

HOW MUCH IS TOO MUCH? EXAMINING DUPLICATIVE IT INVESTMENTS AT DOD AND DOE

HEARING

BEFORE THE
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION
POLICY, INTERGOVERNMENTAL RELATIONS AND
PROCUREMENT REFORM

OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

HOUSE OF REPRESENTATIVES

SECOND SESSION

FEBRUARY 17, 2012

Serial No. 112-135

Printed for the use of the Committee on Oversight and Government Reform



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

U.S. GOVERNMENT PRINTING OFFICE

74-041 PDF

WASHINGTON : 2012

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) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

DARRELL E. ISSA, California, *Chairman*

DAN BURTON, Indiana	ELLJAH E. CUMMINGS, Maryland, <i>Ranking</i>
JOHN L. MICA, Florida	<i>Minority Member</i>
TODD RUSSELL PLATTS, Pennsylvania	EDOLPHUS TOWNS, New York
MICHAEL R. TURNER, Ohio	CAROLYN B. MALONEY, New York
PATRICK T. McHENRY, North Carolina	ELEANOR HOLMES NORTON, District of
JIM JORDAN, Ohio	Columbia
JASON CHAFFETZ, Utah	DENNIS J. KUCINICH, Ohio
CONNIE MACK, Florida	JOHN F. TIERNEY, Massachusetts
TIM WALBERG, Michigan	WM. LACY CLAY, Missouri
JAMES LANKFORD, Oklahoma	STEPHEN F. LYNCH, Massachusetts
JUSTIN AMASH, Michigan	JIM COOPER, Tennessee
ANN MARIE BUERKLE, New York	GERALD E. CONNOLLY, Virginia
PAUL A. GOSAR, Arizona	MIKE QUIGLEY, Illinois
RAÚL R. LABRADOR, Idaho	DANNY K. DAVIS, Illinois
PATRICK MEEHAN, Pennsylvania	BRUCE L. BRALEY, Iowa
SCOTT DESJARLAIS, Tennessee	PETER WELCH, Vermont
JOE WALSH, Illinois	JOHN A. YARMUTH, Kentucky
TREY GOWDY, South Carolina	CHRISTOPHER S. MURPHY, Connecticut
DENNIS A. ROSS, Florida	JACKIE SPEIER, California
FRANK C. GUINTA, New Hampshire	
BLAKE FARENTHOLD, Texas	
MIKE KELLY, Pennsylvania	

LAWRENCE J. BRADY, *Staff Director*

JOHN D. CUADERES, *Deputy Staff Director*

ROBERT BORDEN, *General Counsel*

LINDA A. GOOD, *Chief Clerk*

DAVID RAPALLO, *Minority Staff Director*

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL
RELATIONS AND PROCUREMENT REFORM

JAMES LANKFORD, Oklahoma, *Chairman*

MIKE KELLY, Pennsylvania, <i>Vice Chairman</i>	GERALD E. CONNOLLY, Virginia, <i>Ranking</i>
JASON CHAFFETZ, Utah	<i>Minority Member</i>
TIM WALBERG, Michigan	CHRISTOPHER S. MURPHY, Connecticut
RAÚL R. LABRADOR, Idaho	STEPHEN F. LYNCH, Massachusetts
PATRICK MEEHAN, Pennsylvania	JACKIE SPEIER, California
BLAKE FARENTHOLD, Texas	

CONTENTS

Hearing held on February 17, 2012	Page 1
WITNESSES	
Mr. David A. Powner, Director, Information Technology Management Issues, Government Accountability Office	
Oral statement	2
Written statement	5
Ms. Teresa M. Takai, Chief Information Officer, Department of Defense	
Oral statement	22
Written statement	24
Mr. Michael W. Locatis, III., Chief Information Officer, Department of Energy	
Oral statement	31
Written statement	33
Mr. Richard Spires, Chief Information Officer, Department of Homeland Security	
Oral statement	39
Written statement	41
APPENDIX	
The Honorable James Lankford, A Member of Congress from the State of Oklahoma: Written statement	68
The Honorable Gerald E. Connolly, A Member of Congress from the State of Virginia: Written statement	70
Questions for the record for Teri Takai	71
Questions for the record for Richard Spires	75

HOW MUCH IS TOO MUCH? EXAMINING DUPLICATIVE IT INVESTMENTS AT DOD AND DOE

FRIDAY, FEBRUARY 17, 2012

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

The subcommittee met, pursuant to notice, at 9:30 a.m., in room 2154, Rayburn House Office Building, Hon. James Lankford (chairman of the subcommittee) presiding.

Present: Representatives Lankford, Chaffetz, Walberg, Meehan, and Connolly.

Staff present: Ali Ahmad, Communications Advisor; Richard A. Beutel, Senior Counsel; Molly Boyl, Parliamentarian; Gwen D'Luzansky, Assistant Clerk; Laura L. Rush, Deputy Chief Clerk; Richard Burkard, Detailee; Jaron Bourke, Minority Director of Administration; Jennifer Hoffman, Minority Press Secretary; Carla Hultberg, Minority Chief Clerk; Paul Kinkaid, Minority Press Secretary; Chris Knauer, Minority Senior Investigator; Adam Koshkin, Minority Staff Assistant; and Suzanne Owen, Minority Health Policy Advisor.

Mr. LANKFORD. The hearing on "How Much is Too Much? Examining the Duplicative IT Investments at DOD and DOE," and, honestly, to get a chance to look at what the process that we can do in IT investments governmentwide, will come to order.

Oversight Committee existed—let me start all over.

Good morning.

We exist to secure two fundamental principles: First, Americans have the right to know the money Washington takes from them is well spent; second, Americans deserve an efficient, effective government that works for them. Our duty on the Oversight and Government Reform Committee is to protect these rights.

Our solemn responsibility is to hold government accountable to taxpayers, because taxpayers do have the right to know what they get from their government. We will work tirelessly, in partnership with citizens watchdogs, to deliver the facts to the American people and bring genuine reform to the Federal bureaucracy.

This is the mission of Oversight and Government Reform.

I am going to allow my opening statement to go in for the record, instead of doing it orally.

Mr. LANKFORD. And I have asked the ranking member to also do the same.

Is that okay with you?

Mr. CONNOLLY. It is. And it is one of the first in Congress, I think, Mr. Chairman. Yes.

Mr. LANKFORD. Well, you know what? We can slide that in.

Mr. CONNOLLY. So I can listen to them instead of ourselves.

Mr. LANKFORD. That would be great for this, as far as the help on that.

Mr. LANKFORD. So other Members will have 7 days to submit their opening statements. There may be some others that slip in on this and add extraneous material for the record itself.

Mr. LANKFORD. I would like to welcome our panel.

And let me tell you why we are rushing through the beginning of this. Votes have been called somewhere between 10 to 10:15. It is our goal to try to get in the statements of our witnesses and do additional questions with them. If we can keep close on time, we can get a chance to honor time and not have to break for votes and then come back. We can try to conclude before we head for votes, which will honor every else's time. If we are not able to do that, we will have a nice 30- to 40-minute break in the middle of our hearing, and then we will come back and conclude at the end.

So I would like to welcome this first panel of witnesses.

Mr. David Powner is the director of the Government Accountability Office's Information Technology Management Issues team. Ms. Teri Takai is the chief information officer at the Department of Defense. Mr. Michael Locatis is the chief information officer at the Department of Energy. Mr. Richard Spires is the chief information officer at the Department of Homeland Security.

Thank you all for being here.

Pursuant to committee rules, all witnesses are sworn in before they testify. If you would please stand and raise your right hands, please.

Do you solemnly swear or affirm that the testimony you are about to give to this committee will be the truth, the whole truth, and nothing but the truth, so help you God?

Thank you.

Let the record reflect all the witnesses have answered in the affirmative.

In order to allow time for discussion, I would ask you to limit your testimony to 5 minutes. Of course, your entire written statement will be made part of the permanent record, as well.

With that, I would like to recognize Mr. Powner for his opening statement for 5 minutes.

STATEMENTS OF WITNESSES

STATEMENT OF DAVID A. POWNER

Mr. POWNER. Chairman Lankford, Ranking Member Connolly, it is a pleasure to be here this morning to discuss our latest report that highlights duplicative IT investments. The Federal Government spends nearly \$80 billion on IT, and it is imperative that these investments enable the government to better serve the American people.

The past several years have resulted in major improvements in transparency and focus on IT management. First, in June 2009, the IT Dashboard has been providing cost and schedule information on nearly 800 IT investments and has provided a level of transparency and CIO accountability that is unparalleled.

Today, over 250 investments, totaling nearly \$18 billion, are at risk, meaning that agencies are rating these investments in either a yellow or red status. Focusing on these at-risk investments has made a difference. OMB claims that they have saved nearly \$3 billion through its TechStat reviews that have resulted in poorly performing projects being halted or canceled. However, we still have too many investments at risk.

In addition to the Dashboard, in December 2010 the IT Reform Plan was initiated that lays out an excellent roadmap to strengthen IT acquisition, governance, and program management. It also, if implemented successfully, will result in more cost-effective IT operations by focusing on commodity IT, cloud-based solutions, and data center consolidation. Over 200 data centers have already been closed, and the goal is to close a thousand by 2015. OMB estimates that data center consolidation will result in another \$3 billion in savings.

The Reform Plan emphasizes IT governance. Reforming and strengthening IT investment review boards and executive-level governance can greatly help turn around underperforming projects, as our many reviews for the Congress have highlighted.

These governance processes can also identify and eliminate duplicative spending. This is important because last fall we issued a report that highlighted hundreds of investments providing similar functions across the Federal Government. The numbers here are staggering. For example, last year alone, the Federal Government invested in 781 supply chain systems, totaling \$3.3 billion; 661 human resource systems, totaling \$2.5 billion; and 580 financial management systems, totaling \$2.7 billion. We recommended that Federal agencies ensure that their IT investments are not duplicative as part of their annual budget submissions.

Mr. Chairman, at the committee's request, we followed up this review with a deeper look into IT investments at the Departments of Defense, Homeland Security, and Energy. Specifically, we looked at over 800 investments at these 3 agencies associated with human resources, IT, and supply chain management. We found 37 investments in 12 categories that are potentially duplicative. For example, we found that the Air Force had five similar contract management systems, the Navy had four similar personnel assignment systems, and Energy had three similar back-end infrastructure investments.

Addressing this duplication is important since DOD and Energy have spent \$1.2 billion on these 37 investments over the past 5 years. Our report highlights the details of these investments and makes recommendations to eliminate duplicative spending and to further report on efforts to rout out duplication.

The good news, Mr. Chairman, is that each agency has actions under way to tackle this duplication. DHS is furthest along, having already identified and eliminated duplicative investments through various portfolio reviews. For example, DHS consolidated six per-

sonnel-security-related systems into an enterprise system. At DOD, the Navy has implemented an executive oversight board, chaired by the Navy CIO, and all IT expenditures greater than \$100,000 are reviewed and approved by the Navy CIO to ensure that they are not duplicative.

DOE has various working groups addressing the records management and back-end infrastructure areas we pointed out and, on a broader scale, is holding TechStat sessions that are aimed at troubled investments and consolidating commodity IT services.

Mr. Chairman, I would like to commend the leadership of the individuals on this panel. We expect further results from each agency in the near future as their efforts get more traction, but to be clear, we need more tangible results that eliminate duplicative spending.

In summary, Mr. Chairman, it is safe to say that there is much more IT duplication out there. It is important that the agencies represented here and others use their investment governance processes to identify and address duplicative spending so that billions of taxpayers' dollars are not wasted.

This concludes my statement. I look forward to your questions.

Mr. LANKFORD. Thank you, Mr. Powner.

[Prepared statement of Mr. Powner follows:]

February 17, 2012

Chairman Lankford, Ranking Member Connolly, and Members of the Subcommittee:

I am pleased to be here today to discuss the potentially duplicative information technology (IT) investments at selected agencies and actions these agencies are taking to address them. With at least \$79 billion spent in fiscal year 2011 by the United States government on IT investments, it is important that federal agencies avoid investing in duplicative investments, whenever possible, to ensure the most efficient use of resources.

Last year, we issued a comprehensive report that identified federal programs or functional areas where unnecessary duplication, overlap, or fragmentation exists; the actions needed to address such conditions; and the potential financial and other benefits of doing so.¹ More recently, we reported on the Office of Management and Budget's (OMB) and federal agencies' oversight of IT investments and the initiatives under way to address potentially duplicative IT investments.² Specifically, we recently reported that there are hundreds of IT investments providing similar functions across the federal government. For example, agencies reported about 1,500 investments that perform general information and technology functions, about 775 supply chain management investments, and about 620 human resource management investments.

You asked us to testify on our report being released today that describes the extent to which potentially duplicative IT investments exist within these three categories, including the actions agencies are taking to address them.³ In this regard, my testimony specifically covers potentially duplicative investments we identified at three of the largest agencies with respect to number of investments—the Departments of Defense (DOD), Energy (DOE), and Homeland Security (DHS). In preparing this testimony, we relied on the GAO report being released at today's hearing.

¹GAO, *Opportunities to Reduce Potential Duplication in Government Programs, Save Tax Dollars, and Enhance Revenue*, GAO-11-318SP (Washington, D.C.: Mar. 1, 2011).

²GAO, *Information Technology: OMB Needs to Improve Its Guidance on IT Investments*, GAO-11-826 (Washington, D.C.: Sept. 29, 2011).

³GAO, *Information Technology: Departments of Defense and Energy Need to Address Potentially Duplicative Investments*, GAO-12-241 (Washington, D.C.: Feb. 17, 2012).

In that report, to identify potentially duplicative IT investments within each of the selected agencies, we analyzed a subset of investment data from OMB's exhibit 53 to identify investments with similar functionality.⁴ Specifically, we reviewed 810, or 11 percent, of the approximately 7,200 IT investments federal agencies report to OMB through the exhibit 53. Our review represents approximately 24 percent of DOD's IT portfolio in terms of the number of investments that they report to OMB, 19 percent of DOE's, and 16 percent of DHS's. We then reviewed the name and narrative description of each investment's purpose to identify similarities among related investments within each agency (we did not review investments across agencies).⁵ This formed the basis of establishing groupings of similar investments. We discussed the groupings with each of the selected agencies, and we obtained further information from agency officials and reviewed and assessed agencies' rationales for having multiple systems that perform similar functions. Additionally, when analyzing each investment's description, we compared the investment's designated Federal Enterprise Architecture (FEA)⁶ primary category and sub-category with OMB's definitions for each FEA primary category and sub-category and determined whether the investment was placed in the correct FEA category. We obtained additional information from agency officials about these discrepancies. We also interviewed officials to discuss actions agencies have taken to address the potentially duplicative investments and reviewed supporting documentation.

All work on which this testimony is based was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained

⁴The exhibit 53 identifies all IT projects—both major and non-major—and their associated costs within a federal organization. Information included on agency exhibit 53s is designed, in part, to help OMB better understand what agencies are spending on IT investments

⁵Certain investments were not placed in groups because the investment descriptions were too broad. Additionally, IT investments identified as Funding Contributions were not included, since they are managed by other agencies

⁶The FEA is intended to provide federal agencies and other decision-makers with a common frame of reference or taxonomy for informing agencies' individual enterprise architecture efforts and their planned and ongoing investment activities, and to do so in a way that identifies opportunities for avoiding duplication of effort and launching initiatives to establish and implement common, reusable, and interoperable solutions across agency boundaries

provides a reasonable basis for our findings and conclusions based on our audit objective.

Background

Information technology should enable government to better serve the American people. However, according to OMB, despite spending more than \$600 billion on IT over the past decade, the federal government has achieved little of the productivity improvements that private industry has realized from IT.⁷ Too often, federal IT projects run over budget, behind schedule, or fail to deliver promised functionality. In combating this problem, proper oversight is critical. Both OMB and federal agencies have key roles and responsibilities for overseeing IT investment management. OMB is responsible for working with agencies to ensure investments are appropriately planned and justified. Additionally, each year, OMB and federal agencies work together to determine how much the government plans to spend on IT projects and how these funds are to be allocated.

OMB's IT Oversight Mechanisms

OMB uses the following mechanisms to help it fulfill oversight responsibilities of federal IT spending during the annual budget formulation process.

