

**REDUCING DUPLICATION AND IMPROVING
OUTCOMES IN FEDERAL INFORMATION
TECHNOLOGY**

HEARING

BEFORE THE

COMMITTEE ON
HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE
ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

—————
JUNE 11, 2013
—————

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

Printed for the use of the
Committee on Homeland Security and Governmental Affairs



U.S. GOVERNMENT PRINTING OFFICE

82-569 PDF

WASHINGTON : 2013

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 HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

THOMAS R. CARPER, Delaware *Chairman*

CARL LEVIN, Michigan	TOM COBURN, Oklahoma
MARK L. PRYOR, Arkansas	JOHN McCAIN, Arizona
MARY L. LANDRIEU, Louisiana	RON JOHNSON, Wisconsin
CLAIRE McCASKILL, Missouri	ROB PORTMAN, Ohio
JON TESTER, Montana	RAND PAUL, Kentucky
MARK BEGICH, Alaska	MICHAEL B. ENZI, Wyoming
TAMMY BALDWIN, Wisconsin	KELLY AYOTTE, New Hampshire
HEIDI HEITKAMP, North Dakota	

RICHARD J. KESSLER, *Staff Director*

JOHN P. KILVINGTON, *Deputy Staff Director*

KEITH B. ASHDOWN, *Minority Staff Director*

CHRISTOPHER J. BARKLEY, *Minority Deputy Staff Director*

TRINA D. SHIFFMAN, *Chief Clerk*

LAURA W. KILBRIDE, *Hearing Clerk*

CONTENTS

Opening statements:	Page
Senator Carper	1
Senator Coburn	3
Senator Ayotte	24
Prepared statements:	
Senator Carper	39
Senator Coburn	41

WITNESSES

TUESDAY, JUNE 11, 2013

Steven VanRoekel, U.S. Chief Information Officer, and Administrator for E-Government and Information Technology, Office of Management and Budget	6
Simon Szykman, Chief Information Officer, U.S. Department of Commerce	7
Frank Baitman, Deputy Assistant Secretary for Information Technology, and Chief Information Officer, U.S. Department of Health and Human Services	10
David A. Powner, Director, Information Technology Management Issues, U.S. Government Accountability Office	12

ALPHABETICAL LIST OF WITNESSES

Baitman, Frank:	
Testimony	10
Prepared statement	52
Powner, David A.:	
Testimony	12
Prepared statement	57
Szykman, Simon:	
Testimony	7
Prepared statement	47
VanRoekel, Steven:	
Testimony	6
Prepared statement	43

APPENDIX

Vance E. Hitch, Former Chief Information Officer of the Department of Jus- tice, prepared statement	77
Partnership for Public Service, prepared statement	80
Responses to post-hearing questions for the Record from:	
Mr. VanRoekel	83
Mr. Szykman	102
Mr. Baitman	108
Mr. Powner	112

REDUCING DUPLICATION AND IMPROVING OUTCOMES IN FEDERAL INFORMATION TECHNOLOGY

TUESDAY, JUNE 11, 2013

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:34 a.m., in room SD-342, Dirksen Senate Office Building, Hon. Thomas R. Carper, Chairman of the Committee, presiding.

Present: Senators Carper, Coburn, and Ayotte.

OPENING STATEMENT OF CHAIRMAN CARPER

Chairman CARPER. Well, good morning. Our thanks to our witnesses for joining us today as we examine the Administration's ongoing efforts to identify and eliminate areas of duplication and areas of waste with respect to Federal information technology (IT) and the role that Chief Information Officers (CIOs) can and should play in that process. My thanks as well to Dr. Coburn, to his staff, and to our staff for their help in putting this hearing together, and to all of you for coming and for your preparation.

This Committee is holding this hearing today because, to put it simply, when it comes to information technology, the Federal Government needs to do a better job of managing its considerable investments. I think I will start just by quoting one of our colleagues, and this is his statement:

"Poor information [technology] management is, in fact, one of the biggest threats to the government treasury because it leaves government programs susceptible to waste, fraud, and abuse."

That is the quote. And it is not something that Tom Coburn said or John McCain said or Claire McCaskill said or I said. That is something that Bill Cohen said when he was a Senator. Those are the words that he spoke in 1995 when he testified before this Committee when it was just the Committee on Governmental Affairs in the summer of 1995, and he was testifying on behalf of legislation that he had introduced called the Information Technology Management Reform Act, 18 years ago.

