms. EVANS. Since this is my 3rd day, I would like to take that one back to find out specifically what the details are. Because I do know there are ongoing efforts within OMB, but I would like to get back to you about exploring that opportunity of how we can partner and be able to ensure that these investments, especially where DHS is concerned, are made wisely.

Mr. PUTNAM. I appreciate that, and that is a discussion we need to have because it is important that somebody be the bad cop; and it's important that the communication take place with Congress to make sure there is not an end run, and we don't undermine your efforts on one hand or allow somebody to back-door those efforts. And I'll take that answer as the answer to my next question also, which was, how are we going to incorporate each individual agency's enterprise architecture into the overall plan and link that into their IT budget submissions?

So if you would like to elaborate on that, you can.

Ms. EVANS. Primarily, it will be using the existing processes that are in place by managing the management processes we have in place and the budget process. Progress guidance and—is issued through the budget process. However, ensuring that progress is made is happening through the quarterly scorecard reviews that each agency has through the President's management agenda, more specifically the expanding E-Government Initiative. There are specific milestones that we do work with each agency to ensure that they make that progress and that they are aligned.

Mr. PUTNAM. Well, it is important to make sure that the existing management processes are enforced, but I think personally, based on the information we've collected from previous hearings, that there may be additional processes required, because there have been some breakdowns in the current processes that didn't work. If you look at the smart card programs or some of the other things that we are trying to tear down, stovepipes on the left hand, and the right hand is building them back up. And that's a discussion that will be ongoing, without a doubt.

In July, we held a hearing to review the efficiencies associated with consolidating and integrating the functional business systems, particularly HR, finance data, criminal investigations and so forth. And you have mentioned, each of you, in your testimony some quick-hit IT investments that you plan to pursue.

Could you expand on that? And I will begin with Mr. Cooper.

Mr. COOPER. We can. One of the things that our enterprise architecture, even our early work in this Release 1, helped us to begin to understand was that in some critical mission areas—and I mentioned this before you joined us, so let me quickly repeat these key category areas.

These are labels. These are just working labels inside the Department that help us categorize things, but we talked about a family of applications related to identity credentialing. We talked about a family of applications and issues relating to risk and threat assessment.

Another family related to intelligence information: how we gather and produce information, intelligence products, use them within the Department, move appropriate level of secure, classified and unclassified information out to the various stakeholders and constituents that need that information; integrated case management, collaboration, knowledge management, information presentation, data visualization, those types of things.

Those are all families we identified as areas of opportunity for consolidation, potential areas, OK? We are not automatically saying that everything becomes one, but by using our enterprise architecture and linking it to our investment process, we were able this year, even in the short period of time of the standard for the Department, we have actually written and submitted to OMB consolidated exhibit 300's.

Rather than having, for example, 20-some independent projects and/or applications move forward, each with its own business case and justification to OMB, we wrapped them together and said, wait a minute, these are all the same family; let's write a consolidated business case, let OMB know that our intention is not to violate any rules or regulations or laws or anything, but our intention is to look at these holistically and ask OMB, help us do this. OK?

The same request would come to this committee and to the appropriate committees of Congress to say, hey, look, allow us the opportunity to take this type of look.

One of the challenges in doing this is that many of the initiatives that are under way are—the funding is appropriated independently. So we need to cooperate, we need to collaborate to do the right thing. It's going to take all of us working together to appropriately integrate and consolidate.

Mr. PUTNAM. But before we go to Ms. Evans on that, do you have the flexibility that you need? In a herd of horses, DHS is clearly a zebra. I mean, you are a new creature, recently developed by the Congress, trying to amalgamate all these different agencies, different systems, different legacy systems, different HR systems, different applications.

Do you have the ability in the existing statutory framework and OMB or internal executive branch framework to do the things you need to do, to move people around, move resources around to assimilate those systems?

Mr. COOPER. Thus far, I believe we do. Understand, of course, we're doing it as I give you the answer, and we are continuing to learn.

I think what we would ask, certainly, is if you'll allow us a little bit of continued learning time. We believe that we have all of the appropriate statutory authority necessary to accomplish the mission, goals and objectives of the Department. If you'll allow us a little bit more learning time as we apply them because, remember, this is now the first full fiscal year that we have headed in as a department. It's the first fiscal year we have had a little bit of input into a full budget process, if you will, and even that was kind of constrained and allow us to come back and offer guidance from that learning over the next several months, I think that might be more helpful. But thus far, we believe we are under way and we believe we may be able to accomplish everything we need to accomplish thus far.