- OMB requires 27 federal departments and agencies⁸ to provide information related to their IT investments, including agency IT investment portfolios (called exhibit 53s) and capital asset plans and business cases (called exhibit 300s).⁹

⁷OMB, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Washington, D.C. December 2010)

⁸The 27 agencies are the Agency for International Development, the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs, the Army Corps of Engineers, the Environmental Protection Agency, the General Services Administration, the National Aeronautics and Space Administration; the National Archives and Records Administration, the National Science Foundation; the Nuclear Regulatory Commission, the Office of Personnel Management; the Small Business Administration; the Smithsonian Institution; and the Social Security Administration

⁹The exhibit 300s provide a business case for each major IT investment and allow OMB to monitor IT investments once they are funded. Agencies are required to provide information on each major investment's cost, schedule, and performance

-
- In June 2009, OMB publicly deployed the IT Dashboard, which is intended to display near real-time information on the cost, schedule, and performance of all major IT investments.¹⁰ For each major investment, the Dashboard provides performance ratings on cost and schedule, a chief information officer (CIO) evaluation, and an overall rating. The CIO evaluation is based on his or her evaluation of the performance of each investment and takes into consideration multiple variables. The CIO also has the ability to provide written comments regarding the status of each investment.

According to OMB, the public display of investment data on the IT Dashboard is intended to allow OMB, other oversight bodies, and the general public to hold government agencies accountable for results and progress. In addition, the Dashboard allows users to download exhibit 53 data, which provide details on the more than 7,200 federal IT investments (totaling \$78.8 billion in planned spending for fiscal year 2011).

As we have previously reported, while the IT Dashboard provides IT investment information for 27 federal agencies, it does not include any information about 61 other agencies' investments.¹¹ Specifically, it does not include information from 58 independent executive branch agencies and 3 other agencies. It also does not include information from the legislative or judicial branch agencies. Accordingly, we recommended that OMB specify which executive branch agencies are included when discussing the annual federal IT investment portfolio. OMB disagreed with this recommendation, stating that the agencies included in the federal IT portfolio are already identified in OMB guidance and on the IT Dashboard. However, we maintained that the recommendation had not been fully addressed because OMB officials frequently refer to the federal IT portfolio without clarifying that it does not include all agencies.

¹⁰According to OMB guidance, a major investment is a system or acquisition requiring special management attention because of its importance to the mission or function of the agency, a component of the agency, or another organization, is for financial management and obligates more than \$500,000 annually, has significant program or policy implications, has high executive visibility, has high development, operating, or maintenance costs, is funded through other than direct appropriations, or is defined as major by the agency's capital planning and investment control process.

¹¹GAO-11-826.

Agencies Spend Billions on Poorly Performing IT Investments

Despite OMB's oversight mechanisms, the federal government spends billions of dollars on poorly performing IT investments, as the following examples illustrate:

- In February 2010, the Defense Integrated Military Human Resources System was canceled after 10 years of development and approximately \$850 million spent, due, in part, to a lack of strategic alignment, governance, and requirements management, as well as the overall size and scope of the effort.¹²
- In January 2011, the Secretary of Homeland Security ended the Secure Border Initiative Network program after spending about \$1.5 billion because it did not meet cost-effectiveness and viability standards.¹³
- In February 2011, the Office of Personnel Management canceled its Retirement Systems Modernization program, after several years of trying to improve the implementation of this investment.¹⁴ According to the Office of Personnel Management, it spent approximately \$231 million on this investment.

Additionally, as of August 2011, according to the IT Dashboard, 261 of the federal government's approximately 800 major IT investments—totaling almost \$18 billion—are in need of management attention (rated "yellow" to indicate the need for attention or "red" to indicate significant concerns).¹⁵ (See fig. 1.)

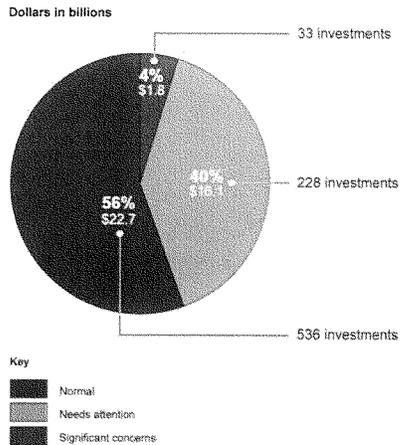
¹²Advance Policy Questions for Testimony of Elizabeth A. McGrath to be Deputy Chief Management Officer of the Department of Defense. <http://armed-services.senate.gov/statemnt/2010/03%20March/McGrath%2003-23-10.pdf> (Washington, D.C.: March 2010).

¹³GAO, *Border Security: Preliminary Observations on the Status of Key Southwest Border Technology Programs*, GAO-11-448T (Washington, D.C.: Mar 15, 2011).

¹⁴GAO, *OPM Retirement Modernization: Longstanding Information Technology Management Weaknesses Need to Be Addressed*, GAO-12-226T (Washington, D.C. Nov 15, 2011)

¹⁵The approximately 800 major IT investments total about \$40.6 billion for fiscal year 2011.

Figure 1: Overall Performance Ratings of Major IT Investments on the Dashboard, as of August 2011



Source: OMB's IT Dashboard.

In recognizing that wasteful spending continues to plague IT investment management, OMB has recently implemented additional efforts to address this problem. These efforts include the following:

- *TechStat reviews.* In January 2010, the Federal CIO began leading reviews—known as “TechStat” sessions—of selected IT investments involving OMB and agency leadership to increase accountability and transparency and improve performance. OMB officials stated that, as of December 2010, 58 sessions had been held and resulted in improvements to or termination of IT investments with performance problems. In addition, OMB has identified 26 additional high-priority IT projects and plans to develop corrective action plans with agencies at future TechStat sessions. According to the former Federal CIO, OMB's efforts to improve management and oversight of IT investments have resulted in \$3 billion in savings.
- *IT reform.* In December 2010, the Federal CIO issued a *25 Point Implementation Plan to Reform Federal Information Technology*

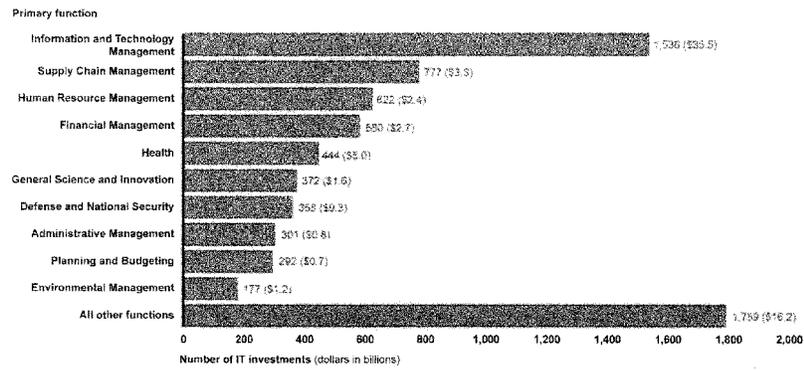
Management. This 18-month plan specified five major goals: strengthening program management, streamlining governance and improving accountability, increasing engagement with industry, aligning the acquisition and budget processes with the technology cycle, and applying "light technology" and shared solutions. As part of this plan, OMB outlined actions to, among other things, strengthen agencies' investment review boards and consolidate federal data centers. The plan stated that OMB will work with Congress to consolidate commodity IT spending (e.g., e-mail, data centers, content management systems, and web infrastructure) under agency CIOs. Further, the plan called for the role of federal agency CIOs to focus more on IT portfolio management.

Categorization of IT Investments Is Intended to Facilitate Identification of Similar IT Investments

In addition to these efforts to improve government spending on IT, avoiding unnecessary duplicative investments is critically important. In February 2002, OMB established the FEA initiative. According to OMB, the FEA is intended to facilitate governmentwide improvement through cross-agency analysis and identification of duplicative investments, gaps, and opportunities for collaboration, interoperability, and integration within and across agency programs. Since the fiscal year 2004 budget cycle, OMB has required agencies to categorize their IT investments in their annual exhibit 53s according to primary function and sub-function.

In their fiscal year 2011 submissions, agencies reported the greatest number of IT investments in Information and Technology Management (1,536 investments), followed by Supply Chain Management (777 investments), and Human Resource Management (622 investments). Similarly, planned expenditures on investments were greatest in Information and Technology Management, at about \$35.5 billion. Figure 2 depicts, by primary function, the total number of investments within the 27 federal agencies that report to the IT Dashboard.

Figure 2: Number of Government IT Investments by Primary Function, as of July 2011



Additionally, agencies were required to choose a sub-function for each investment related to the primary function.

GAO Has Previously Reported on Potential Duplication and the Challenges of Identifying Duplicative Investments

During the past several years, we have issued multiple reports and testimonies and made numerous recommendations to OMB and federal

agencies to identify and reduce duplication within the federal government's portfolio of IT investments.¹⁶

In March 2011, we reported an overview of federal programs and functional areas where unnecessary duplication, overlap, or fragmentation existed.¹⁷ Specifically, we identified 34 areas where agencies, offices, or initiatives had similar or overlapping objectives or provided similar services to the same populations, or where government missions were fragmented across multiple agencies or programs. The report touched on hundreds of federal programs, including IT programs, affecting virtually all major federal departments and agencies.

We reported that overlap and fragmentation among government programs or activities could be harbingers of unnecessary duplication. Thus, the reduction or elimination of duplication, overlap, or fragmentation could potentially save billions of tax dollars annually and help agencies provide more efficient and effective services. For example, we reported that, according to OMB, the number of federal data centers (defined as data processing and storage facilities) grew from 432 in 1998 to more than 2,000 in 2010. These data centers often house similar types of equipment and provide similar processing and storage capabilities. These factors have led to concerns associated with the provision of redundant capabilities, the underutilization of resources, and the significant consumption of energy. Operating such a large number of centers places costly demands on the government. In an effort to address these inefficiencies, in February 2010, OMB launched the Federal Data Center

¹⁶GAO, *IT Dashboard Accuracy Has Improved, and Additional Efforts Are Under Way to Better Inform Decision Making*, GAO-12-210 (Washington, D.C. Nov 7, 2011); GAO-11-826, *Information Technology: OMB Has Made Improvements to Its Dashboard, but Further Work Is Needed by Agencies and OMB to Ensure Data Accuracy*, GAO-11-262 (Washington, D.C. Mar. 15, 2011); *Information Technology: OMB's Dashboard Has Increased Transparency and Oversight, but Improvements Needed*, GAO-10-701 (Washington, D.C. July 16, 2010); *Information Technology: Management and Oversight of Projects Totalling Billions of Dollars Need Attention*, GAO-09-624T (Washington, D.C. Apr. 28, 2009); *Information Technology: OMB and Agencies Need to Improve Planning, Management, and Oversight of Projects Totalling Billions of Dollars*, GAO-08-1051T (Washington, D.C. July 31, 2008); *Information Technology: Further Improvements Needed to Identify and Oversee Poorly Planned and Performing Projects*, GAO-07-1211T (Washington, D.C. Sept. 20, 2007); *Information Technology: Improvements Needed to More Accurately Identify and Better Oversee Risky Projects Totalling Billions of Dollars*, GAO-06-1099T (Washington, D.C. Sept. 7, 2006); *Information Technology Agencies and OMB Should Strengthen Processes for Identifying and Overseeing High Risk Projects*, GAO-06-647 (Washington, D.C. June 15, 2006).

¹⁷GAO-11-318SP

Consolidation Initiative to guide federal agencies in consolidating data centers. Specifically, OMB and agencies plan to close more than 950 of the over 2,100 federal data centers by 2015. As of November 2011, agencies reported that a total of 149 data centers have been closed across the federal government. For example, 16 DOD data centers, 3 DOE centers, and 7 DHS centers have been closed.

In September 2011, we reported that limitations in OMB's guidance hindered efforts to identify IT duplication.¹⁸ Specifically, OMB guidance stated that each IT investment needs to be mapped to a single functional category within the FEA to allow for the identification and analysis of potentially duplicative investments across agencies. We noted that this limits OMB's ability to identify potentially duplicative investments both within and across agencies because similar investments may be organized under different functions. Accordingly, we recommended that OMB revise guidance to federal agencies on categorizing IT investments to ensure that the categorizations are clear and that it allow agencies to choose secondary categories, where applicable. OMB officials generally agreed with this recommendation and stated that they plan to update the FEA reference models to provide additional clarity on how agencies should characterize investments in order to enhance the identification of potentially duplicative investments.

We also reported that results of OMB initiatives to identify potentially duplicative investments were mixed and that several federal agencies did not routinely assess their entire IT portfolios to identify and remove or consolidate duplicative systems. Specifically, we said that most of OMB's recent initiatives have not yet demonstrated results, and several agencies did not routinely assess legacy systems to determine if they are duplicative. As a result, we recommended that OMB require federal agencies to report the steps they take to ensure that their IT investments are not duplicative as part of their annual budget and IT investment submissions. OMB generally agreed with this recommendation.

¹⁸GAO-11-826

Selected Agencies Have Potentially Duplicative Investments; DOD and DOE Need to Do More to Address Them

Although the Departments of Defense, Energy, and Homeland Security utilize various processes to prevent and reduce investment in duplicative programs and systems, potentially duplicative IT investments exist. Further complicating agencies' ability to identify and address duplicative investments is miscategorization of investments within agencies. Each of the agencies has recently initiated plans to address many of these investments. DHS's efforts have resulted in the identification and elimination of duplication, but DOD's and DOE's initiatives have not yet led to the elimination or consolidation of duplicative investments or functionality. Until DOD and DOE demonstrate progress on their efforts to identify and eliminate duplicative investments, and correctly categorize investments, it will remain unclear whether they are avoiding investment in unnecessary systems.

Potentially Duplicative IT Investments Exist at Selected Agencies

Each of the agencies we reviewed has IT investment management processes in place that are, in part, intended to prevent, identify, and eliminate unnecessary duplicative investments. For example, DOD's *Information Technology Portfolio Management Implementation* guide requires the evaluation of existing systems to identify duplication and determine whether to maintain, upgrade, delete, or replace identified systems. Similarly, DOE's *Guide to IT Capital Planning and Investment Control* specifies that investment business case summaries should be reviewed for redundancies and opportunities for collaboration. Additionally, according to DHS's *Capital Planning and Investment Control Guide*, proposed investments must be reviewed at the department level to determine if the proposed need is, among other things, being fulfilled by another DHS program, or already fulfilled by an existing capability.

Even with such investment review processes, of the 810 investments we reviewed,¹⁹ we identified 37 potentially duplicative investments at DOD and DOE within three FEA categories (Human Resource Management,

¹⁹We reviewed 11 percent of the total number of IT investments that agencies report to OMB through the IT Dashboard (810 of 7,227). The investments we reviewed represent approximately 24 percent of DOD's IT portfolio in terms of the number of investments reported to the Dashboard, 19 percent of DOE's, and 16 percent of DHS's.

Information and Technology Management, and Supply Chain Management).²⁰ These investments account for about \$1.2 billion in total IT spending for fiscal years 2007 through 2012. Specifically, we identified

- 31 potentially duplicative investments totaling approximately \$1.2 billion at DOD, and
- 6 potentially duplicative investments totaling approximately \$8 million at DOE.

The 37 investments comprise 12 groups of investments that appear to have duplicative purposes based on our analysis of each investment's description, budget information, and other supporting documentation from agency officials (see table 1). For example, we identified three investments at DOE that were each responsible for managing the back-end infrastructure at three different locations. We also identified four DOD Navy personnel assignment investments—one system for officers, one for enlisted personnel, one for reservists, and a general assignment system—each of which is responsible for managing similar assignment functions. Additionally, the Air Force has five investments that are each responsible for contract management, and within the Navy there are another five contract management investments. Table 1 summarizes the 12 groups of potentially duplicative investments we identified by purpose and agency.