That bill is also known as the Clinger-Cohen Act, and I have no doubt that all of the witnesses on this panel are quite familiar with it because it created the position of agency Chief Information Officer. The Clinger-Cohen Act was passed almost two decades ago. Back then, a blackberry was a fruit, a tweet was something that

only birds did, and Google was just a really big number. Today we live in a world of smartphones and tablets, social media and the cloud. Yet the more things change, the more they stay the same. Despite passage of the Clinger-Cohen Act and the creation of agency chief information officers, our Federal Government still wastes a tremendous amount of money by poorly managing IT systems and investing in duplicative systems.

In 1996, when the Clinger-Cohen proposal became law, the Federal Government was spending about \$25 billion a year on information technology systems. That is not an insignificant amount of money, but today we spend more than three times that amount. We spend about \$80 billion a year.

I would ask today's witnesses, with all the money we spend each year on information technology, do we really think we are getting what we are paying for? Can agency managers look at their investments in this area and tell the American people that they are managing the taxpayer dollars entrusted to them effectively? And I am afraid the answer to both questions has to be no.

In 2013, we see many of the same problems that Senator Cohen found in 1995: Poor management of information technology systems, wasted and duplicative investments, and billions of dollars spent on outdated legacy systems. Too often, agencies, or components of agencies, seek to develop new solutions first before assessing existing options for sharing services with other agencies or even within their own agency. As I mentioned before, the more things change, the more they stay the same.

To address these persistent problems, in 2012 the Administration launched a new initiative called "PortfolioStat" which required Chief Operating Officers (COOs) across government to lead an agency-wide review of their IT systems and eliminate areas of duplication and waste. The Federal CIO then met with each agency to discuss, among other things, potential duplicative systems and investments that did not appear to be well aligned to agency missions. Through this process, agencies identified more than \$2.5 billion in IT spending reductions that could be achieved from 2013 through 2015.

We are happy to have the Federal Chief Information Officer here with us today to tell us about the first version of PortfolioStat and what the future holds for that initiative. Mr. VanRoekel, I understand that you have new responsibilities at the Office of Management and Budget (OMB), but I am hopeful that, as our Federal CIO, you will stay actively engaged in the PortfolioStat process because I strongly believe that your participation in those meetings with the Chief Operating Officers and the other agency leaders is key to getting the kind of results we want.

One of the key takeaways from the first round of PortfolioStat sessions was that the decentralized manner in which many agencies managed their information technology investments lead to "inefficiencies and duplication." The fact is that despite the Clinger-Cohen Act, agency CIOs are frequently not recognized as the key leaders in managing information technology at an agency. Too often there are many CIOs in a department, and many of them act independently of one another. And as a result, departments are unable to take an enterprise-wide view of their investments which re-

sults in duplication and missed opportunities to leverage existing systems.

I am very interested to hear from our panel, and especially from Mr. Szykman.

Chairman CARPER. Mr. Szykman, Mr. Baitman, and Mr. Powner, I know how to say your name. We have said your name a lot. But I want to hear from our panel, especially from Mr. Szykman and Mr. Baitman about their experiences at large decentralized Departments like Commerce and Health and Human Services (HHS).

Let me just finish my statement with another quote from the same guy, Bill Cohen. Here is what he said, “But we must also understand that statutory change is only half the battle. The other half involves changing the management culture at agencies that has traditionally focused on technical performance and bureaucratic process. We must ensure that the top levels of agency management understand how information technology can change and improve their agencies. Cultural change is critical to changing the way government approaches its information technology needs.”

And I end with that quote because I think it highlights the fact that our job is not done once a bill is passed into law. In many ways that is when the hard work really begins—when we roll up our sleeves and do the oversight necessary on this Committee and in other places necessary to ensure that a law is being implemented properly. It is ultimately congressional oversight that lets agency leaders know where our priorities lie and that can help agency leaders break through any resistance there may be to change.

With that being said, I am happy to turn to Dr. Coburn for whatever comments he would like to make. Dr. Coburn.

OPENING STATEMENT OF SENATOR COBURN

Senator COBURN. Well, thank you, Senator Carper, and welcome, all of you.

I think there are four or five problems in front of us, and having done this a number of years, we keep trying to solve the same problems. And here is the crux of it.