Mr. PUTNAM. That's certainly a reasonable request, but just understand that you're operating on a narrow margin, considering the nature of your mission and Congress' very strong desire to see a seamless transition that is as short as possible with everybody pulling in the same direction. And from the IT side, there's probably an awful lot of people in the government who would like to see you fail to amalgamate all these systems and that you'll eliminate all of their excuses for not being able to do it. Because if DHS can pull it off, there's no reason why everybody can't really make this thing work.

Ms. Evans.

Ms. EVANS. My predecessor did previously brief on lines of business opportunities. And so, as you asked about some quick hits in there, the work continued on the lines of business analysis, and it continues on for four specific lines of business, which is criminal investigations, public health, financial management and human resources. The one quick hit that was identified through the analysis dealt with data statistics, and that effort has moved over to the Smart Buy Initiative, where it was identified we could truly leverage the buying power of our agencies that are involved in statistical analysis and move forward to get a quick hit as far as realizing benefits of purchasing statistical packages for those groups.

As far as the other four initiatives, I'd be happy to followup with the committee and provide additional detail on the current status as it moves through and completes through the budget process this year.

Mr. PUTNAM. That would be very helpful.

You're probably familiar that I sent a letter to GSA about an opportunity to realize some immediate savings in the relicensure of software. Could you give us a status report on where that is?

Ms. EVANS. We are currently, based on the letter that you sent, relooking at the opportunities so we can move forward; and I am in the process right now of looking at opportunities that GSA has provided in response to your letter. And, again, I would be glad to come back and talk to you in further detail about what actions will be taken so we can realize the benefits of the Smart Buy program.

Mr. PUTNAM. Absolutely. I think it has tremendous potential.

Mr. Cooper, who is the person in the Department actually responsible for holding the business owners accountable for implementing the business transaction strategy?

Mr. COOPER. I think it is a shared responsibility. I have direct responsibility for ensuring that we develop and use departmental enterprise architecture. I need help, quite candidly, from all of the senior leadership of the Department. The enterprise architecture, as I stated previously, is not an information technology initiative, it is a business initiative; and therefore, I need the help and support of the Secretary, the Under Secretaries, the appropriate agency and bureau heads in order for all of us to be successful in this endeavor. But I am the person who is held accountable.

Mr. PUTNAM. Ms. Evans, coming from the Department of Energy, the last zebra to lose its stripes, what lessons learned from DOE can be applied to the newest department in government?

Ms. EVANS. There are a lot of opportunities in that I think that the management team and the partnership moving forward is really key. And based on my new role, I know DHS is committed to the mission overall. The enterprise architecture was truly an effort that we really used.

Again, it is leadership with partnership. It's not necessarily leadership through ownership of any of these types of things, but it is really leadership through partnership. As you use the enterprise architecture and you move through the steps, it really does, as my esteemed colleague pointed out, remove the emotion from the situation where people really are committed to making good sound investment business decisions and ensuring that the dollars are invested wisely; and the architecture provides a method for that communication to occur.

That really is what happened within the Department, and I would say that I had a wonderful Secretary and Deputy Secretary who were committed to the President's management agenda and really realizing the full benefits of what can be achieved through proper, sound information technology investments.

Mr. PUTNAM. Mr. Cooper, how often do the highest level IT persons in each of the 20-some-odd agencies that have merged into DHS get together and swap ideas and communicate?

Mr. COOPER. We do that formally on a weekly basis. I established the Department of Homeland Security CIO Council almost a year ago, even before the Department was established, even though it wasn't called the DHS Security Council at the time. We have been meeting on a weekly basis for that period of time.

That council is comprised of the CIOs of each of the component agencies that came into the Department where there was a named CIO. We didn't exclude anybody—small, large didn't matter; everybody is a member. We have augmented that with some additional key senior leadership in IT.

We use that group in a couple of different ways. First of all, we absolutely meet to share. Our whole goal is to create a single information technology-coordinated function in support of the mission of the Department of Homeland Security, and I'd argue that we are, in fact, well under way in achieving that type of goal and collaboration.

Second, that same council, reconvened in a formal manner, becomes the first-level review process of our capital planning and investment review process for the Department. So for all information technology investments, we're the first step. So that initiative will come before us and we meet then as the enterprise architecture board, same membership, to pass and enforce compliance with the enterprise architecture.

Mr. PUTNAM. As you know, this subcommittee has done an awful lot on cyber security. If you would, please comment on how security is addressed in DHS-EA.

Mr. COOPER. You'll actually see it. If you get up close enough to this thing, you will see the appropriate parts of the information security.