²⁰Within the three selected functions, we narrowed our review to the following seven sub-functions: Benefits Management, Organization and Position Management, Employee Performance Management, Information Management, Information Security, Inventory Control, and Goods Acquisition

Table 1: Potentially Duplicative Investments

Dollars in millions

Department	Branch or bureau	Purpose	Number of investments	Planned and actual spending fiscal years 2007-2012
DOD	Air Force	Contract Management	5	\$41
	Army	Personnel Assignment Management	2	\$12
	Navy	Acquisition Management	4	\$407
		Aviation Maintenance and Logistics	2	\$85
		Contract Management	5	\$17
		Housing Management	2	\$5
		Personnel Assignment Management	4	\$28
		Promotion Rating	2	\$3
		Workforce Management	3	\$109
	DOD Enterprisewide	Civilian Personnel Management	2	\$504
DOE	Energy Programs	Back-end Infrastructure	3	\$1
	Energy Programs & Environmental and Other Defense Activities	Electronic Records and Document Management	3	\$7
	Total		37	\$1,219

Source: GAO analysis of agencies' data

We did not identify any potentially duplicative investments at DHS within our sample; however, DHS has independently identified several duplicative investments and systems. Specifically, DHS officials have identified and, more importantly, reduced duplicative functionality in four investments by consolidating or eliminating certain systems within each of these investments, including a personnel security investment, time and attendance investment, human resources investment, and an information network investment. DHS officials have also identified 38 additional systems that they have determined to be duplicative. For example, officials identified multiple personnel action processing systems that could be consolidated.

Officials from the three agencies reported that duplicative investments exist for a number of reasons, including decentralized governance within the departments and a lack of control over contractor facilities. For example, DOE investments for the management of back-end infrastructure are for facilities which DOE oversees but does not control. In addition, DOD officials indicated that a key reason for potential duplication at the Department of the Navy is that it had traditionally used a

decentralized IT management approach, which allowed offices to develop systems independent of any other office's IT needs or acquisitions.

Further complicating the agencies' ability to prevent investment in duplicative systems or programs is the miscategorization of investments. Among the 810 investments we reviewed, we identified 22 investments where the selected agencies assigned incorrect FEA primary functions or sub-functions. Specifically, we identified 13 miscategorized investments at DOD, 4 at DOE, and 5 at DHS. For example, DHS's Federal Emergency Management Agency—Minor Personnel/Training Systems investment was initially categorized within the Employee Performance Management sub-function, but DHS agreed that this investment should be assigned to the Human Resources Development sub-function.

Agency officials agreed that they had inadvertently miscategorized 15 of the 22 investments we identified. However, proper categorization is necessary in order to analyze and identify duplicative investments, both within and across agencies. Each improper categorization represents a possible missed opportunity to identify and eliminate an unjustified duplicative investment. Until agencies correctly categorize their investments, they cannot be confident that their investments are not duplicative and are justified, and they may continue expending valuable resources developing and maintaining unnecessarily duplicative systems.

Therefore, we recommended in our report that the agencies correct the miscategorizations for the investments we identified and ensure that investments are correctly categorized in agency submissions. In response, DOD stated that it agreed, and will attempt to make the categorization changes for certain investments in its fiscal year 2013 submission. DHS also agreed with the recommendation, and provided documentation showing that the department had recently corrected the miscategorizations for each of the investments we identified. DOE agreed that two of the four investments we identified could be recategorized, and reported that the department has made those changes. However, DOE disagreed that the other two investments we identified were miscategorized, explaining that its categorizations reflect funding considerations. However, OMB guidance indicates that investments should be classified according to their intended purpose. Consequently, we believe the recommendation is warranted.

Agencies Have Recently Initiated Plans to Address Potential Duplication in Many Investments, but Results Have Yet to Be Realized at DOD and DOE

DHS has taken action to improve its processes for identifying and eliminating duplicative investments, which has produced tangible results. Specifically, in 2010 and 2011, the DHS CIO conducted program and portfolio reviews of hundreds of IT investments and systems. DHS evaluated portfolios of investments within its components to avoid investing in systems that are duplicative or overlapping, and to identify and leverage investments across the department. Among other things, this effort contributed to the identification and consolidation of duplicative functionality within four investments. DHS also has plans to further consolidate systems within these investments by 2014, which is expected to produce approximately \$41 million in cost savings. The portfolio reviews also contributed to the identification of 38 additional systems that are duplicative. For example, officials identified multiple personnel action processing systems that could be consolidated.

DOD has begun taking action to address 29 of the 31 duplicative investments we identified. For example, according to DOD officials, four of the DOD Navy acquisition management investments—two for Naval Sea Systems Command and two for Space and Naval Warfare Systems Command—will be reviewed to determine whether these multiple support systems are necessary. In addition, DOD reported that the Air Force is in the process of developing a single contract writing system to replace the five potentially duplicative investments we have identified. Moreover, the Department of the Navy has implemented an executive oversight board that is chaired by the Navy CIO, and it is now the Navy's single senior information management and technology policy and governance forum. The Department of the Navy also required all IT expenditures greater than \$100,000 to be centrally reviewed and approved by the Navy CIO to ensure that they are not duplicative. Officials reported that these initiatives will include the review of Navy's 22 potentially duplicative investments that we identified.

Similarly, DOE has plans under way to address each of the 6 investments we identified as potentially duplicative. Specifically, DOE officials established working groups that are addressing the two groups of duplicative investments we identified. These working groups are to address records management and back-end infrastructure, and are looking across the department to minimize redundancy in each of these areas. In addition, the CIO stated that DOE has developed a departmental strategy for electronic records management whereby a small number of approved records management applications will be

identified for departmentwide use. Moreover, in a broader effort to reduce duplication across the department, in September and October 2011, DOE held technical strategic reviews, known as “TechStrat” sessions, which are aimed at exploring opportunities to consolidate DOE’s commodity IT services, such as e-mail and help desk support, among the various DOE offices. The first two sessions provided opportunities for DOE bureaus to identify and share lessons learned, and established action items to improve DOE’s IT investment portfolio.

While these efforts could eventually yield results, DOD’s and DOE’s initiatives have not yet led to the consolidation or elimination of duplication. For example, while DOD provided us with documented milestones—several of which have passed—for improving the Department of the Navy’s IT investment review processes, officials did not provide us with any examples of duplicative investments that they had consolidated or eliminated. Similarly, while DOE officials have documented time frames for consolidating DOE’s commodity IT services, electronic records management investments, and identity management investments, officials were unable to demonstrate that they have consolidated or eliminated unjustified duplicative investments.

Additionally, DOD does not have plans under way to address the remaining 2 of the 31 potentially duplicative investments, which are two civilian personnel management investments. Specifically, DOD officials stated that they do not have plans to address these two investments because they do not agree that they are potentially duplicative. However, agency officials were unable to demonstrate that investing in these systems and programs was justified.

Until DOD and DOE demonstrate, through existing transparency mechanisms, such as OMB’s IT Dashboard, that they are making progress in identifying and eliminating duplicative investments, it will remain unclear whether they are avoiding investment in unnecessary systems. Therefore, we recommended that these two agencies utilize existing transparency mechanisms, such as the IT Dashboard, to report on the results of their departments’ efforts to identify and eliminate, where appropriate, each potentially duplicative investment we identified, as well as any other duplicative investments. In response to our report, DOD and DOE stated that they agreed with the recommendation. Additionally, DOE added that for the non-major investments that we identified as being potentially duplicative, it will update GAO on its progress through means other than the IT Dashboard, since non-major investments are not individually tracked on the Dashboard.

In summary, while agencies have various investment review processes in place that are partially designed to avoid investing in systems that are duplicative, we have identified 37 potentially duplicative investments at DOD and DOE that account for about \$1.2 billion in total IT spending for fiscal years 2007 through 2012. Given that our review covered 11 percent (810 investments) of the total number of IT investments that agencies report to OMB, it raises questions about how much more potential duplication exists.

DHS's recent efforts have resulted in the identification and consolidation of duplicative functionality in several investments and related systems. DOD and DOE have also recently initiated plans to address many investments that we identified, but these recent initiatives have not yet resulted in the consolidation or elimination of duplicative investments or functionality. Further complicating agencies' ability to prevent, identify, and eliminate duplicative investments is miscategorization of investments within agencies. Implementation of our recommendations should provide better assurance that agencies are avoiding investment in unnecessary systems.

Chairman Lankford, Ranking Member Connolly, and Members of the Subcommittee, this concludes my statement. I would be happy to answer any questions at this time.

GAO Contact and Staff Acknowledgments

If you should have any questions about this testimony, please contact me at (202) 512-9286 or by e-mail at powned@gao.gov. Individuals who made key contributions to this testimony are Shannin O'Neill, Assistant Director; Javier Irizarry; Lee McCracken; and Kevin Walsh.

Mr. LANKFORD. Ms. Takai?

STATEMENT OF TERESA M. TAKAI

Ms. TAKAI. Good morning, Chairman Lankford and Ranking Member Connolly. Thank you so much for the opportunity to testify this morning on the findings of the GAO report that Mr. Powner just spoke of.

The GAO report highlights 31 business-related DOD IT investments that cover a range of areas. And, as mentioned, it specifically examined contracts, personnel management, and logistics systems. The Department is taking action to address 27 of the investments reviewed by GAO. The Department has looked at the remaining four systems, and we are prepared to discuss why those particular areas are actually not duplicative but more complementary. And we can go into more detail as you desire.

The Defense Department's IT budget presents a unique challenge, not only in terms of its magnitude—it constitutes one-half of the Federal Government's overall IT expenditure—but in scope and complexity, as well, as you know. The Department's fiscal year 1913 budget request of approximately \$37 billion includes funding all the way from desktop computers, tactical radios, human resource systems, commercial satellite communications, financial management, and you name it. These investments support mission-critical operations both in our Pentagon and office environment and on the battlefield. Our IT environment is even more complex when one considers that we operate in 6,000 locations around the world.

In this complex environment, the Department's business IT systems are essential enablers of a much broader set of integrated business operations. For example, paying our servicemembers on time is a responsibility shared among various members in our organization; it includes both human resources and financial professionals. So the business systems challenges for us really require a reform not only of our technologies but of our processes and our governance and our policies.

In my written statement, I have described for you the well-defined IT investment governance process that the Department uses. The Defense Business Systems Management Committee and our investment review boards, as well as our acquisition process, are major touch points for us to ensure that we are examining our IT investments. We use those processes to examine our new investments, but starting in fiscal year 1913 it will also include our existing IT capabilities and the dollars that we spend.

These processes are important in helping the Department accelerate the transition away from our legacy environment into our target business systems environment, but there are other activities under way within the Department to further support this goal.

But, first, I would like to provide you some specific examples of what the Department has done.

The Army reduced the number of IT applications from 218 to 77, a 65 percent reduction, during their BRAC move from Fort Monmouth, New Jersey, to the Aberdeen Proving Grounds. The Army Acquisition Domain has reduced the number of IT systems within that portfolio by 41 percent from 2006. The Logistics Modernization Program has sunset all 42 instances of the Army's Standard Depot

System. Additionally, they have sunset all but one instance of the Commodity Command Standard System, a system comprised of 460 applications.

The Navy has reduced by 50 percent the number of applications across 21 functional areas since 2003. And since 2008, the Navy has eliminated over 400 legacy networks. The Marine Corps has reduced its applications by approximately 30 percent just over the last year and a half.

The Air Force has taken an aggressive action, as well, and has reduced its IT budget request by \$100 million in 2012. Air Force Materiel Command headquarters has organized a Tiger Team committed to finding software application duplication and outdated systems that can be terminated with acceptable risk.

These efforts, coupled with their ongoing work to reform acquisition of information capabilities and consolidating our infrastructure, are delivering better results for the business operations that our warfighters depend on.

To continue our progress, an important part of moving forward is the infrastructure on which our business systems reside. We have developed an IT enterprise strategy and roadmap to optimize our DOD IT infrastructure. And we plan to continue reducing that infrastructure footprint, creating a joint enterprise, developing an enterprise identity management system, and reducing the number of data centers to drive our networks to enterprise solutions. With the roadmap, we are developing implementation plans to establish aggressive milestones to accomplish that goal.

We are actively working with OMB on the data center consolidation. To date, we made significant progress in that regard. We are working with the military departments, DISA, and other components. In fiscal year 1911, DOD closed over 50 data centers, and we plan to eliminate more than 125 data centers in fiscal year 1912.

Our focus on improving and designing an enterprise architecture and infrastructure will not only help DOD with migrating to enterprise solutions, but, more importantly, it will provide the Department with an improved ability to secure our information networks and our information and data. These efforts are key to transforming how we operate, how we acquire, and how we manage our IT investment in order to ensure efficiency, effectiveness, and security while still providing capability.

I welcome the support of the subcommittee and really look forward to working with you and other Members of Congress as we strive to meet the challenges of streamlining and improving our overall IT capability. Thank you for your interest in our efforts, and I would be glad to answer any questions as they come up.

Mr. LANKFORD. Thank you, as well.

[Prepared statement of Ms. Takai follows:]

Mr. Chairman and Members of the Subcommittee:

I am pleased to appear before the subcommittee today to discuss the findings of the Government Accountability Office report, "Departments of Defense and Energy Need to Address Potentially Duplicative Investments," and to review with you some of the Defense Department's policies, processes, and initiatives that we use to address the issues identified.

Introduction and Background

The Defense Department's information technology (IT) budget presents a unique challenge when compared with other Federal agencies' IT budgets not only in terms of its magnitude, constituting approximately one-half of the federal government's overall IT budget, but in its scope and complexity. The Department's FY13 IT budget request of approximately \$37 billion includes funding for desktop computers, tactical radios, identity management technology, human resource systems, commercial satellite communications, financial management systems, and much more. These investments support mission critical operations that must be delivered in both an office environment and at the tactical edge on the battlefield. The Department's IT environment is even more complex when one considers that these investments operate in over 6000 locations worldwide, support the unique needs and missions of the three Military Departments and over 40 Defense Agencies and Field Activities within the Department.

The GAO has highlighted 31 business-related DoD IT investments, which included contract management, personnel management, and logistics that they consider duplicative. As the GAO reports, the Department has taken action to address 27 of these investments, in part through processes I will describe below. The four remaining four systems are non-duplicative, and satisfy very different requirements in the human resource management functional area.

Department of Defense IT Investment Management

The Department's business IT systems are essential enablers of a broader set of integrated business operations, rather than ends unto themselves. The Department is approaching its business areas as a cross-functional, integrated enterprise comprised of a series of end-to-end processes, rather than as individual stove-piped organizations performing specific and oftentimes disconnected business functions. For example, paying our Service members on-time is a shared responsibility among numerous members of our enterprise, including human resources and financial professionals. Additionally, it is not an issue that can be addressed solely through new IT systems, but instead requires reform of our processes, governance, and policies.

The 2005 National Defense Authorization Act (NDAA) established the Department's defense business system investment management framework to address Congressional concern that the Department has continued to invest billions of dollars in systems that

were not integrated and failed to provide timely and reliable financial and business information for daily operations. In response to this legislation, the Department created the Defense Business Systems Management Committee (DBSMC) and five Investment Review Boards (IRBs) - the Human Resources Management IRB, the Real Property Infrastructure Lifecycle Management IRB, the Financial Management IRB, the Weapon Systems Lifecycle Management IRB, and the Materiel Supply and Support Management IRB.

Since that time, the IRBs and DBSMC have certified and approved hundreds of defense business system development/modernization investments worth billions of dollars. As the IRB / DBSMC governance process has matured, its ability to provide oversight has significantly advanced. It has improved the collection of data by which it makes decisions along with improvements to its cross-functional approach to portfolio management and use of performance management. It has also adapted to additional legislative requirements, such as Section 1072 of the National Defense Authorization Act for Fiscal Year 2010, which required the IRBs conduct reviews of investments Business Process Reengineering efforts.

Congress made additional changes to the IRB structure through Section 901 of the National Defense Authorization Act for Fiscal Year 2012. These changes include consolidating the five IRBs into a single IRB chaired by the Department's Deputy Chief Management Officer and expanding the scope of the IRBs to look at all of DoD's business systems, including those in sustainment, rather than just new or

modernizing systems. We thank Congress for these changes and believe that they are an important step forward in helping the Department accelerate the transition away from our legacy environment into our target business systems environment.