We are well intentioned. You are well intentioned. But we do not give people the authority to do what we ask them to do. And even in OMB’s recent guidelines, they essentially in four or five areas undercut the Chief Information Officer and agencies by allowing them to place other than our key computer IT people in charge of the programs. That is the first problem I see, and I will go into detail as we go through the questioning on that.

The second problem is we do not have real transparency and metrics on what we are doing. We do in one Department. It is very rarely we get to really praise the Department of Homeland Security (DHS). But if you look at what they have done on their data centers, they actually track it transparently, know what they are doing, know how many they have, know how many they have eliminated, and know how much money they have saved. You cannot do that anywhere else in the Federal Government.

So we lack transparency, and we lack good metrics. As a matter of fact, the metrics are changing in the middle of all this, according to OMB.

The other thing is the IT Dashboard is a farce. We have looked at computer programs at the Pentagon, and according to the IT Dashboard, they are doing fine, which is absolutely opposite of what is actually happening in the Pentagon. Half of the money we spend on IT goes through the Pentagon. Half of it is wasted every year. And yet the Dashboard shows no problems with the Pentagon's programs, just like the Pentagon shows no problems in improper payments. Just because they do not have any idea whether they have a problem, and they do not have any idea whether they really have improperly payments. Which goes back to Audit the Pentagon Act, that you are never going to control the Pentagon until we can have numbers and accountability and metrics to get it done.

The fourth area is just the communication of what is actually happening. Some of our agencies, some represented here today, actually know. But once you actually get to working on this, some of our Secretaries and some of the people inside some of the agencies do not like it because there is accountability coming and our CIOs get thrown out, two of which recently, which were actually doing a good job. But because other priorities other than transparency, other than metrics, other than good management take precedence—which goes back to the first problem, because if you are not going to give CIOs the authority to do what they need to do, then why do you need a CIO?

And we have read the testimony. We have looked at all this. I hope to have a great discussion. But some change ought to come out of this oversight hearing, both in terms of transparency, in terms of giving CIOs the authority they need to actually make the decisions, and create the transparencies associated with that so it can be measured. And actually my compliments to DHS to create a timeline so you can actually see it and manage it, and we can as you see it and manage it.

My final point I would just make is we had expected savings coming out of the data center consolidation initiative. Those savings really are not materialized because if we did have savings, we are spending it somewhere else, essentially. And now we are going to consolidate the savings to less than what we had hoped to achieve through the latest iteration. So we are actually going backward. The stream is more powerful than our oars. And, with excess of \$80 billion a year spent on IT, of which a conservative estimate, at least a third of it is not effectively spent. We can do better, and, that is \$24 billion. That is 30 percent of the sequester. I mean, everybody talks about the sequester, how hard it is. But there is plenty of money in this government. There is \$250 billion of waste, fraud, duplication, and stupidity, and what we need is to give you all the authority to go after it and to make smart decisions.

I will just end with this: I trust the vast majority of executives in our government. What I do not trust is Congress to treat them like grownups and give them authority and then hold them accountable for it. And hopefully through this hearing today we can make some steps and get some learning through the communication that will allow us to do that.

David has been great through what he has done through the years. Almost every question I am going to ask you, I am going to

ask him what he thinks about it and your answer because what we want is the best. And this is not meant to knock on anybody, but we have big problems. And they are getting worse. They are not getting better. They are getting worse. And the effort is being made at OMB. I am not saying it is not. But we can do a far better job than we are doing.

So I look forward to your testimony. Again, I thank you for being here to discuss these things.

Thank you, Tom.

Chairman CARPER. Thanks, Dr. Coburn.

Just to put what Dr. Coburn has said in context, if that \$24 billion number that he held out was roughly a third of the money we are spending on—that is in the ballpark. That is a 1-year number. We just passed this week a farm bill that is designed to overhaul the way we run agriculture programs. It is expected to save about \$24 billion over 10 years. And we are talking about literally the equivalent, if that \$24 billion is correct, of doing that every year for the next 10 years, like \$240 billion. That is a quarter of a trillion dollars. That is real money, a lot of money.

The other thing I would say is that if the Department of Health and Human Services, if they can get this right, if they can serve as an example, maybe the rest of us can, too. So it is always good to have somebody out there providing a good example, and I think we have one. And we are happy that you are here to talk about that.