But in addition to evolving it as an integral part of all appropriate business processes, particularly with regard to our classified host of processes and information, we have a formal information security program headed by our chief information security officer, Robert West, inside the Department. He has already established an information security advisory board that is comprised of the information system security officers and information security managers of every component of the Department, including the smaller agencies that didn't—that got that from their parent departments. They actually now have designated DHS individuals inside the Department.

They meet on a regular basis, usually not lengthier than monthly, to not only address all information security policy issues, the compliance thereof, any type of reporting, such as FISMA, that we have recently completed our report out to you and to OMB; but they also serve to coordinate all of the processes that look at building—as we have mentioned, both Karen and I, building information security into all of our initiatives, not kind of pasting it on or tacking it on after the fact.

Mr. PUTNAM. Ms. Evans, perhaps you would like to comment on the role of security in the Federal Enterprise Architecture.

Ms. EVANS. And I would be happy to do that, sir.

Cyber security, right now, through the work of the Federal CIO council on the architecture subcommittee, there is an effort under way that is specifically dealing with cyber security to ensure that it is integrated throughout the models that are being produced that support the Federal Enterprise Architecture.

So it is not going to be a separate entity or a separate model unto itself, but each model comprised and rolled up into the Federal Enterprise Architecture will have a cyber security element to ensure that every decision, everything that we go forward with that cyber security is adequately addressed to ensure the cyber posture for the Nation.

Mr. PUTNAM. Thank you.

We have had our share of worms and viruses this year. And my understanding is that 90 percent of the Federal Government is a single operating system, the same one. And so while we talk about not building more stovepipes on the one hand, there is this concept out there of monoculture, of a particular vulnerability that wipes out the entire enterprise. And I am curious how we work through those issues with regard to the Federal Enterprise Architecture.

Knowing the vulnerabilities that are out there, knowing that it could be exacerbated by having the vast majority of the Federal enterprise on the same operating system, how do we guard against these worms and viruses and issues that will only grow worse and more rapid as time goes by?

Ms. EVANS. When we look at that and look at the worms and viruses that are going forward, it really comes down to configuration management and how each entity moves forward and deals with configuration management. And as OMB moves forward and works with each department and agency, most of these situations, when you look at them—and I can speak—I will step back into my DOE role, when we did the analysis in the past year of things that occurred within the Department. They were all related to, if we had patched in a timely and appropriate manner, that we would have avoided that situation.

So this really does come down to being able to ensure that patches are applied in a timely manner and that good configuration management processes are in place within each department.

Mr. PUTNAM. And how quickly is information on the latest patch disseminated throughout the Federal Government right down to local case work type—the local Social Security offices around the country and USDA offices and bases around the world? How quickly can we get the word out and have reason to expect and hold people accountable for applying that patch?

Ms. EVANS. I would say currently—I still sit in as the vice chair of the CIO Council, so I am aware that my predecessor has also briefed on that particular area. But we have moved through the Federal CIO Council to put procedures in place so the dissemination of that information happens very quickly through cooperation, and also with the efforts of FedCIRC over at DHS; so that then there is a process that's in place within each department that then makes sure that information gets disseminated to all the appropriate sources for the patching.

As far as how quickly that occurs within each agency, I would be glad to go back and get more information on that and brief the committee; because OMB did collect that information from each agency, and so I would be glad to discuss that with you in further detail.

Mr. PUTNAM. Since you have it, yes, I would be very interested in knowing to what extent enterprise-wide we're actually applying the patches that are available. I mean, undoubtedly it's just like business or home users or anything else, people don't want to fool with it, they don't think they need to, they don't think it applies to them, they don't think that they'll get it, they don't feel like stopping what they're doing to do it. All the same human issues that go into the private sector apply to government and perhaps even more so.

So it would make sense the same reluctance that exists in the private sector would exist in the government, and I would be curious to know how effectively we have ingrained the importance of adequate patch management and rapid response to that.

If you would, though, comment on the fact that is such a high percentage of a single operating system. Is that a concern? Is that a nonissue? Elaborate on that if you would.

Mr. COOPER. Can I jump in?

Mr. PUTNAM. Certainly.

Mr. COOPER. I think for us—let me answer it this way.

For us, when we took a quick look across the inherited components of the Department, particularly in kind of a desktop space, what we saw was that about 80 percent of our inherited environments were a single vendor. It was a very easy business decision from an economic standpoint to say, OK, in that space, for the time being, let's go with what we have.

The costs of changing would have been prohibitive. It also would have led to very serious concerns about the abilities to sustain mission capability from day one.