The Department has identified 15 essential end-to-end processes, such as Hire-to-Retire, in the human resource management functional area, and Procure-to-Pay, in the supply chain management area, that the DBSMC and IRBs are using to help make targeted investments in business IT capabilities and ensure those investments are interoperable, efficient and non-duplicative. These end-to-end processes, which are represented in the Department's Strategic Management Plan and Business Enterprise Architecture, are being used to identify the sub-processes, systems, data standards, performance measures and laws, regulations, and policies necessary to improve our business and drive better IT implementations. This more holistic understanding of our business will allow us to make more informed Enterprise-wide decisions.

We have already made progress in this area by focusing on process improvement first, and then ensuring the right tools and governance structures are in place. Our Business Enterprise Architecture is maturing and serves as a tool that guides our investment decisions as well as aligning the Department to common standards and approaches. Our investment management process, from our IRBs to the DBSMC that I mentioned earlier, provide us with the ability to ensure planned investments fit the target environment, align to the architecture, and have successfully undertaken business process reengineering. These efforts, coupled with our on-going work to reform

acquisition of information capabilities is delivering better results for the business operations our Warfighters depend upon.

Though these planning activities are critical to sustained long term success, they are not enough. The Department is using the end-to-end framework as a reference for rationalizing our current business IT investments, and ensuring each investment supports the Department's mission through enterprise architecture, the DoD business strategy. It is also being used to identify those investments that need to be terminated, integrated with another solution or sunset.

IT Modernization Efforts

In the summer of 2010, the Secretary of Defense directed a consolidation of IT to improve mission effectiveness and security while driving down costs. As a result of that direction, the DoD CIO developed the IT Enterprise Strategy and Roadmap. Our goal is to optimize our IT infrastructure by doing the following:

- Reduce DoD Footprint – Right Size Capacity
 - Networks / Servers / Data Centers / Applications
 - Simplify the ability to raise security
- Standardize to an Enterprise Level – Improve Combatant Command effectiveness
- Joint Infrastructure – Authorized Users can access authorized data

- Find People & Information – Enterprise User Identity Management
- Democratize Technology – drive DoD Networks toward Enterprise Solutions

In addition to the IT Enterprise Strategy and Roadmap, we are developing Implementation Plans to establish aggressive milestones for a series of specific actions with measurable goals and outcomes. For example, our near term focus is in the following areas:

- Data Center consolidation/virtualization
- Optimize/Reduce Number of Networks (NIPR/SIPR)
- Identity Management – secure authentication to network and data
- Enterprise Email – Single global directory service
- Commercial Hardware/Software Procurement
 - Leverage Department’s buying power

Additionally, we are working to resolve some of the cultural, structural, and other challenges in migrating to enterprise solutions. For example, we believe that the “Cloud First” strategy developed by the Office of Management and Budget (OMB) as part of the 25 Point Implementation Plan to Reform Federal Information Technology Management is a promising approach towards consolidating IT and reducing duplicative IT applications. We have developed a draft cloud strategy for the Department and will be working hard with the Military Departments, the Defense

Information Systems Agency (DISA), and other Components to implement cloud approaches and better optimize our IT infrastructure and applications.

Another significant initiative is the consolidation of data centers under the data center consolidation initiative as part of the 25-Point Implementation Plan. We have already made significant progress and have an aggressive time line to achieve further substantial reductions. As with our cloud efforts, we are working with the Military Departments, DISA, and other Components to eliminate unused capacity, drive up usage rates, and optimize our architectures and resources.

We are working all of these initiatives hard and expect to achieve remarkable success over time. We have already made substantial progress in improving effectiveness and lowering costs and we will continue to improve effectiveness and efficiency as these efforts mature and bear fruit.

I welcome the support of this Subcommittee and look forward to working with you and other members of Congress in the coming year as we strive to meet the challenges of streamlining and improving our IT infrastructure and rationalizing applications.

Thank you for this opportunity to share the Department's progress with you.

Mr. LANKFORD. Mr. Locatis?

STATEMENT OF MICHAEL W. LOCATIS, III

Mr. LOCATIS. Good morning, Chairman Lankford, Ranking Member Connolly, and other members of the subcommittee. Thank you for this opportunity to testify today on GAO's report on potentially duplicative IT investments.

The Department of Energy appreciates the work being performed by the GAO to identify opportunities to improve mission effectiveness and fiscal efficiency. The DOE is dedicated to improving our overall IT portfolio management and to address areas identified in the GAO report. We are committed to ensuring DOE's IT investments make efficient use of taxpayer dollars at all times.

As chief information officer for the DOE, one of my roles is to enable science, energy, and nuclear security missions through technology that provides tangible, positive outcomes. DOE is actively supporting and executing OMB's 25-point plan and other strategies championed by Vivek Kundra and now Steven VanRoekel. The Federal CIO community greatly appreciates their leadership and commitment to service. DOE is also supporting GSA by taking advantage of their sourcing and contract vehicles whenever we can and providing input to make them more usable wherever possible.

Upon my arrival 16 months ago, I conducted a 45-day assessment and identified many opportunities to improve effectiveness and efficiencies of our IT. Many of these opportunities stemmed from fragmentation and duplication. As a result, I partnered with our program offices and moved forward to change the way we do business. DOE has implemented an Information Management Governance Council that solidifies accountability in our senior officials and has already delivered tangible outcomes that have enabled us to maximize the return of our IT investments and reduce duplication.

In the areas of duplication, let me highlight three examples for you.

First is our Joint Cybersecurity Coordination Center, or JC3. There is nothing more important than our national security, and DOE needed to connect its cybersecurity resources more efficiently across the complex. We established the JC3 to take a collaborative approach to cyber information-sharing and analysis and instant response across DOE enterprise and more effectively leverage the technical expertise of our national laboratories. This has made our cyber programs stronger and consolidated a number of duplicative functions.

The second is our new virtual desktop infrastructure which consolidates applications deployed across thousands of desktop computers into a small number of servers that deliver productivity to virtually any end-user device, including thin clients, smart phones, and tablets. The virtual desktop infrastructure creates an environment that is energy-efficient, inherently more secure, and costs much less to maintain.

The third is unified communications and desktop videoconferencing. We are consolidating into a low-cost, common desktop videoconferencing solution that better connects our employees. By enabling employees through instant messaging, Web confer-

encing, and desktop videoconferencing, we are targeting millions of dollars in travel savings and creating new efficiencies through enhanced collaboration and productivity, even where travel would not have been previously required.

In conclusion, the GAO report has identified IT investment efficiency improvement opportunities for the DOE. I have just mentioned other areas in which we are aggressively breaking down silos and enabling the mission through technology across the Department.

Thank you for this opportunity to discuss the report's findings. Mr. Chairman, this concludes my statement, and I look forward to answering your questions.

Mr. LANKFORD. Thank you.

[prepared statement of Mr. Locatis follows:]

Statement of Michael W. Locatis, III

Chief Information Officer

U.S. Department of Energy

Before the

Subcommittee on Technology, Information Policy, Intergovernmental Relations and
Procurement Reform

of the

Committee on Oversight and Government Reform

U.S. House of Representatives

February 17, 2012

Good morning, Chairman Lankford, Ranking Member Connolly and other members of the Subcommittee. Thank you for this opportunity to testify today on the Government Accountability Office's (GAO) report on potentially duplicative IT investments. The Department of Energy (DOE) appreciates the work performed by the GAO to identify opportunities to improve mission effectiveness and fiscal efficiency. The DOE is dedicated to improving our overall IT portfolio management and to address areas identified in the GAO report. We are committed to ensuring DOE's IT investments make efficient use of taxpayer dollars at all times.

Background

In August 2011, the GAO began a multi-agency review to identify potentially duplicative IT investments. At DOE, GAO's report identified 6 potentially duplicative IT investments in two different areas:

- Back-end Infrastructure
- Electronic Records and Document Management.

Department of Energy Response

As the Chief Information Officer (CIO) for the DOE, one of my roles is to bring our science, energy, and nuclear security program offices together with internal and external IT resources and capabilities to promote agency-wide innovation and efficient operations that add value to DOE's activities and provide tangible, positive outcomes for the nation.

Over the past 16 months, DOE has established a strong, mission-focused IT and cybersecurity governance framework to manage DOE's IT portfolio. Our governance process is led by the Information Management Governance Council (IMGC), which is comprised of our three Undersecretaries, representing the primary DOE missions of energy, science, and nuclear security, and me, the CIO, representing the technology enablers. The IMGC is advised by the Chief Health, Safety and Security Officer, the Director of Intelligence and Counterintelligence and a select group of National Lab CIOs. The IMGC develops strategy and policy for the effective management of IT across DOE and provides oversight of the implementation.

Complimentary to this, we have executive management and subject matter expert working groups to formulate policies and effectively manage our federal IT portfolio on a day-to-day basis. Through our governance process and our close partnerships with mission program offices

we can ensure that we effectively and efficiently meet the mission needs of the Department. To monitor performance of our IT investments, we have strengthened our investment review processes, including our annual IT portfolio reviews, Quarterly Investment Control Reviews, and monthly IT Dashboard reporting, all of which support senior management decision-making and enhance IT oversight. These processes enable a solid foundation for effectively transforming the IT portfolio throughout the Department.

DOE is actively supporting and executing the Office of Management and Budget's (OMB) *25 Point Implementation Plan to Reform Federal IT Management*¹ as part of our broader IT management effort, and as a key enabler to ensure mission success.

In particular, DOE has implemented technical status reviews, or TechStats, to assess potentially troubled IT investments and, in a collaborative manner, turnaround underperforming investments and make them successful. For example, we reviewed the Office of Energy Efficiency and Renewable Energy's (EERE) State Grant Administration investment. As a result of implementing recommendations from the TechStat, the Department saved approximately \$1 million and the investment is back on track in both cost and schedule and is rated green on DOE's IT Dashboard. We subsequently modified the approach of our TechStats to include a more strategic look at investments. In 2011, my office led three strategic TechStat reviews on Identity, Credential, and Access Management (ICAM); Public Key Infrastructure; and Commodity IT. As a result of these reviews, the Department developed new policies, procedures and governance processes to effectively manage the coordination and delivery of each of the three initiatives. Specifically, we developed a new Department-wide PKI strategy that projects

¹ OMB, *25 Point Implementation Plan to Reform Federal IT Management*

to save \$1 million annually by migrating PKI to a shared service provider. In addition, the Office of the CIO has established partnership initiatives with DOE organizations to both improve services and reduce costs and duplication of Departmental infrastructure. As part of our commitment to transparency, we included participation from the staff of the Senate Homeland Security and Governmental Affairs Committee (HSGAC), GAO, and OMB's E-Gov office in our recent commodity IT reviews.

I will now summarize the specific actions we are taking to address each of the areas identified by GAO in the report: Back-end Infrastructure and Electronic Records and Document Management.

Back-end Infrastructure

Because the Identity Credential and Management (ICAM) requirements needed to be implemented at multiple locations-- Chicago, Oak Ridge, and Washington, DC Headquarters, we determined that there was a need for separate investments in the local hardware and software costs associated with the deployment of the technology. These costs could not be avoided or reduced by consolidation given their diverse locations. The three investments were listed separately in the Department's IT budget. This was done not to report them as separate and distinct investments but rather to show separate budget line items where funding was being distributed to different locations to implement the infrastructure. The Office of Science is initiating the Science IT Initiatives Working Group, a group that will meet regularly with key stakeholders to ensure the oversight of infrastructure, consolidating where needed and establishing a governance process.

Electronic Records and Document Management

With regard to records management, DOE has undertaken a comprehensive approach to records management revitalization that is examining everything from policy and governance to records management applications for electronic records. The objectives of our efforts include:

- *Implement updated policy and guidance.* DOE recently updated its principal records management directive to provide better and clearer guidance on the management of electronic records, including e-mail. We are also revising our vital records, policy and updating our web-based tools that include:
 - Establishing a records management information sharing environment by leveraging Microsoft SharePoint 2010 to provide collaboration opportunities; announcements; calendar of related events; links to records management information and resources; and stakeholder contact information;
 - Annual records management training for all DOE employees (including contractors) via DOE's electronic Online Learning Center's web-site. DOE will deploy this in FY12 by leveraging the National Archives and Records Administration's (NARA) general training package entitled "*Records Management for Everyone*". This training was created as a shared service for federal agencies to meet their annual regulatory training requirement and is a free tool; and
 - Additional program-specific records management training for DOE records management program officials, field officers, records liaisons and various records management community members via webinar and video teleconferencing.
- *Create a records management community of practice.* DOE is taking a more collaborative approach to identifying records management issues and solutions, including best practices. We formed a working group comprised of records management personnel

from across the Department to identify common obstacles and issues, and to work with IT professionals to recommend solutions.

Finally, our strategy for electronic records management is to identify records management applications that can serve Department-wide needs. This approach will reduce cost and duplication and promote shared services, but still support the diverse DOE program missions and their associated records requirements. The records management investments cited in GAO's report are existing systems that will remain in place while the Departmental strategy is being implemented. A decision on these investments will be made once the approved Departmental-wide applications are identified.

Conclusion

In conclusion, the GAO report has identified IT investment efficiency improvement opportunities for the DOE. We will address these in addition to our broader, ongoing efforts to improve the effectiveness and efficiency of our IT portfolio.

Thank you for this opportunity to discuss the report's findings. Mr. Chairman, this concludes my statement and I look forward to answering your questions.

Mr. LANKFORD. Mr. Spires?

STATEMENT OF RICHARD SPIRES

Mr. SPIRES. Chairman Lankford, Ranking Member Connolly, thank you, and good morning. Today I will discuss efforts at the Department of Homeland Security to reduce duplicative IT investments.

The key for an agency to eliminate system duplication is to develop an environment at the senior executive level that: one, enables a group of executives representing all appropriate organizations to work collaboratively to understand agency needs in a particular mission or business area; two, completes a comprehensive analysis in the mission or business area to identify ways to improve both effectiveness and efficiency across the enterprise; and, three, has a decisionmaking process in which those same executives can effectively drive change based on the analysis.

I have found both in government and the private sector that if you can create these conditions, over time executives will be able to make the hard decisions on the tradeoffs and compromises necessary for the good of the enterprise. I use the term "strategic alignment" to reflect what is necessary for success. In my experience, the best way to achieve such alignment is through strong enterprise and portfolio governance buttressed by segment enterprise architecture.

Enterprise governance provides large organizations with the ability to effectively make informed decisions that involve stakeholders across the enterprise. In smaller organizations, it is possible to execute enterprise governance with one governance body that represents top leadership. But in larger and more complex organizations, we need to break the challenge down into what we call portfolios, or logical partitions, that can support various elements of an organization's mission and business outcomes.

Portfolios should typically represent functional groupings that can drive improvements to mission and business effectiveness. At DHS, we are working to implement 13 functionally oriented portfolios, to include mission support functions such as include screening and incident response, along with business functions such as finance.

So how does this work? Each portfolio has a governance board of appropriate senior executives that look over a multiyear planning horizon and define a set of measurable stretch objectives that would significantly improve mission or business effectiveness. To achieve those objectives, the portfolio governance board must establish capabilities that are required to meet such objectives.

For instance, in a human resource portfolio, a capability may be to have an automated end-to-end tracking of all steps in a hiring process, with the objective to reduce the average time to hire by 50 percent. Once the objectives and capabilities are set, the board works with subject-matter experts to define the business process changes, IT system changes, elimination of redundant systems, and other appropriate program changes to achieve a goal end state. Once that goal end state is defined, the board sets a transition strategy that defines the step-by-step process to go from the current or as-is state to the goal or desired state.

The approach outlined above applies the generally accepted Federal Segment and applies Architecture methodology to a portfolio.

At DHS, we are working to implement portfolios to drive and improve mission effectiveness while eliminating duplication. For instance, a comprehensive HR system inventory revealed 124 systems, including many duplicative systems. We established an HR IT portfolio governance board and recently completed our Human Capital Segment Architecture, which will effectively shift a large number of these component-based systems and services to enterprise or Federal Government solutions.

Likewise, we identified more than 20 separate common operating picture systems supporting the situational awareness needs of the Homeland Security mission. Leveraging a portfolio approach, this month our National Operations Center will stand up an upgraded version of the DHS common operating picture that incorporates all components requirements. The plan is then to roll out the new common operating picture to DHS operations centers across the enterprise over the next year, eliminating numerous duplicative common operating picture investments.