Senator COBURN. Could I—

Chairman CARPER. Go ahead, please.

Senator COBURN. Could I just have a moment of disagreement with my Chairman? We state that it saves \$24 billion—6 comes from sequester, \$2 billion is the real savings, and none of that will be there if prices of crops go down. So what politicians in Washington put out as fact are not fact. My quote is based on all the hearings we have done through the years, knowing where we are, and oversighting the Department of Defense (DOD) and knowing how much they waste. And so that is not even looking at any of the other departments.

So the efforts that you are doing, we did save some money, and that is a marked improvement. But we did not come anywhere close to saving \$24 billion for the American people.

Chairman CARPER. All right. Well, the Congressional Budget Office (CBO), they are the ones who score these things, and that is what they told us, so we will see. We do not want to get into that argument.

I am glad you are here. Let me just briefly introduce each of you.

Our first witness is Steven VanRoekel, who was appointed as U.S. Chief Information Officer by President Obama in August 2011. Prior to his position in the White House, he served in executive positions in the U.S. Agency for International Development (USAID) and for the Federal Communications Commission (FCC). Before joining government, Mr. VanRoekel spent a number of years at Microsoft Corporation where he worked closely with the corporation's co-founder Bill Gates.

Our next witness, Simon Szykman, serves as the Chief Information Officer of the U.S. Department of Commerce. As the Depart-

ment's CIO, Mr. Szykman is responsible for maintaining oversight over a diverse portfolio of programs across the Commerce Department's dozen bureaus. He previously served as the CIO of the National Institute of Standards and Technology (NIST).

Our next witness is Frank Baitman. Mr. Baitman is currently the Chief Information Officer with the Department of Health and Human Services, where his emphasis has been on delivering improved business outcomes for the agency's technology investments. Recently Mr. Baitman served as the White House entrepreneur in residence on assignment at the Food and Drug Administration (FDA).

And our final witness today is David Powner. David is no stranger to our Committee. Mr. Powner is the Director of Information Technology Issues at the U.S. Government Accountability Office (GAO). He is currently responsible for a large segment of GAO's IT investigations. He has over 20 years of experience in information technology in both the public and private sectors.

Your entire statements will be made part of the record. We will start with Mr. VanRoekel, and I look forward to your comments, each of you, and then to our questions and conversation. Thank you. Welcome. Please proceed.

TESTIMONY OF STEVEN VANROEKEL,¹ U.S. CHIEF INFORMATION OFFICER, AND ADMINISTRATOR FOR E-GOVERNMENT AND INFORMATION TECHNOLOGY, OFFICE OF MANAGEMENT AND BUDGET

Mr. VANROEKEL. Thank you. Good morning, Chairman Carper, Ranking Member Coburn, and Members—we do not have other Members of the Committee—staff of the Committee. Thank you for this opportunity to testify on the Administration's efforts to manage the Federal Government's investment in information technology.

During my nearly 20 years in the private sector, I witnessed firsthand the power technology can have on organizations and have seen the incredible impact innovation has on society. As an executive at Microsoft, I focused every day on improving core services and customer value while also cutting costs. And as the United States Chief Information Officer and now Acting Deputy Director for Management at OMB, I bring that same vision with me to help drive innovation to grow the American economy, drive efficiency and effectiveness into government, and foster an accountable and transparent government that provides better service to the American people.

Current expectations from the American public underscore the need to drive innovation and efficiency in government. Though they make up a small portion of overall government spending, IT investments have widespread impacts across agencies and are central to everything we do. As such, we must ensure that the government maximizes the return on its investment in IT, drives innovation to meet our customer needs, and establishes a trusted foundation for securing and protecting our assets and information.

¹The prepared statement of Mr. VanRoekel appears in the Appendix on page 43.

Simply put, we must manage our IT investments so they deliver results for our most important customer—the American people.

Sound management is rooted in evidence, metrics, data, and incentives. This is why in March 2012, I initiated PortfolioStat to take a data-driven look across agencies to identify common areas of spending to reduce duplication and lower costs. Throughout last summer, I conducted a series of face-to-face sessions with agency leadership to examine their IT portfolios. Rather than look at individual investments, the review took a very broad, horizontal approach. For example, they spanned agency components and employed both qualitative and quantitative data to benchmark these agencies against their peers.