However, having said that, we are paying a lot of attention to the security vulnerabilities of that particular operating system environment. We are, within the Department of Homeland Security, very actively encouraging a heterogenous environment, particularly in our mission application space as opposed to desktop type of space. So as we have mission-critical applications, we are taking a look at what is the environment we want to put that particular application or application hosting in. We do have a lot of inherited environments that are not that same particular vendor; and we will not only continue to support, but probably expand some of that capability in a Unix environment or a Linux environment because we think that is highly appropriate to what we are trying to accomplish in the Department.

We want to do no harm to mission capability. We want to do it in an effective and economic way. And we want to do it so if we need to migrate, we are migrating in a way that is cost effective, rapid, and again, does not harm the delivery of mission capability.

Mr. PUTNAM. That's a very helpful response. I have no hidden agenda in the question. I am the guy that just wrote a letter to GSA demanding to know why they are not standardizing this stuff. I just recognize that there's a line where the economic incentives of a common vendor and common applications are superseded by security concerns, and that's an art and not a science, and that's why we pay you the big bucks to decide where that line is, but I am not being critical of any vendor at all. As long as human beings are going to be designing and developing this stuff, there will be problems.

But there is certainly a vast opportunity in the Federal Government for nonmission-critical desktop applications and things where there are tremendous cost savings to be realized and certain niche components in agencies like yours where you want redundancy. And so I think that's perfectly appropriate.

Ms. EVANS. I would like to say, sir, that even if it is a single operating system, any type of approach as we go forward—and I would really like to get back to configuration, it is a risk-based approach that all of us take in moving forward and assessing the risk; how quickly and how can we apply resources to ensure that things are properly patched.

Technology does exist where, regardless of what the operating system is, you can automate the application of the patch and then move forward.

So as we move forward to whether it's standards-based or a single type of operating system or the known operating systems that we are managing in our environments, technology exists so that we can look at how we can apply our resources the best way that we can, automate the things that can be automated, such as patch management, and then allow those resources that we have, the scarce resources that we have that are doing these daily operations to really be focused on the high-level, mission-critical operations and ensuring that those are adequately secure as we move forward.

Mr. COOPER. If I may add one additional thought, and I don't mean this to be as controversial as it may end up sounding.

Mr. PUTNAM. Choose carefully. There are a lot of pens and pads in the room.

Mr. COOPER. But, I mean, this in a constructive way.

Patch management is something that we have to do because of what we're dealt. We have entered into conversations with this particular company that none of us are naming and had some very serious and candid conversations about, Look, realistically you have to improve the quality of your product relating to information security. It's that simple.

Karen is absolutely right. We have invested a significant amount of time and energy and people's, you know, resources and expertise and everything in configuration management, in patch management. But I also argue that we could lessen the need for that if we worked cooperatively and collaboratively with some of our major vendors to produce quality product that doesn't have quite so many vulnerabilities in it.

Mr. PUTNAM. Well said. And certainly the purchasing power of the Federal Government would be a powerful incentive to improve the quality of any particular vendor's given product. As long as we are willing to buy products that are not to the standard that they should be, people will continue to sell those to us.

Both of you have been down in the trenches and have seen the Federal Government's IT enterprises at the field level, and you understand, certainly better than anyone on this subcommittee without a doubt, the real-world cultural differences.

As you have assumed these new major positions of responsibility, what are your thoughts on ways to break down those barriers and really have effective information sharing, effective cross-agency coordination and cooperation?

Mr. COOPER. I think, from my perspective, one of the biggest challenges is kind of—I guess it's communication, meaning getting the right folks in one room at one time to have the type of conversation that really then almost always enables us to reach the type of collaborative decisions we need to make. And I'm not sure that's anybody's fault.

Right now in the Department we have so much coming at us, we're literally trying to change the tires on the car while it's moving 70 miles an hour. We're still staffing, meaning we're still trying to hire folks into some of our authorized positions, things like that. So getting quality time with some of the key people to address many of the challenges of information sharing is difficult. I mean, it is a very real challenge. It's not because anybody is trying to do the wrong thing.

When we are able to do that, we're actually able to reach consensus and move forward rather quickly. But doing that first within the Department of Homeland Security, then doing it among and between the Department and other Federal agencies, then doing it with each of our stakeholders—it's a numbers game.

There are 56 States and territories. We have a State homeland security coordinator in each of the 56 States and territories. That one is easy, and we have regular conversations with those folks a couple times a week. But if we then try to reach out and collaborate around information sharing with, for example, counties, there are 33,000 counties.

I don't know how to do it, I admit. I don't know how to get exactly the right representation. How do we collectively pull all these folks together?