It takes about 3 years of hard work for a portfolio governance approach to mature to the point where the portfolio has a solid set of business objectives and measures, a defined goal end state, and a viable enterprise transition strategy. Despite the difficulties, the benefit of this work can be tremendous.

These methods can and should support implementation of the Shared First initiative aimed at routing out waste and duplication across the Federal IT portfolio.

Thank you, and I look forward to taking your questions.

[Prepared statement of Mr. Spires follows:]

**TESTIMONY OF
Richard A. Spires
Chief Information Officer
U.S. Department of Homeland Security
Before the
House Committee on Oversight and Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations, and
Procurement Reform
February 17, 2012**

Chairman Lankford, Ranking Member Connolly, and Members of the Subcommittee, thank you and good morning. Today, I will discuss efforts at the Department of Homeland Security (DHS) to reduce duplicative information technology (IT) investments. As detailed in GAO Public Report, GAO-12-241, *Departments of Defense and Energy Need to Address Potentially Duplicative Investments*, duplicative IT systems exist throughout the Federal Government. By their nature, duplicative IT systems are inefficient; they increase costs, prevent standardization, limit collaboration, and inhibit information sharing among and across the Federal Enterprise. Reducing duplicative IT systems is critical for the efficient operation of our Government, and I am grateful to have the opportunity to testify before you today. I have had the good fortune of being involved in large-scale IT organizations and programs for 25 years in both the public and private sector. Though I see and learn new things in this business every day, the successes and failures I have witnessed throughout my career have helped forge the strong beliefs I hold concerning how to effectively leverage IT to support the mission and business needs of a large organization.

Systems Duplication at DHS and in the Federal Government

The nature of DHS's creation has led to the existence of duplicative systems which we are trying to reduce and consolidate as the Department matures. As the department's architects worked to merge a number of different federal agencies and unite 22 DHS components, legacy systems were patched together to support the five DHS mission areas and address critical business process needs. We stood up DHS very quickly, and, out of necessity, we merged and modified available systems to get the information we needed and the work done.

Looking beyond DHS, there are two main reasons why duplicative systems exist in departments and agencies, and why consolidation of these systems is so difficult. The first reflects a basic human dynamic within organizations. Over time, people seek to optimize their business processes to deliver their specific services or products. These specialized business processes lead organizations to believe they have "unique" requirements that require dedicated, customized solutions to continue meeting needs. Left unchecked, such specialization leads to the creation of unique requirements in even traditional "back office" functions like finance, human resources, and administration.

Beginning in the 1970s, revolutions in technological capabilities led to the development of IT solutions that could standardize and automate mission and business functions. Eager to leverage rapidly modernizing capabilities, government executives developed and deployed IT systems to address their business needs, customizing these systems to meet specific and often unique business needs. However, by the late 1990s, the Federal Government realized that there were significant inefficiencies in allowing each agency to handle IT in this way, and Congress passed

the Clinger-Cohen Act in 1996, followed by the E-Gov Act in 2002. These laws created and were meant to empower an agency Chief Information Officer (CIO) to develop a strong centralized IT capability and to drive efficiencies and effectiveness in providing IT to support agency mission and business needs. The reason duplicative systems remain a decade later is the second reason agencies struggle to eliminate duplication – CIOs and their IT organizations are just one of a number of stakeholders who must concur in order to implement change. The evidence of this is recently documented in a report by GAO entitled, “*Federal Chief Information Officers – Opportunities Exist to Improve Role in Information Technology Management.*” Without an active partnership of CIOs, senior department or agency leaders, and other key stakeholders, the natural inclination of organizations is to drive to unique requirements, making it very difficult to eliminate system duplication.

Enterprise and Portfolio Governance Critical to Success

CIOs are responsible for driving the efficient use of IT in their department or agency. Clearly identifying and eliminating duplicative IT systems is a key component to driving efficiencies in the use of IT. Unfortunately, as CIOs, we cannot just mandate the elimination of these duplicative systems. An effective CIO must find a way to drive the change required to remove duplication in agencies and overcome the desire to maintain the status quo. The key is to develop an environment at the senior executive level that: 1) enables a group of executives representing all appropriate organizations to work collaboratively to understand agency needs in a particular mission or business area; 2) completes a comprehensive analysis in the mission or business area to identify ways to improve both effectiveness and efficiency across the enterprise; and 3) has a decision-making process in which those same executives can effectively drive

change based on the analysis. I have found both in government and the private sector that if you can create these conditions, over time executives will be able to make the hard decisions on the trade-offs and compromises necessary for the good of the enterprise, even if it is not optimal for their own organization. I use the term “strategic alignment” to reflect what is necessary for success. In my experience, the best way to achieve such alignment is through strong enterprise and portfolio governance buttressed by segment enterprise architecture.

Enterprise governance provides large organizations with the ability to effectively make informed decisions that involve stakeholders across the enterprise. The objective is simple: to have key executives across the enterprise determine the optimal allocation of capabilities and resources across programs to best support the achievement of mission and business outcomes. In mature organizations, enterprise governance regularly brings together senior leadership to decide which new capabilities best support the mission and then prioritize them for development and fielding. Effective enterprise governance is integral to the planning cycle before the launch of a new program (or the elimination of an existing system to reduce duplication), providing clear direction and stated outcomes in support of a program’s execution. Mature enterprise governance is focused on all capabilities to produce mission and business outcomes, and, as such, enterprise governance is not specific to just IT or IT programs.

In smaller organizations, it is possible to execute enterprise governance with one governance body that represents top leadership. But, in larger and more complex organizations, it becomes daunting for the top leadership to deal with all programs and program allocation decisions.

Portfolio governance provides the scale necessary for leadership to deal with decisions in large organizations. We break the challenge down into what we call “portfolios,” or logical partitions, that can support various elements of an organization’s mission and business outcomes.

Portfolios may be defined based on the organizational structure of an agency, but, in many instances, the better approach is to have portfolios represent functional groupings that can drive improvements to mission and business effectiveness. The approach to defining a set of portfolios for an organization is unique to that organization’s structure and mission.

For example, DHS has more than 200,000 employees organized into seven large operating components (e.g., U.S. Coast Guard, FEMA, and TSA) along with several other smaller offices and components. A number of these components support similar functions, such as incident response handling (FEMA and the Coast Guard), or the screening of individuals (TSA, CBP, USCIS, ICE, and the Coast Guard). As the DHS Under Secretary for Management has testified, we are implementing a strategy to increase the Department’s effectiveness in fulfilling our missions and business by integrating and aligning functional areas at both the Department and Component levels. In particular, we are working to implement 13 functionally-oriented portfolios to include mission support functions (e.g., securing, screening, and incident response) and business functions (e.g., finance and human resources).

At DHS, it was important that we defined the portfolios functionally to drive cross-component integration since the systems duplication here is a byproduct of our organizational structure. By

defining and analyzing our portfolios along functions, we can more effectively identify and address duplication and redundancy in both business processes and in systems.

In my experience, the most effective model is to create a Portfolio Governance Board for each portfolio. Just like enterprise governance boards, key executives must actively participate in portfolio governance boards. For example, a financial portfolio board would typically be chaired by the CFO as the business executive owner and include an IT executive as a member, along with other executives from closely integrated user communities such as security, procurement, and asset management. Other members of the board may include executives from operating and planning organizations.

Segment Enterprise Architecture Leading to Transformation

So what do these portfolio governance boards do and how can they get it done? Each board looks over a multi-year planning horizon and defines a set of measurable stretch objectives that would significantly improve mission or business effectiveness. Measurable objectives could include items such as reductions in response or service times, customer satisfaction survey scores, or cost efficiencies through elimination of duplicative systems. To achieve those objectives, the portfolio governance board must establish capabilities that are required to meet such objectives. For instance, in a human resource portfolio, a capability may be to have automated end-to-end tracking of all steps in the hiring process, with the objective to reduce the average time to hire by 50%. Once the objectives and capabilities are set, the hard part is defining a goal end state that will meet those objectives for that portfolio. This goal end state

could include business process changes, IT system change, elimination of redundant systems, and other appropriate program changes. To do this work, I recommend the portfolio board be supported by subject matter experts (e.g., finance experts who support the finance governance board) along with the Enterprise Architecture (EA) organization. These specialists, along with EA, provide significant analysis support in defining and analyzing alternatives, along with providing knowledge of the current state. Once a goal state is defined, the board sets a transition strategy that defines the step-by-step process to go from the current, or “as-is,” state to the goal, or “desired,” state. The transition strategy will allocate the capabilities that have been defined to programs for their implementation. If done properly, this transition strategy also serves as the underpinning by which a portfolio governance board can present a cogent budget request that shows how the investments in programs support achieving the goal state.

The approach outlined above applies the generally accepted Federal Segment Architecture Methodology to a portfolio. By applying this methodology and leveraging a robust governance model, we can look across portfolios to identify capabilities and gaps across the enterprise. This is the essence of portfolio governance – to support the strategic goals and objectives of the department or agency and maximize enterprise outcomes while minimizing duplication across systems and investments both within individual portfolios and across portfolios. Portfolio governance also enables a department or agency to identify strategic gaps in mission and business areas and identify the investments required to fill those gaps. The process includes all stakeholders and a governance model to bridge the gap between the “want” and the “need.”

Having implemented such enterprise and portfolio governance in the private sector, the IRS, and now working to mature it at DHS, I know firsthand how difficult this process can be. It takes about three years for a portfolio governance approach to mature to the point where the portfolio has a solid set of business objectives and measures, a defined goal end state, and a viable enterprise transition strategy. This approach cannot be treated as a budget exercise in which you gather people once a year to do analysis. The boards and support organizations must persist, with boards meeting at least every quarter, and typically more often during the first two years upon the standup of a portfolio. Even when mature, the capabilities and end state must be reassessed annually based on changing priorities and realities. The board will then move the planning cycle out by one year, make adjustments to the end-state, and readjust the transition plan. Despite the difficulties, the benefit of this work can be tremendous. It has given me great pride to be associated with organizations that have solid strategies and transition plans. Even in times of significant turbulence, the leadership has sound analysis by which to assess its options and adjust, while still being able to keep its long-term objectives in mind.

DHS Example – Human Resources IT Consolidation Drives Transformation

Recently, DHS reached a milestone in the effort to implement functionally-oriented portfolios for mission-support and business functions: completion of our Human Capital Segment Architecture (HCSA), which will be our model for conducting segment enterprise architectures going forward. HCSA promises to guide real and lasting transformation in our human capital organization.

The HCSA was not an academic exercise but a practical, executable way forward that combines both strategic and tactical approaches. Our first business-driven segment architecture, the HCSA, got underway in November 2010. The project involved a core team of DHS component representatives and enterprise architecture experts from the Office of the CIO working collaboratively with the Chief Human Capital Office (CHCO) planning team to provide project leadership and analysis. Oversight of the HCSA project came from the Human Resources Information Technology Executive Steering Committee (HRIT ESC), a portfolio governance board of human capital and IT executive representatives from every DHS component.

The HCSA effort conducted an in-depth analysis, formulated recommendations for executive review, and ultimately created a plan of action to guide DHS HRIT investments and human capital business processes for the next five years. The plan identifies several near-term efficiencies, as well as critical longer-term improvements to fill automation gaps and reduce redundancy.

Outcomes from this project were not exclusive to technology. The HCSA also took an in-depth look at key business processes that, when combined with enabling technologies, represent the way work is done today. The plan of action cites as many improvement opportunities in business processes as it does in technology. And, for the first time, the vision for human capital is shared across all DHS components. The HRIT Strategic Plan, created as an outcome from this effort, reflects the goals and objectives that will guide the department's HRIT investments over the next five years.

One of HCSA's key outcomes was a first-ever enterprise view of the current state of human capital people, processes, technology, and data. A comprehensive HRIT system inventory revealed 124 HRIT systems at DHS, including many duplicative systems and applications across the enterprise. As an example, DHS currently maintains nine different Learning Management Systems (LMS). The HCSA plan of action will effectively shift a large number of these component-based systems and services to enterprise or Federal Government solutions, reducing redundancy and driving cost savings.

To maintain the momentum of the HCSA effort, we took actions to continue to mature the overall governance process as the HCSA neared completion. The department's HRIT ESC, which reviewed every stage of the HCSA, will continue to make final decisions on HRIT investments and hold components accountable for their role in the transformation. Commitment, accountability, and diligence will be required: from executives to make decisions, from HR and IT subject matter experts to collaborate on transformational projects, and from all organizations to operate within the governance guidelines established and execute on the agreed upon plan of action.

The HCSA has been a watershed for expanding HR and IT communication channels between the department and components. Never before have the department's HR and IT communities worked together so closely for such an extended period of time. The long-term impact of this level of close collaboration on the department's function cannot be overstated. More than 80 DHS employees, including a core team of HR and IT thought leaders from every component,

met regularly to validate analysis, share ideas, and explain their systems, making possible a giant leap forward in aligning and coordinating activity between HR and IT across DHS.

DHS Example - Common Operating Picture Technologies Help in Incident Management

Common Operating Picture (COP) systems are critical for supporting the situational awareness needs of the homeland security mission. Through our portfolio review process, we identified more than 20 different COP investments, most of which were largely uncoordinated, stand-alone investments. To establish governance in this area, we reached out to the National Operation Center (NOC), the DHS component responsible for situation awareness. The NOC has primary responsibility for serving as the nation's homeland security nerve center for information collection and sharing.

DHS now has an effective COP Governance Board chaired by the Director of the NOC. The COP governance board has been operating for about nine months. Under the Director's leadership, all DHS components with COP investments, as well representatives from the DHS Office of Policy, actively participate in activities designed to bring these diverse investments together.

The unity of effort is already producing significant outcomes in the short time the COP governance board has been operating. We have documented more than 1,000 sources of trusted and authoritative data sets used for the homeland security mission. Those engaged in the use of

COP technologies can now rapidly find many key sources of data, enabling them to be more efficient in supporting the mission and avoiding duplication of effort.

As a direct result of the work done by the COP governance board, FEMA provided critical data and technologies to support the NOC during the response to Hurricane Irene. Further supporting the operational mission, the NOC will stand up a new version of the DHS COP later this month. The new DHS COP includes key updates informed by the requirements defined by the COP governance board. The plan is to roll out the new COP to DHS operation centers across the enterprise over the next year, eliminating numerous duplicative COP investments.

In addition to internal coordination, the COP governance board also coordinates with the Federal Geographic Data Committee on the standup of the Federal GeoPlatform. The goal is to assess how this potential shared service can support portions of our unclassified missions and provide solutions for government-to-citizen services. As a result of the efforts of the COP governance board, today we are better able to share information across the department and with homeland security stakeholders more effectively.

Conclusion

This Administration, under the leadership of Federal Government CIO Steve VanRoekel, recently announced a “Shared First” initiative aimed at rooting out waste and duplication across the Federal IT portfolio. Government agencies must identify and eliminate duplicative IT

systems as part of an overall strategy to enhance efficiencies and drive more effective operations. As I have highlighted, DHS has taken many steps to lead this effort to increase the effectiveness and efficiency of the Department's systems. A collaborative, analysis-based approach that leverages the implementation of robust enterprise governance, cross-enterprise portfolio governance, together with segment enterprise architecture, is imperative to ensuring IT efficiently and effectively supports the mission and business functions of a government agency. A positive byproduct of this work is the identification and eventual elimination of duplicative IT systems. These methods can support implementation of "Shared First," and they should be used throughout the Federal Government to drive real improvements in effectiveness and efficiency in government operations and services.

Thank you.

Mr. LANKFORD. I thank all of our witnesses for testifying today. Let me recognize myself for 5 minutes, and let's have some conversation on this as well.

I have a couple thoughts here. One is, Mr. Powner, you mentioned the Dashboard at this point. What I would like to know, for all of you that have integrated with that as well, has that been helpful, and what is missing from that? Is there a next level for that use in the Dashboard, and is it a helpful tool?

So anyone can jump in and be able to respond to that.

Ms. TAKAI. Well, let me start, and I am sure my colleagues have the same view.