To date, PortfolioStat, as you mentioned, has yielded nearly 100 opportunities to consolidate or eliminate redundant IT investments representing more than \$2.5 billion in potential savings for the next 3 years. So far, and a year in, agencies have reported approximately \$300 million in realized savings, putting us ahead of our target. As we expand PortfolioStat, we expect our goals to expand, and we will work hard to continue to drive those results.

OMB recently released guidance for PortfolioStat 2013. This guidance streamlines agency data collection, adds analytical capabilities, and establishes consistent reporting to hold agencies accountable for the goals they set in 2012.

The initial PortfolioStat sessions concentrated on commodity IT. The fiscal year 2013 effort continues this work, but focuses on providing agencies with tools to better manage IT as a strategic investment.

There has never been a more crucial time to make smart investments in IT. Advances such as cloud computing, big data, and mobile provide new opportunities for transforming how we live and function as a society. They equally provide opportunities for transforming how we operate government. Our efforts to date have shown that there remains tremendous opportunity to improve our management of Federal IT, and we should seize on this opportunity to continuously drive the delivery of better service, the realization of greater efficiencies, and the implementation of more vigilant cybersecurity.

I appreciate the Committee's interest and continued support. Thank you again for this opportunity, and I look forward to our conversation. Thank you.

Chairman CARPER. Good. Thanks. Thank you, sir.

Next, Mr. Szykman. Please proceed.

TESTIMONY OF SIMON SZYKMAN,¹ CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF COMMERCE

Mr. SZYKMAN. Chairman Carper, Ranking Member Coburn, members of the staff, I am pleased to have been invited here today to discuss with you ongoing efforts at the U.S. Department of Commerce aimed at eliminating duplication and improving outcomes associated with the Department's information technology investments.

¹The prepared statement of Mr. Szykman appears in the Appendix on page 47.

I have been the Chief Information Officer at the Department of Commerce for just over 3 years and spent over 3 years before that as the CIO at the National Institute of Standards and Technology. And in my 6 years in the role of CIO, I have spent much of my time working to improve efficiencies and governance in the organizations that I have supported. Over the past 3 years, Commerce has taken a variety of steps to strengthen governance relating to its IT investments as well as to improve the efficiency and effectiveness of IT spending at Commerce.

We have made significant advances in strengthening governance, both generally and specifically in the area of IT. Since 2010, Commerce has significantly improved how it conducts oversight of IT investments through the establishment of a new Office of Program Evaluation and Risk Management (OPERM), and through existing mechanisms such as our IT Review Board, our IT Dashboard Review and Assessment Process, and TechStat reviews.

Last year, then-Commerce Deputy Secretary Dr. Rebecca Blank recognized the importance of CIO authorities in the quest for greater efficiencies in the Department's IT spending. She directed me in my role as CIO to develop an IT Portfolio Management Policy, which was subsequently issued in June of last year. The provisions in this policy give the Commerce CIO a greater role in setting department-wide architecture standards, identifying and implementing shared services, supporting department-level budget formulation, reviewing IT investments, and managing the IT workforce at the Department.

The new policy and related delegations have provided significant new support for several of the initiatives I will be discussing today.

The Commerce IT Portfolio Management Policy has led to a broad push into shared services, both within bureaus and across bureaus. My written testimony includes several examples of shared services that have been implemented within Commerce bureaus. In some cases, implementation of cross-servicing models has extended beyond individual services and covers a complete suite of IT services.

At the beginning of this fiscal year, Commerce's Minority Business Development Agency transitioned its full portfolio of IT services, staff, and infrastructure to the Office of IT Services within my office. A similar transition of services is underway for the Economic Development Administration (EDA).

At the department-wide level, Commerce's Enterprise Continuous Monitoring Operations Initiative, currently in implementation, will deploy a single security continuous monitoring infrastructure across the entire Department. Next year we are expecting to establish for the first time an enterprise security operations center that will provide department-wide analytical capabilities and improve our ability to respond to and detect cybersecurity incidents.

In addition to these shared services initiatives, data center consolidation efforts are also underway across Commerce. In the headquarters building, several bureau level data centers or data facilities have been closed and consolidated into a single data center that supports all of the occupants of the building. Among the larger bureaus, we also have several bureaus that are now hosting equip-

ment that belongs to the smaller bureaus, which had previously been located in independently managed facilities.