There are 89,000 municipalities at the local level. Now layer on top of that the five major sectors of the emergency responder community or the first responder community. Our struggle is, how do you get the right people together to have the discussion.

Mr. PUTNAM. Well, you've done an outstanding job of laying out the challenge, but I would just respond to that by saying the primary purpose in your Department's creation was information sharing. I mean, all the functions of the Department of Homeland Security were already there, but it was a breakdown in information sharing that allows bad guys to fly in on airliners and allows bad guys to cross the border and allows bad guys to smuggle bad things in the bottoms of ships. So I view your role in the Department of Homeland Security as being the most critical. That was the reason why I voted to create it.

We are not going to save any money in the near future. We hope to in the long run, but it's going to cost us more in the short run to merge all this stuff together. It was the fact that one file wasn't being transferred from one desktop to another desktop. It was the fact that people in one border guard station weren't talking to the one right next to them, and they were wearing separate uniforms at the same time. It was that information sharing, I think, that led the Congress to make that leap. And so it's vitally important.

I know that both of you have other engagements and need to leave very shortly, and I can't hold it against you since I was an hour and a half late getting here myself. I will give you the opportunity at this point in the meeting to express whatever is on your mind, and you think is important to go in the record and for the subcommittee to hear.

And as you embark on your 3rd day on the job, we'll give you a few more moments to collect your thoughts and go with Mr. Cooper first and let him respond, and then we'll go to you, Ms. Evans.

Mr. COOPER. Thank you very much for the opportunity to join you today. And I would welcome the opportunity to come back and continue the dialog. I think that's very, very important.

The key message that I want to deliver is that, in a very short period of time, we have developed our first release of an enterprise architecture for the Department of Homeland Security, and we are using it. So in spite of some of the challenges and things I shared with you, we are really doing real things on the ground.

We are making progress in the information sharing arena. We have connected between States and local governments and that type of thing that previously we had no connection. And we are sharing information on a daily basis.

We need to expand that. We need to buildupon it. We're not where we all want to be, but there is very positive news and a lot of it is linked to what we are learning and continuing to learn, developing our enterprise architecture.

I also would like to thank some of the folks that have joined me today and would like to introduce them by name to the committee, because they really are the key people who have led a significant amount of the effort that I've been just the spokesperson for here this morning. Sitting behind me, George Brundage, Charles Thomas, Amy Wheelock and two other individuals who weren't able to join us, Katherine Santana and Ron Williams, really form kind of the core team that guided a whole host of other individuals too lengthy to name across the Department and have achieved Release 1 of our enterprise architecture.

Mr. PUTNAM. Thank you very much. And I do want to note that DHS produced the first EA in 4 months.

Mr. COOPER. That's correct.

Mr. PUTNAM. And I don't think that can be overstated. It's very impressive, and it's a testament to your hard work and folks on your team, and a lot of the other departments can derive some lessons from that accomplishment.

Ms. Evans.

Ms. EVANS. I too would like to thank you for the opportunity to be here today.

I would like to state that I will plan to continue the work of my predecessor. I believe that he started many great things here in the government to be able to move us forward to achieve things and to really achieve value for the government and the American citizen.

So I really would plan to drive toward the full utilization of the President's E-Government Initiative and progressing the work of the enterprise architectures within the agency, as well as the Federal Enterprise Architecture through the work of the CIO Council, and ensuring that the CIO Council remains a forum for discussion and for agencies as we move forward; and then continue to work to institutionalize the work he started within the management processes that are available to us, and continue to work with the subcommittee as we move forward, ensuring things such as IT security, privacy, planning, implementation and evaluation of all these IT investments for the agencies.

Mr. PUTNAM. Thank you very much. And I want to thank both of you for your hard work and for your commitment to public service. Obviously, you bring a tremendous expertise in coordinating our IT blueprint toward eliminating those stovepipes that we talked so much about, reducing redundancies where it's appropriate and making systems more secure and maybe even saving us a buck or two. It is a complicated issue that will not be solved overnight, and I speak for the entire subcommittee in saying you have our support in working through this process.

I hope that you will not burn out and cash out but keep the faith and keep plugging away because it's certainly an important yet difficult task.

In the event that there are some questions from the subcommittee that we were not able to get to, I would ask the record remain open for 2 weeks for those submissions. And I believe both of you have made notes on things that we have discussed that we would like further clarification on from the subcommittee.

Again, we wish you the best and thank you for your support. And with that, the subcommittee will stand adjourned.

[Whereupon, at 12:15 p.m., the subcommittee was adjourned.]

○