We have found the Dashboard process to be very, very helpful. It does really—I think it really, in many ways, takes the OMB desire for transparency and really gives us the opportunity to be able to put priority on that Dashboard process. So it does give the kind of transparency that we all need, but it also gives it at a higher level, which I think is helpful.

In terms of going forward, I think our major challenge is to make sure that we are taking the best advantage of that Dashboard process internally, to make sure that we are driving the kind of process change that is needed.

Mr. LANKFORD. Not every agency is engaged in that; is that correct, Mr. Powner?

Mr. POWNER. Yeah, I think—a couple things. I think the improved transparency is very important from an oversight perspective, whether you are at OMB, if you are an agency, or if you are in the Congress. The one thing that the Dashboard did is I think it greatly increased CIO accountability. What it says is, for all major investments—there are 800 of them across the major departments—is the CIO is ultimately accountable. So Ms. Takai has her pictures next to her 72 major investments. That actually was a good thing for some agencies where we needed more CIO accountability. It was very helpful moving forward.

Mr. LANKFORD. The issue is, is the number right? Are there other projects that need to be there? Obviously, not every agency has not that large of an investment. Ms. Takai has very large, complicated, numerous projects on it. Should that work its way down to other agencies and say, okay, this is large for your agency, instead of setting a single standard for every agency?

Mr. POWNER. Well, there are 7,200 investments, so there are 800 major and the rest are non-major. I think over time, as the Dashboard matures, it would be helpful to get insights into those non-majors. But, again, we probably ought to do that in a step-wise fashion to get the majors correct first.

Mr. LANKFORD. Sure. But the question is, what is “major” to the Federal Government or what is “major” to your agency, if there a difference there. You can look at each agency and say, you know, I know you don't reach this level, but give us your five largest, most significant projects that are on there, whatever dollar amount that is, and those are your majors.

Mr. POWNER. No, that is an excellent point. It does differ. And, in fact, several non-majors at DOD would clearly be majors at other agencies.

Mr. LANKFORD. Right.

Ms. Takai, where you going to mention something as well?

Ms. TAKAI. I would like to add to Mr. Powner's comments, that the visibility and transparency is important, not only for us as CIOs, but actually what we would view as more important is the visibility to the business process owners and the business process changes that really have to happen for any IT implementation to be successful.

The success of these large-scale business systems are really more around, can we change the processes and can we actually make the business changes that we need, the necessarily just being dictated by the dynamics of the technology implementation. And the Dashboard really brings the opportunity for us to have the dialog at a much different level than if it were just delegated to being a technology discussion.

Mr. LANKFORD. Okay. We may have some other time for other questions as we go from here. Let me address one thing with DHS, because I have a lot of very positive things and just ideas I want to get a chance to kick around.

DHS had the Secure Border Initiative network. I know that is a long-term—that is not your favorite project to talk about because it was this long-term project that ended up spending a billion dollars and then getting folded down and saying, "This didn't work," on it.

That is something every agency deals with, to experiment, to try. Technology is always going to be out on the leading edge of saying, how can we accomplish that. The issue is, how can you—how do we integrate—well, let me rephrase it a couple ways. One is, it is integrating off-the-shelf technology, commodity IT stuff, when it is appropriate. And the second one is, how do we anticipate through our process of going through contracting to try to find areas saying, "This is outside of our expertise," and so we don't end up with a dead-end and a billion-dollar debt and we don't have anything at the end.

So, two separate projects: integrating the commodity IT stuff, where appropriate; and the second one is, how do head off a dead-end before we get there?

Mr. SPIRES. That is a great example, sir, to bring up, SBI-net. There were a lot of things that DHS did wrong early on that program.

I would like to say, in the follow-on of what we are doing—because the concept of fixed towers with the kinds of surveillance equipment on those towers to monitor the southwest border is still a concept that the Border Patrol within CBP really wants. And so we are actually moving forward with a new program, but we are using, as you say, commodity—just not IT, but commodity technologies. And, in fact, we are about ready to go out with a request for proposal to the industry based on market research we have done, okay, in order to procure what we are calling "non-developmental solutions," meaning solutions that already exist somewhere in the world, to be able to do this kind of surveillance work.

I think that is where the government really needs to look. How is it that we can leverage things that already exist within industry or within other governments or within other agencies rather than,

to your point, rather than going out and trying to build things custom? And I believe this is a good example.

And I have worked closely with Mr. Mark Borkowski on this, who is the program manager of that new initiative. And we were both aligned, if we go with that RFP and we get something that is developmental in nature in any way, we are just not going to award. We are only going to award if it is truly non-developmental, that exists somewhere, and that you can just field this thing. All right? And that I think is more what we need to do as a government.

And we need to have the discipline, though, to make sure that we have the requirements approach. When we work with the business owners, we have to work with them in such a way—and this is part of good governance—so that they understand it is much better for them to perhaps give a bit on their requirements, okay, get 80 percent of the solution that is off the shelf, rather than requiring us to try to build that additional 20 percent custom. If you start with the 80 percent solution that is off the shelf and then work with the vendor community for existing products over time for them to upgrade their products to address more and more of our requirements, that is a much less costly and it is a much less risky approach to delivering IT.

Mr. LANKFORD. Okay. Thank—

Mr. SPIRES. Hopefully I have gotten to—

Mr. LANKFORD. No, that is great. We are working on solutions on that.

Let me recognize Mr. Connolly.

Mr. CONNOLLY. Thank you, Mr. Chairman.

And immediately after this round of questioning, I am going to have to leave to go to the floor. We are going to be voting shortly. We have 1 hour of debate, and then we are going to vote.

Welcome all, to the panel.

And, Mr. Chairman, let me respectfully invite you again to consider H.R. 1713, the Federal Cost Reduction Act I introduced a number of months ago, to try to codify what Vivek Kundra started in terms of the data center consolidation and to ensure taxpayer savings with that consolidation. And I would love to have your co-sponsorship, but certainly I think it might be timely after this hearing to hold a hearing on that, if you would.

And, again, I want to thank you all for being here.

Mr. POWNER, how do you feel the data center consolidation, the closure and consolidation, is going? And what is your estimate of, in a sense, the utility savings—because I gather that is the lion's share of the savings from these consolidations—what we might expect to achieve with it?

Mr. POWNER. Well, we have had a good start on data center consolidation. And I know Mr. Spires chairs a committee that, governmentwide, that looks at this.

A couple key things that our work has shown—and we have done several reviews of the data center inventories and plans. One, we need to ensure that we are capturing all the inventory out there and then have solid plans for consolidation. And the numbers are fine, Ranking Member Connolly, where we have X number of cen-

ters that we closed to date, so that is good progress and we have good goal of a thousand centers by 2015.

But, ultimately, it is about saving money. So we really need to look at those plans in terms of when can we start seeing the dollar savings through those consolidation efforts. And that is something that we are currently reviewing for the Congress when we are looking at those detailed consolidation plans.

So, good start, but we still need to see—the ultimate measure is a reduction in costs associated with these centers and more efficiencies going forward.

Mr. CONNOLLY. Right, because the efficiency and the cost savings was sort of the name of the game.

Mr. POWNER. That is right.

Mr. CONNOLLY. Do you believe we can build on that? The last time we had Vivek Kundra here, which was the swan song before this committee, he actually expressed some enthusiasm for this bill I referred to and actually agreed that we could do more as we move out to the future. Your sense of that?

Mr. POWNER. Clearly, we need to do more. I think the IT Reform Plan, which data center consolidation is front and center, there were very clear deliverables 6, 12, and 18 months. But if you look at the data center consolidation initiative, that is a long-term initiative. That will go beyond 18 months, and we need to keep the momentum beyond 18 months.

I commend the administration for the stretch goals on the 6, 12, and 18 months, but we need to have a plan that would go beyond 18 to truly achieve those cost efficiencies.

Mr. CONNOLLY. Yeah. Which I think means more ambitious numbers in terms of consolidation than even originally envisioned in the 25-point plan, would you agree?

Mr. POWNER. Yeah, I actually think if we would hit that 1,000 center reduction mark we would see some great efficiencies with that.

Mr. CONNOLLY. And let me start with you, too, but invite your colleagues to comment. Cloud computing. It is estimated that—well, it is an inevitable part of the Federal future. The question is, how much, how fast, and how secure. And there are also some liability/legal questions depending on where the cloud is located, what company is registered, in what country, how our data and how other laws affect us.

But assuming all of that, what is your sense of where we are headed in cloud computing for our Federal agencies? And what concerns might you have from a legislative point of view, cybersecurity for example, that ought to be on our plate?

Mr. POWNER. So, a couple things with cloud computing. Similar to data center consolidation, I mean, their efforts—the IT Reform Plan calls for the major departments and agencies to consolidate three services to the cloud. That is a good start. Again, we want to consolidate those services. I think Mr. Locatis has a number of initiatives looking at commodity IT where he is looking at this. Ultimately, it is about cost savings, when it is all said and done. It is not about three.

From a security perspective, a couple key things. If there are great security concerns, you can start with private clouds over pub-

lic clouds. I know Mr. Spires has a number of initiatives where he is focused more on the private clouds, where you can put your security requirements in. Some of the initiatives at GSA with FedRAMP, that will clearly help.

I do think security needs to be front and center when we move to the cloud, but between FedRAMP and some of those initiatives or considering the private clouds, you can address those security concerns and still move to the cloud.

Mr. CONNOLLY. Mr. Locatis?

Mr. LOCATIS. Yes, we—

Mr. CONNOLLY. Could you speak up?

Mr. LOCATIS. Oh, absolutely.

We see this now as an opportunity for the data center consolidation effort to intersect the cloud offerings that are being offered by the private sector, private cloud offerings that can be FISMA-certified. And so, in our first round of data center consolidation, we closed three data centers. We will have another two data centers—we don't have the size that the Department of Defense has, but we are aggressively approaching that. And we have saved approximately \$7 million through those data center closures.

But now in our next round of planning, this is where we are looking at infrastructure as a service and working with the private sector through the security issues that you discussed to break through, working very closely with GSA on their sourcing capabilities, contracts, procurements, the FedRAMP and FISMA processes.

Mr. SPIRES. I might add, sir, that we at DHS are taking a very aggressive approach to the cloud. As Mr. Powner noted, we have private cloud capability within our two enterprise data centers, which is our target for all of our consolidation initiatives, so that ties to what Mr. Locatis said as well.

The next is between data center consolidation and leveraging cloud services, particularly for commodity IT. We are rolling out nine different cloud offerings in our private cloud, including such things as email as a service, development and test as a service, infrastructure as a service—very aggressive.

On the public cloud side, we are going more slowly because of the security concerns at this point. We are moving our public-facing Web sites to the public cloud, however, because it is non-sensitive data, and then we are going to assess. As FedRAMP matures and we see that the public cloud service providers begin to meet FISMA low and moderate capabilities, I think you are going to see a much more aggressive approach by ourselves and by other agencies over the next 2 to 3 years.

Mr. CONNOLLY. I am actually—Mr. Chairman, I know I am over my time—but I am glad to hear that. My own feeling is that, actually, though it may see counterintuitive to us in the public sector, frankly security may be better in the private sector, because they live or die on their reputation and on their protection of data and on taking care of clients.

And sometimes in the public sector, you know, we may have a bad moment in terms of a compromise, a cybersecurity compromise. The consequences are—you know, perhaps it affects your promotion, but, I mean, it is—you know, whereas in the private sector, literally you can go out of business if you screw up.

And so I think there may be some advantages in the private sector, and I think the approach you have outlined makes a lot of sense.

Thank you, Mr. Chairman.

Mr. LANKFORD. Thank you.

Mr. Walberg?

Mr. WALBERG. Thank you, Mr. Chairman.

And I appreciate the ranking member's questions on that area and you giving latitude to continue that process, because that was a concern that I wanted to hear about, as well. And I appreciate, Mr. Spires, your response specifically as we look at security issues across the spectrum.

Let me ask Mr. Spires, specifically what distinguishes—you know, we have seen that you have the best record of not having redundancies and you have done a good effort there—what distinguishes DHS from the other agencies in terms of its identification and elimination of overlapping or duplicative IT investments?

Mr. SPIRES. Sir, I would go back to the testimony. I put a tremendous effort on setting up what we call these functional portfolios. And so, as I am sure you are well aware, within DHS we have 22 separate components, some very large like the Coast Guard and CBP and some relatively small like our health affairs organization. But what is interesting is that a lot of the functions of DHS crosscut those components.

And what I have tried to really do as the CIO is make sure that we look functionally at DHS, not just vertically from the organizational standpoint. Because when you look functionally, whether we are doing screening or incident response if you were on the mission side or whether we are doing the business functions like finance and HR, you see a tremendous amount of duplication when you look at it from that functional perspective.

So I am just a big believer, if you bring the right executives together in a functional area and get a dialog going, or a structured dialog, over time they see the commonality, okay, they start to recognize it, they start to see the advantages of working together rather than continuing in their stovepipes.

Mr. WALBERG. That gets them beyond the turf mentality—

Mr. SPIRES. Well, I mean, this is not easy. As I said, it takes 3 years or so, in my experience both in the private sector at IRS and now at DHS, to get this to really work well, but it does work. And we have seen tremendous improvements.

We are right now—in fact, screening is a great example, passenger screening or people screening. You know, we have six different components doing this screening. Okay? And we have systems in each of these components, all right, that are essentially duplicative. And now even the Deputy Secretary is taking this on. We are working together. We have the right type of governance model set up with this portfolio around screening to really look at, where can we consolidate, where can we standardize in order to eliminate this kind of duplication?

It is a very different way of looking at an agency's functions. And I think in any federated kind of agency—and, certainly, my colleagues here are also at federated agencies—this kind of process can work to help eliminate duplication.

Mr. WALBERG. Well, I applaud that, and may it continue and expand.

And I would then move to Ms. Takai and Mr. Locatis. On the reverse side, with much duplication or concerns of duplication in your agencies, what are the causes that you have come to ascertain at this point in time for the duplication?

Mr. LOCATIS. Well, as Richard said, he has 3 years, so we have really studied the Department of Homeland Security governance model and, in fact, implemented many of the same work groups and governance capabilities, including our Information Management Governance Council, which has accountability at the Under Secretary level of our three primary programs.

The other thing we have done is looked at it from an interagency sharing perspective, where can we leverage capabilities in other agencies and not duplicate or reinvent the wheel. And it is not just in the technology areas; it is the investment in people, process, and technology for running operations. So one of those examples is, the Department of Energy did not create its own payroll system. It leverages the Defense Finance and Accounting Services' capability and buys those services directly from DOD versus creating our own capability.

So another important piece of this is working across the departments to leverage shared services and not making the investment at all but simply subscribe to it where you have a center of excellence, like DFAS within DOD.

Mr. WALBERG. Ms. Takai, again, what causes for duplication have you addressed?

Ms. TAKAI. Well, historically at DOD, our information technology spend was very decentralized and very focused on mission capability in our services and then, clearly, what was necessary in our forward deployed areas. And the business systems were also distributed from the standpoint of the funding and the decisionmaking process.

So, in answer to your question in terms of what happened in the past to get us to this point, I think that that particular model really caused a sense of uniqueness in different organizations and then the funding to actually look at that.

I think to the point that, you know, both Mr. Locatis and Mr. Spires have made, those are the things that we are working to really change. You know, we recognize that spending in a decentralized fashion, not taking a view of what our overall portfolio management should be, has led to the duplication that we have today.

But our larger challenge is actually getting past the process piece, which says that we don't need to have specific systems that do personnel processing differently, because each of the services actually does do personnel processing a little bit differently. And so our challenge is to really be able to address those process issues, as well.

The other challenge that we have is always the demand from—we need to have capability at the tactical edge. And I think back to the question, Mr. Chairman, that you asked about, that really then gets us into not only looking at the business systems piece of it but some of the forward technologies that you talked about and

our ability to really look at different processes in order to be able to introduce commercial technology, as well as the challenges there.

The last item I would point to is that, to the discussion on our ability to move forward on some of these areas and the way that we are addressing the cloud strategies, it is a challenge for us particularly across all of our networks—classified, secret, and top-secret—to really understand the way forward in terms of working with our commercial partners from a security perspective. The ramifications for us from a national security perspective and making sure that our data are secure are significant.