Commerce has also been making use of strategic sourcing as another mechanism to improve the efficiency of our IT spending. In 2011, the Department had over 100 contracts for purchasing PCs. In January of last year, we replaced those contracts with a single contract supporting the entire Department, and we are now realizing savings of 30 to 35 percent for every PC, desktop, and laptop computer that we purchase.

Since that time, a number of other department-wide strategic sourcing vehicles have also been put into place, and several examples are provided in my written testimony.

The benefits of strategic sourcing contracts go beyond just the direct cost savings. They also provide significant improvements in terms of managing of existing staff resources, because it allows our existing acquisitions staff to focus on local requirements and mission-unique requirements rather than replicating the effort of focusing on commodity investments that are common to multiple organizations.

In order to maintain a department-wide focus on implementation of improvements in portfolio management, my office and all of Commerce's bureaus have been asked to include reporting on IT priorities in our quarterly performance updates. Through the Department's balanced scorecard process, the Office of the Secretary, the Secretary, and Deputy Secretary track outcomes-oriented measures and have covered a range of initiatives, including updates on implementation of shared services, strategic sourcing initiatives, bureau IT portfolio management plans, and improvements to Commerce's IT security.

I am pleased to have had the opportunity to discuss with you today the evolution in IT portfolio management at Commerce. Although we have many accomplishments we are proud of, we recognize that many more opportunities lie ahead of us. And with support from the Office of the Secretary, we intend to press aggressively forward to pursue these opportunities.

The benefits we have realized from these initiatives are merely representative of more fundamental changes to IT management that is going on at Commerce. Commerce leadership has worked together to take on one of the most significant challenges facing senior IT leadership: The need for greater empowerment to support better decisionmaking needed to drive efficiencies and improve effectiveness of IT spending across all Federal agencies. The policies, plans, and initiatives that have been instituted have created a foundation for sweeping changes to how IT is being managed. The results of these portfolio management efforts are only starting to be realized, and the ultimate impacts are expected to grow over time.

Thank you very much.

Chairman CARPER. Thank you. Mr. Baitman.

TESTIMONY OF FRANK BAITMAN,¹ DEPUTY ASSISTANT SECRETARY FOR INFORMATION TECHNOLOGY, AND CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Mr. BAITMAN. Good morning, Chairman Carper, Ranking Member Coburn, and Members of the Committee. My name is Frank Baitman, and I am the Deputy Assistant Secretary for Information Technology and the Chief Information Officer at the U.S. Department of Health and Human Services. I am honored to join you here today.

The work of this Committee is crucial to the effective management of government resources. Information technology is deeply integrated into the business of HHS, and we are continually focused on delivering improved results through our portfolio of investments.

The Department of Health and Human Services is a large knowledge-based organization. We deal with health and human services spanning fundamental knowledge to delivery, from applied research to the regulation of drugs and devices, from public health preparedness to the reimbursement for medical services. Each of the many missions at HHS is managed by a distinct operating division, and each division has their own Chief Information Officer.

Given this federated structure, my role as the Department's CIO is to have a holistic view of the entire HHS enterprise. With that high-level view, my responsibility is to ensure the various distinct missions being carried out across the Department are supported by a secure, cost-effective IT infrastructure. I believe this affords me a unique vantage to reduce duplication and streamline operations. But just as importantly, because we are a knowledge enterprise, there is great value in promoting collaboration and enabling information developed in one corner of the Department to flow freely to others who can use it to advance public health and human services.

In my 15 months at HHS, we have seen some notable successes in providing that kind of secure, cost-effective infrastructure for the Department. Just a few weeks ago, we announced that through the FedRAMP process, HHS had granted Amazon Web Services (AWS) an authority to operate. I highlight that accomplishment because, with the authority to operate, the entire Federal Government could now quickly and confidently use Amazon Web Services for their own business needs, knowing that this vendor meets strict Federal cybersecurity standards.

I am proud that our team did such a thorough job of building a robust process that other departments are now asking to replicate our approach with other vendors. So with that one project, we have created real value not just for HHS but for the entire Federal Government. And as other cloud service providers are approved through the FedRAMP process, we will create a competitive environment that ultimately benefits the American taxpayer.

That is a good example of providing the infrastructure I talk about. When it comes to preventing duplication and streamlining operations, we are also excited about some of the structural and procedural advances we are making at HHS. Most importantly, I

¹The prepared statement of Mr. Baitman appears in the Appendix on page 52.

think, is our recently implemented IT governance model across HHS.