And so we are moving forward in that direction. We are looking to take advantage of the same things that DHS is from the standpoint of FISMA and then the recent FedRAMP process. But we are walking through that methodically, because we do have to be very concerned about the protection of our information, you know, as a national asset.

Mr. WALBERG. Thank you.

Thank you, Mr. Chairman.

Mr. LANKFORD. Thank you.

Mr. Meehan?

Mr. MEEHAN. Thank you, Mr. Chairman.

I am grateful for the opportunity to be here this morning to listen to your testimony and to speak with you. I think you are some of the most powerful people in Washington because you are the folks that understand these systems, or purportedly do, and any institution I have ever been associated with always comes down to somebody saying, who understands how to get information out this and move it efficiently? And I appreciate the challenge that you have, as well.

I know it is easy to pontificate up here, but I often struggled when I would have authority in the Department of Justice or otherwise over numerous agencies. There seemed to be a lot of discussion about systems, that it often went back to situations in which individuals had their own little turf to protect. And I don't know how we get beyond turf protection and get to the real issue of evaluating what is working.

Mr. Spires, I particularly appreciate the work that you and your folks are doing. I just sat through—in my capacity not in Oversight but in my capacity on Homeland Security, we had the occasion to listen to testimony from the director. We were looking at budget issues. I know there are a lot of good efforts that are being made to create efficiencies at DHS.

I also have the fortune of visiting within my district numerous businesses from time to time, and I am very pleased to have an industry leader, SAP, in my district. And we were talking, I asked him, you know, what are you really doing? And one of the things we spent some time talking about was some of the systems they have been using effectively in DHS. In particular, I think they are working for the Customs and Border Patrol. They were very proud to have had the one group that had a clean audit, based on going back and using that.

Now FEMA is coming out and looking at a system. If one system is working, why are we looking at a new approach to try and have

FEMA—why aren't we just taking what is working at CBP and using it with FEMA?

Mr. SPIRES. Sir, that is a very good question. We are in a situation of evaluating for FEMA right now what is the best way forward for them for financial management. I believe the system you referred to at Customs and Border Patrol is their financial system; that is a SAP system.

Mr. MEEHAN. Yeah. Yeah.

Mr. SPIRES. Because of the contractual relationships that we have, we cannot take, for instance, the system we have at CBP and leverage it for enterprise use. That is a contractual issue, the way it was set up, sir. So we can't just use—

Mr. MEEHAN. You mean we are dealing with a legacy issue, so to speak?

Mr. SPIRES. It is a legacy—yes. The way these contracts were originally set up, we just cannot do that. We have wanted to do that, and we have not been able to.

Mr. MEEHAN. Because, you know, in industries, there are liquidated damages for non-performance. Is there any kind of circumstance under which—if you are looking at a better system, do people go back and look at systems that aren't working and, therefore, have the ability to break through previous contract provisions for non-performance?

Mr. SPIRES. Well, I don't think in this case it is an issue of non-performance. Okay? FEMA is looking to upgrade its system. It is on a legacy system that is, frankly, outdated. It does not provide all the functionality they need.

We are assessing our options. As you probably are aware, we have gone through a number of procurements that even predate my tenure on trying to look at an enterprise capability for financial management across DHS, and we have just never been able to even get to an award because of protests and some legal issues that we ran into. I hate to say that, but that is the truth.

Mr. MEEHAN. Well, I would be interested to hear what we can do to help you in that regard. Because, Ms. Takai, I would be interested in your observation, again. It is incredible how we get little bits of information from time to time and you seize on things, but because of my work on this committee, I am aware of, you know, the Air Force circumstances right now, with the effort.

My recollection was—I asked my staff to look into it, and they did give me a little information about the Expeditionary Combat Support System. We are talking about a system now that, to my information, is—you are billions of dollars into it, they are coming back to us for \$90 million more. Why aren't we looking across the board to see—there are other things working right here in other parts of the Department of Defense.

And how is it that we continue to be locked into these silos? Is it because they are protecting their interests with the lawyers?

Ms. TAKAI. Well, let me address the logistics question that you are asking, the question around logistics systems, and then come back to the broader question.

First of all, the ECSS system, as it is—you know, they have to have an acronym or you can't be from DOD—is one of the logistics systems that is under a review of a set of eight logistics systems

in the Department. And the acquisition technology and logistics organization is actually doing a review right now to look across that portfolio to say, where is there duplication and where can we actually look at a different way and a better way of doing it?

I think, second, there are two answers to your question of how does this happen. One of them is that, in some cases, again, we do have unique requirements. So, for instance, in our operation, what Air Force has to do from a material logistics process is not necessarily the same in terms of doing maintenance in our man, train, and equip organizations, isn't exactly the same as what a TRANSCOM operation has to do in terms of being able to make sure that there are supply lines to our forward deployed troops.

So I do think there is some terminology that are differences, and they are legitimate differences.

But there is also this situation, I think to the point that you are making, where there are processes embedded in terms of the way that we do things. It may not necessarily be a single individual, but it certainly is a single organization. And the question that has to be weighed is, what is the ability of a large organization to make a change, even in some fairly what we would consider straightforward business processes, in order to be able to implement standard technology versus keeping the processes that we have today and actually being able to use a more standard solution?

It is a challenge. You know, both Mr. Locatis and I were in State government in several States. We saw it from a State government perspective, just in terms of being able to draw departments and agencies together. Same kind of experience in the private sector. And it really is around that ability to change from the way we are used to doing things today, the way that we know works, to something that is even a little different that may yield the same result but makes organizations uneasy in terms of their ability to make that change.

Mr. MEEHAN. Well, I know I probably share the sentiments of my colleagues on this committee. If you have suggestions about things that you think would make your job easier to do to get to these efficiencies, I am sure that we would entertain those suggestions and include them in our own deliberations.

Thank you, Mr. Chairman. I yield back.

Mr. LANKFORD. Thank you.

We are going to do a quick second round of some questions. As you have probably guessed, the votes have moved around again. They will be closer to 10:45 now. That will give us a little more buffer time to be able to pummel you with a few more questions and try to get some of this information on the record, as well.

I want to follow up on a comment that Mr. Spires made about, we would like to take a system from over here and use it over here but the contract doesn't allow it. It leads me into a couple issues that I have on keeping contracting officers engaged in what technology is needed. They cannot be specialists in every single area that they are dealing with all their different contracts on.

What are you doing to keep those contracting officers engaged on—a couple of things. One is to say, watching for when it comes down, who has the expertise in this area? Is it actually accurate for what we are looking for, so we are not having to get a system

and then redo the system and go, no, that doesn't work and let's redo it again, and how to get through all that process.

And then to be able to protect in the future in our contracts that if we are using it over here, we can also use it over here. Now, I understand these private vendors want to sell it in 15 different places. I get that. But within an agency, especially, there has to be some level of flexibility, even if it is to say, if we use it here and we use it over here, we pay you another fee but it is a smaller fee than it is over here, but we are not blocked out and have to start all over again when it is a very simple difference.

You talked before about supply chains and financial management and managing human capital. Those are fairly consistent with minor adaptations on them. So how do we start developing contracts so that we can actually not reinvent the wheel time after time with the exact same vendor over and over again?

Mr. POWNER. Within DHS, I partner very closely with our chief procurement officer—he is a peer of mine—Mr. Nick Nayak. And two things that he is really taking on to address your very points. One, he has created a special cadre of contracting officers who do nothing but work closely with us and specialize on IT. Okay? So that doesn't make them technology specialists in IT, but over time they start to understand the complexities of helping us buy IT, right, and work closely with our programs. And I think that is a best practice that a number of other agencies are adopting, as well. So that is not an immediate fix, but over time it does make a big difference. And the individual that heads that organization works with us every day, okay, very, very closely.

I would say to your other point, we are also working on standard contract language now that covers exactly what you suggested. I am amazed, I walk in here and there is a number of these issues where I say, we would to leverage this capability we have in one component in DHS in another and we can't because the contract does not allow us. And so we are forced back into having to go out in full and open competition when, if it was set up right in the first place, we could do exactly what you suggested.

So we are putting standard contract language in. When we go out with these procurements, it can be at least leveraged DHS-wide. And, in fact, we are working in the Federal CIO Council with OMB, can we come up with standard language that allows us to even issue contracts that could be leveraged by other agencies as well.

So we are taking that issue on.

Mr. LANKFORD. Yeah. Long term, that is obviously what is going to help us the most. I mean, if companies are competing, they are going to give us a much lower bid at the beginning, thinking, if I can get this and do it well, and I can also multiply it out, if I can get this to five other agencies and it would be cheaper in all those and beat all those contracts as well, it is to their benefit, it is to the Federal Government's benefit because we will get cheaper contracts all the way across the board as it is duplicated out.

My concern is—and this is just interaction with some different guys that do programming and do some of the writing. Everyone who does that, especially for their own agency that has tapped for it, seems to have the perspective, "They didn't do it as well as we

would do it, and so we are not going to take their stuff; we are going to start all over and do our stuff.”

Now, I am not saying that is an arrogance. Quite frankly, they are tenacious about security, they are tenacious about the coding and to make sure everything is correct on that, which is great. We need those gifts. But it also seems to lock people into, “It needs to be done by me because I know us better than other things.” When it is a supply chain, it is fairly consistent, when you give them the whole lot.

Mr. POWNER. I would just comment, and Ms. Takai really hit upon this issue of this idea of uniqueness, right, and how unique are my requirements. And I think we really need, through the CIO community and through the leadership of agencies—and this is where it gets difficult, to your point, particularly on these standard capabilities and what I would consider back-office—finance and HR and others—these are very similar. Right? And if we can get to the 80 or 90 percent solution, we can get to the kind of environment you want where we are leveraging each other’s capabilities, we are not having to build new. And I think we really need to take that on as a government.

Mr. LANKFORD. Okay. Thank you.

Let me yield to Mr. Chaffetz.

Mr. CHAFFETZ. Thank you.

And thank you, Mr. Chairman, for holding this hearing.

My apologies for stepping in a few minutes late. If this is—I hope it is not redundant, but that is sort of the theme of what we are talking about today, so I won’t feel too bad about it.

I want to start with the Department of Defense, a question about the Defense Finance Accounting System, or DFAS. Is there any progress being made with that?

I mean, my understanding is there is a facility in Indiana, a lot of good people working there, a lot of good stuff, but it is still so manual. It really hasn’t come into the 21st century.

Can you give me an update on what is happening there?

Ms. TAKAI. One of the challenges for us is to continue to move DFAS forward. And we are making significant progress in terms of both the utilization of the system and the system itself. It is going to be very critically important to us as we move forward on our audit readiness requirements. And so it is a major part of the finance portfolio that the chief management information officer is looking at.

Mr. CHAFFETZ. And we don’t have time here, but I would appreciate it if somebody on the staff somewhere could update me on where it is at and where it is going and what the timeframe looks like. And I am looking forward to actually coming and visiting that facility at some point.

I also want to ask the Department of Defense again, we have been looking in my subcommittee within Oversight at the duplication and the problems and challenges between the different agencies within our departments, within DOD, on the health care and the sharing of that information, so that when somebody is actually—you know, somebody has been serving in the military and they are going back into their private life, getting those records back to their doctor sometimes will take in excess of a year. And

I just don't understand why it is so complicated and why it has been so tremendously expensive.

Ms. TAKAI. Well, on that particular front, I think you are aware that we have made considerable progress in terms of looking at the way forward. In fact, there is an initiative now which has been signed out and actually has the visibility of both the Secretary of the Veterans Administration as well as the Secretary of Defense. And they have a joint project now to look at a combined electronic health records—

Mr. CHAFFETZ. What I can't get is a commitment as to the timing, as to when this is actually going to get completed. Do you have any idea when this is going to get completed?

Ms. TAKAI. Well, we can certainly come back. I know the group is today working on putting all of their plans together. So if you will let us, we will come back to you with the detail on DFAS and then also with the project plan for the electronic health records.

Mr. CHAFFETZ. I would certainly appreciate it, because it is such a major problem. I had an opportunity to talk to then-Secretary Gates about this issue and the concern of the timing. And I was shocked at—A, I was pleased that he knew what the timing issue was. But to try to cut it to the timeline that he had talked about, which would still be over a year to get these records into the hands, is just unacceptable to me, and I do want to continue to follow up.

Going now to the Department of Energy, there is evidently—I had an organization, group, Energy Enterprise Solutions. And I don't suspect that you know about every contract, Mr. Locatis—is that how you pronounce it?

Mr. LOCATIS. It is pronounced "Locatis."

Mr. CHAFFETZ. "Locatis." My apologies.

They had had a performance-based contract, and there is some sort of dispute there. I was just hoping that you could give us some assurance that you would look at that personally. If you are willing to make that commitment, I would appreciate it if you would look at that contract and get personally involved in that, if you would be so kind.

Mr. LOCATIS. I am reviewing it now.

Mr. CHAFFETZ. Okay. Thank you. I do appreciate you doing that.

The last thing, Mr. Chairman, I wanted to ask about—and stop me or let me know if this has been talked about. OMB is having some challenges because there are different coding mechanisms for accounting. And when I talk to the outside interest groups, you know, the people that want good, open, transparent government, it is very difficult to compare the individual data because they use different coding within different departments, a certain number of digits.

Where on the radar screen, between the four of you all, is this? And I am sorry I didn't do a good job of articulating it, but where is this on your radar screens?

Ms. TAKAI. Well, let me start.

Certainly, as it relates to being able to report and work with OMB on the IT budget line items, we have been working very closely with them, because it is an issue in terms of our internal reporting and working with OMB. And certainly that is, you know, a major part.

I think the second piece is, for us within DOD, we are concerned about just the overall coding and reporting for our effort around being audit-ready.

So those are two efforts, certainly, for us inside DOD and working with OMB that have escalated the importance.

Mr. CHAFFETZ. Mr. Chairman, my time has expired.

And I will do a better job of articulating or perhaps putting in a letter that I would love to share with you all about the concern from OMB, particularly—again, this is the genesis coming from outside the groups that want to be able to compare apples to apples on line items amongst the various departments. You obviously represent some of the largest departments in our Federal Government, so I would like to follow up with you on that, as well.

But I appreciate your commitment and your service. It is a very difficult, fast-paced sector but vital to good government and to making sure that they operate.

And so I appreciate you holding this hearing, Mr. Chairman. Thank you.

Mr. LANKFORD. Thank you.

Ms. Takai, one last question, as well. You brought up the famous “audit” word on DOD. Where are things on that? Give us a timeline and progress on when it will be auditable and tracking.

Ms. TAKAI. The Secretary has tasked us to move up the prior plan, which was to be ready by 2017, to be ready by the beginning of 2015. And so the organization has put in place a number of different activities and a number of different measurements to get there. So we are all geared up, and we are ready to go.

Mr. LANKFORD. Terrific. I appreciate that.

And as I have mentioned at the very beginning, on the IT Dashboard as well, I appreciate all that you are doing there, but also keeping it up to date. It is one thing to report and it is another thing to keep those reports up to date. And that is always a wonderful, I am sure, extra thing on your desk, but try to continue to push. There are some elements that have been out there that have some lower scores but they are not being kept up to date, and so we don't know how to be able to track that. And so that is important, to be able to keep that up as well.

I appreciate the success stories that you are sharing. I hope that this also is indicative of a forum of sharing ideas across our Federal agencies. I am confident that you all get together as well, that you are establishing your own TechStat reviews within your own agencies and doing all those dynamics to try to identify some of these things. But as we identify this, please encourage your peers on ways of being able to share good ideas on how we can resolve this, as I am confident that you are. But as you solve some of the issues, share the solutions. And it is not bad to be able to brag when we are saving money and making things more efficient.

So, with that, I adjourn this hearing, and we are concluded.

[Whereupon, at 10:40 a.m., the subcommittee was adjourned.]

Chairman Lankford Opening Statement

This hearing on Duplicative Information Technology investments is one part of a larger effort to help ensure that our government is doing everything it can to reduce wasteful government spending. Earlier this week the Oversight and Reform Committee held a hearing to discuss a request for authority to reorganize government agencies to increase efficiencies. In a few weeks, we will hold another hearing to discuss GAO's latest report to identify overlapping and duplicative federal programs.

When we consider ways to "do more with less" or to reduce redundancies and waste in federal spending, focusing on federal IT investment is a perfect place to start. The government now spends about \$80 billion in spending each year on IT investments and has spent \$600 billion during the past decade. Two of the Departments represented here today have experienced some major IT disasters including the Department of Defense - Defense Integrated Military Human Resources System which was cancelled after 10 years of development and \$850 million in expenditures. Similarly, the Department of Homeland Security ended its Secure Border Initiative Network Program after investing about \$1.5 billion.

IT reform has been a challenge for decades. Congress has enacted numerous laws, including the Clinger-Cohen Act, highlighting the need to tackle this problem of wasteful IT spending. The former Federal Chief Information Officer, Vivek Kundra, stated, "IT has transformed how the private sector operates and has revolutionized the way in which it serves its customer. The Federal Government has largely missed out on these transformations, due in part to its poor management of large Information Technology investments." To his credit, a little more than one year ago, Mr. Kundra, in consultation with key stakeholders, including many of not all of our witnesses today, developed a 25 point plan for IT Reform. Item number 1 addresses duplication and the need to for consolidation of IT assets: it calls for "complete detailed implementation plans to consolidate at least 800 data centers by 2015." The plan also calls for development of a strategy for shared services and the need to leverage the government's purchasing power for commodity IT service—IT systems that all agencies use, but that are often developed separately and inefficiently. The plan recognizes that demand aggregation across agencies for IT related goods will drive value for agencies. While the plan calls for agencies to "work with Congress to consolidate IT Spending under an Agency CIO, unfortunately, OMB has identified this action item to be one of 3 that are "behind schedule."

As the subcommittee with jurisdiction over government-wide technology and information policy issues, we welcome the opportunity to work with the CIO community to address these thorny and persistent problems of wasteful IT spending. The GAO report issued today provides an important opportunity to begin that dialogue. Both Congress and the White House have empowered the agency CIOs to lead IT reform. The topic of the hearing today raises some questions in my mind about whether the CIOs are demonstrating sufficient leadership and are effectively managing their large IT investments. For example, how is it that GAO was able to

identify 37 potentially duplicative investments in DOD's and DOE's portfolios when the professionals and experts at these agencies could not? Even when these investments were identified to CIO offices, the response to GAO was: "we will form a working group to look into this" or "all investments will be reviewed in the future." In other words, I am concerned that agencies are not proactively identifying duplication and are not making this the priority that it deserves to be. I look forward to hearing success stories about reducing IT investment duplication and increasing cost efficiency. I anticipate we will find the answers on the impediments that CIOs are facing that prevent more action from being taken; and if IT professionals have the tools needed to do the important work entrusted to them.

We hope to explore these and other issues at today's hearing.

Statement of Congressman Gerald E. Connolly

Subcommittee on Technology and Procurement

February 17th, 2012

Chairman Lankford, I appreciate the opportunity to consider information technology investments by federal agencies, including possible benefits and opportunities for improved efficiency. This inquiry should consider not only whether there are possible duplicative investments but also whether foregone investments represent a missed opportunity to improve delivery of services, realization of an agency's mission, or possible cost savings.

In the case of the Department of Energy (DOE), the Government Accountability Office (GAO) identified a relatively modest \$14 million in possible duplicative investments. Based on the information before us, it seems that the DOE has responded to GAO's inquiry by examining opportunities to reduce duplication and save money. Specifically, DOE agreed that 11 of 12 possible duplicative information technology systems identified by GAO are worthy of further investigation. The DOE proactively conducts reviews of ongoing investments to identify consolidation or other cost savings opportunities and assesses system inventories to see if its systems meet performance requirements which already are in place. In addition to these ongoing evaluations, I look forward to learning more about the DOE's analysis of possible cost savings through data center consolidation and a shift to cloud-based data storage and management. As part of that inquiry, DOE should consider whether a public or private cloud offers a lower cost solution with requisite levels of cybersecurity.

DOE's possible duplicative investments pale in comparison to those at the Department of Defense (DOD). GAO took a sample of 810 DOD information technology investments, not a comprehensive survey, and found that 42 of them potentially are duplicative. According to GAO, this represents up to \$1.2 billion in duplicative investments. During the previous administration, the quantity of contract spending doubled while the number of acquisition personnel hardly changed. Predictably, overworked, underpaid staff cannot possibly manage federal contract expenditures as well as a fully staffed, appropriately trained workforce. This is an example of how attacks on the federal workforce, which always are predicated on promised savings, often are penny wise and pound foolish. We may save a little money on salaries and benefits but lose a great deal of money through insufficient contracting oversight. GAO says that DOD could save up to \$465 million through improved acquisition and contract management. The information in this GAO report should raise the question—and I don't think we know the answer yet—whether a hollowed out staff is related to the duplicative information technology investments raised in the report.

Thank you to our panelists for joining us today. I look forward to your testimony and a discussion about the opportunity of information technology investments to save money and improve delivery of services.

Questions for Teri M. Takai
Chief Information Officer
Department of Defense

Chairman Issa
Committee on Oversight and Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and Procurement Reform

Hearing on "How Much is Too Much? Examining Duplicative IT Investments at DOD and DOE"

1. Question: Large organizations - whether private sector companies or federal agencies often do a poor job of managing complex software license agreements, obligations, and metrics throughout an organization to avoid over-purchasing software licenses. As a result, organizations and companies not only fail to realize the benefits of economies of scale, but also risk spending too much on unneeded software. We have heard that this leads to tremendous waste. We understand that the Naval Facilities Engineering Command has utilized an automated solution called "enterprise license optimization" that has allowed the Command to audit its use of software licenses and address unnecessary spending for licenses.- Does the Department of Defense plan to expand these kinds of assessments to achieve the greatest possible economies of scale and cost-savings in the procurement of IT infrastructure such as enterprise software?

Answer: The Department understands the importance of effective IT asset management in order to avoid over buying or over deployment of commercial software. License management at the enterprise level includes process change in addition to implementation of a variety of technology solutions. In addition to providing access to software when needed, the negotiation and adoption of software licensing terms and conditions that allow for sharing of licenses among authorized users rather than purchasing a license for each user regardless of frequency of use introduces the opportunity for reduced license and sustainment costs.

To this end, the Department proactively shares best practices, such as the Navy Facilities Engineering Command's enterprise license optimization approach, with and among Defense Components. Establishing and enhancing an IT asset management framework for use in the Department that includes software license management optimized at the enterprise level is an element of the emerging DoD Joint Information Environment (JIE).

Questions for Teri M. Takai
Chief Information Officer
Department of Defense

Representative Chaffetz
Committee on Oversight and Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and Procurement Reform

Hearing on "How Much is Too Much? Examining Duplicative IT Investments at DOD and DOE"

1. Question: Please provide an update on the Department's plans to modernize the IT systems at the Defense Finance Accounting System (DFAS) facility in Indiana. Please include a timeline clearly explaining when the plan will be completed.

Answer: The Defense Finance and Accounting Service (DFAS) proudly serves America's heroes by providing finance and accounting support to the Department of Defense (DoD). DFAS is the world's largest accounting organization, processing 171.7 million pay transactions, totaling \$608 billion, to 6.6 million people or accounts in 2011. DFAS pays all DoD military and civilian personnel, retirees and annuitants, as well as DoD contractors and vendors. DFAS also provides civilian payroll support to other agencies outside the DoD, such as the Executive Office of the President, the Environmental Protection Agency, the Department of Energy, and the Department of Veterans Affairs.

Since its inception in 1991, DFAS has reduced infrastructure and operating costs by consolidating more than 300 offices and 330 systems, into nine sites and 105 systems through continuously improving processes, systems, and functions. The savings from these reduced costs are returned to the Services, agencies, and other customer we support. DFAS Indianapolis, the agency's headquarters and largest site, provides accounting and finance services primarily to the Army, the Air Force, and twenty-six Defense Agencies.

Efforts are continuously underway to use newer technology to improve systems. Moving to web tools and other business applications have helped to automate data entry and extraction. In August 2011, DFAS developed a Web version of the Master Military Pay Account (MMPA). This web tool translates legacy data into plain English, giving customers new ability to easily tailor data queries to individual needs. Both the Army and Navy payroll offices are currently utilizing this application. The Air Force is planning a phased implementation during FY 12. The Defense Military Pay Office (DMO) web tool was approved March 2012 with planned fielding in early 2014. Additional efforts are underway to implement Business Intelligence tools allowing for more data mining and customization. Both of these efforts improve the Defense Joint Military Pay System's capability to efficiently pay military service members.

Another major effort where DFAS is heavily engaged to promote new technology capabilities is DFAS's direct support to the DoD Military Services and Defense Agencies' Enterprise Resource Planning (ERP) program implementations. For the ERP systems, DFAS is developing systems' Financial Management (FM) requirements to ensure compliance, and conducting Business Process Reengineering (BPR) to improve the DoD's

and DFAS's FM efficiency and effectiveness. DFAS is also coordinating, collaborating, and integrating with the Military Services and Defense Agencies ERP program offices to identify and prioritize functions and processes to increase systems interoperability. For DFAS, the ERP implementations are vital to improving and modernizing our systems and processes to meet the goals of audit readiness and auditable financial statements. Specifically at DFAS Indianapolis, the General Fund Enterprise Business Systems (GFEBs), Defense Agencies Initiative (DAI), and Global Combat Support System-Army (GCCS-Army) ERP systems are in use. The GFEBs scheduled releases are planned for the fourth quarter of fiscal year 2012, with new releases and capability improvements planned through the fourth quarter of fiscal year 2013. DAI is planned for fielding to five additional agencies in the first quarter of 2013 and six additional agencies in fiscal year 2014. Finally, GCCS-Army is planned for installations to multiple DoD sites every quarter from the fourth quarter of fiscal year 2012 to the fourth quarter of fiscal year 2014.

The expansion of ERP fielding improves upon DFAS' low-cost, high-quality payroll, accounting and finance services throughout DoD, and maintains DFAS' unique position in providing critical mission support and informing financial stewardship.

2. Question: Please provide an update on the status of efforts by the Department of Defense and the Department of Veterans Affairs to combine or share electronic health records? Please provide the project plan for electronic records that you referenced at the hearing, including an estimated completion date.

Answer: On March 17, 2011, the Secretary of Veterans Affairs (SECVA) and the Secretary of Defense (SECDEF) reached an agreement to work cooperatively on the development of a common Electronic Health Record (HER) and are planning to sunset some of the legacy systems and transition to the new integrated Electronic Health Record, or iEHR.

This effort is known as iEHR since both Departments are modernizing their EHRs together, using incremental methodology to create a single framework for all the data related to a medical record, whether that data belongs to VA or DoD. iEHR is a joint acquisition and development of a new system that will provide a shared architecture and infrastructure between the Departments. It will standardize the user interface, provide common applications, and enhance ease of access to systems and information for both Departments.

The Interagency Program Office (IPO), established by section 1635 of the National Defense Authorization Act (NDAA) of 2008, to accelerate the exchange of health care information between the Departments, will lead the Departments in the acquisition, development, and implementation of iEHR and the Virtual Lifetime Electronic Record health systems, capabilities, and initiatives that follow to achieve full information interoperability.

In October 2011, the IPO was re-chartered to state that the IPO "Serves as the single point of accountability for the Departments in the development and implementation of the integrated electronic health record ... system, capabilities, and initiatives with the goal of full interoperability between the DoD and VA. ... [It] is authorized by the Departments to lead, oversee, and manage all interagency planning, programming and budgeting, contracting, architecture, capability acquisition and development, data strategy and management, testing and evaluation planning, infrastructure requirements and funding, common services, implementation, and sustainment related to and including the integrated EHR (iEHR) ..."

The iEHR program is currently in the Planning State. iEHR will be subject to the programmatic requirements of both the DoD Business Capability Lifecycle (BCL) and the VA Program Management Accountability System (PMAS). The IPO, DoD, and VA are identifying areas where process differences may exist, and are collaboratively engaging in efforts to ensure that any impediment that may arise is resolved in an efficient manner. The IPO will leverage BCL and PMAS to create a Capability Development Life Cycle Framework which will capture the required documentation and milestone decisions for each phase, to include funding and investment decisions. Given the complexity of the iEHR effort and the need to merge two acquisition lifecycles, the Departments have acknowledged the need to optimally align their processes to ensure agile and cost efficient delivery of capabilities to the clinical community.

FY12 Accomplishments to Date:

- ▶ Signed Interagency Program Office Charter, October 27, 2011
- ▶ Defined the Organization Structure and Staff Profile for the IPO and iEHR Program Management Office (PMO)
- ▶ Initiated Development Test Center / Environment (DTC/DTE) Configuration
- ▶ Deployed early version of iEHR joint presentation layer at North Chicago on December 1, 2011
- ▶ Achieved high level definition of Capability Sets 0 and 1 from the DoD/VA Interagency Clinical Informatics Board, December 6, 2011
- ▶ Stood-up iEHR PMO Working Groups / Integrated Product Teams

Questions for Richard Spires
Chief Information Officer
Department of Homeland Security

Representative Meehan
Committee on Oversight and Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and Procurement
Reform

Hearing on "How Much is Too Much? Examining Duplicative IT Investments at DOD and DOE"

Question: During an exchange with Congressman Meehan, you stated that there were contractual limitations which prohibited DHS from taking the Customs and Border Patrol (CBP) finance and accounting system and implementing it at the Federal Emergency Management Agency (FEMA).

What specific contractual limitations were you referring to in your testimony that would prohibit DHS from using CBP's financial system for FEMA?

Response: The CBP system was acquired competitively to meet CBP specific requirements, not those of the DHS Enterprise. Therefore, under the scope of the existing contract, DHS has no contractual ability to expand the "use" the CBP system by or at other components, such as FEMA. If other DHS components were migrated to the CBP system using the existing contract, interested vendors could protest the action as being outside of the scope of the existing contract.

Question: In your testimony you indicated that you would like to implement the same CBP finance and accounting system for FEMA but were not able to do so due to contractual relationships. What contractual relationships would need to change in order to allow FEMA to use the finance and accounting system which has proved so successful for CBP?

Response: It is not a contractual relationship that must change. As stated above, the original contract that supported the deployment of the CBP system was competed based on CBP specific requirements and any action taken "outside of the scope" of the existing contract could be subject to protest by industry.

Question: As you stated in your testimony, FEMA is currently operating an outdated legacy system. What is FEMA's plan for upgrading to a new finance and accounting system?

Response: FEMA's IFMIS solution was purchased as a COTS product in 1993, implemented in 1996, and customized since then by FEMA. IFMIS is based on 20 year old technology, using COBOL programming which was modified to provide graphical user interface input screens. It operates in a mainframe environment, with limited capability to expand to support catastrophic disasters. Because of the customizations, IFMIS software updates are difficult and expensive. The antiquated system environment is becoming unstable.

Due to this instability, IFMIS will likely not remain stable for the anticipated 18 month implementation of a new solution. Therefore, FEMA will first perform a technology refresh to mitigate current performance issues and ensure a stable technical baseline for the future transition. The technology refresh investment will extend the financial management solution lifecycle by approximately 3 years, during which time FEMA can continue to review its requirements to determine the best way to meet those requirements for the long term.

Question: Does DHS need Congressional authority to provide the flexibility necessary to allow themselves and other federal agencies to more easily evaluate and use the best and most proven systems across the government so as to avoid the unnecessary and costly development of new information technology systems?

Response: The laws that govern the acquisition of supplies and services that DHS and other federal agencies must abide by do not always lend themselves well to the continuous innovation and rapid change that characterize Information Technology (IT).

Because of the need to judiciously assess the full scope of existing mandates on the IT procurement process government-wide, and to carefully weigh competing priorities, OMB has been collaborating with the Federal Chief Information Officer (CIO) Council to develop a set of specific recommendations on how best to achieve the goals of acquiring the latest and most innovative technology to address evolving requirements, avoid the costly and time consuming development of new technology systems, and leverage existing capabilities to the fullest degree possible. The Federal Government's CIO, Mr. Steve VanRoekel, is helping drive these changes through the "Shared First" and "Future First" initiatives.