Because the majority of the Department's IT resources are tied directly to our programs and our operating divisions, we have established three IT steering committees to bring together technology and program leaders from across these divisions. That is a key point I would like to emphasize. We believe that the best investment decisions are made when both the IT and program leadership collaborate and there is executive ownership to drive agreement to closure.

These three committees bring together technical and business leaders to take a functional view of health and human service systems, scientific research systems, and administrative and management systems to provide functional oversight across the Department's IT portfolio.

Some of these priorities we are driving at HHS, but I would also like to recognize the impact of administrative initiatives on the technology direction we are taking at HHS, including those priorities I have just described.

PortfolioStat that we have talked about this morning in particular is proving to be a valuable tool. As with everything I am talking about here, knowledge and transparency are key to success. The first iteration of PortfolioStat helped the most by making sure that we shared IT planning information across our enterprise in a clear and consistent way.

Second, PortfolioStat provided a mechanism to drive a conversation within the Department about department-wide IT consolidation activities. One of our most comprehensive consolidation efforts currently underway is the Hire-to-Retire IT modernization program. Moving the IT systems that support our core human resources, payroll, and time and leave functions to a shared service provider. We are effectively outsourcing a commodity activity and getting a better, more cost-effective solution than we have in-house today. By the completion of this effort, we will have sunset at least ten legacy systems, and we will have consolidated multiple conflicting H.R. data sources into a single authoritative system of record. PortfolioStat helped us push forward on this effort.

We are also evaluating the prospect of consolidating our six existing e-mail systems and moving them to a cloud e-mail provider, which we expect could have comparable benefits to the Hire-to-Retire effort. And, of course, we are looking for more opportunities like these across the Department.

To be sure, there is an opportunity to improve the management of IT activities, but that does not necessarily mean that centralization is the right solution in every instance. Mission-related technologies and business operations are often best driven by those closest to the mission. What is important to me at HHS is striking a balance so that I can provide the support that I am expected to provide while not getting in the way of anyone accomplishing their specific mission.

As the CIO at HHS, my job is to make sure we effectively and efficiently manage our information resources. To be successful, we need to leverage our new governance structure to identify similar functions that take place across the Department through a strong

business IT partnership. When dedicated individuals from across the Department come to the table with this knowledge, we can make enterprise decisions that reduce our administrative overhead and allow our programs more resources to accomplish their vital public health and human services missions.

Thank you for the opportunity to appear here today.

Chairman CARPER. Thanks so much, and thanks for coming and telling that story. That is good.

Mr. Powner, glad to see you. Please proceed.

TESTIMONY OF DAVID A. POWNER,¹ DIRECTOR, INFORMATION TECHNOLOGY MANAGEMENT ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. POWNER. Chairman Carper, Dr. Coburn, we appreciate the opportunity to testify on the Federal Government's efforts to address duplicative IT spending and save taxpayers billions of dollars.

The Federal Government spends \$80 billion annually on IT, and the past several years has resulted in major improvements in the transparency in the return on these investments. For example, the Federal IT Dashboard provides a CIO assessment of over 700 major IT investments, and the information has been used to terminate and rescope underperforming projects, and according to OMB has resulted in almost \$4 billion in life cycle savings.

In addition, the data center consolidation effort was initiated to improve the government's low server utilization rates, which was estimated between 5 and 15 percent, far below the goal of 60 percent. This effort is to result in closing 1,000 centers and save \$3 billion.

Despite great progress on these initiatives, much more needs to be done since the Dashboard currently shows that we have about 160 projects at risk totaling \$10 billion.

Dr. Coburn, to your point, these numbers are understated because we still have the Department of Defense reporting no red investments when we all know it has many, and on data centers, our report delivered last month for this Committee showed that OMB, the General Services Administration (GSA), and the Data Center Task Force need to step up efforts to track cost savings and define metrics further for those centers that remain to optimize performance.

Also, we are 3 years into the data center consolidation effort, and the government still does not know how many centers it has. Just last week, we learned that about an additional 3,000 data centers are now being reported, bringing the government's total north of 6,000 data centers.

Turning to duplication, this \$80 billion IT spend has many duplicative investments that OMB, to its credit, is attempting to tackle with its latest IT initiative called "PortfolioStat." Before I comment on OMB's efforts, I would like to present some numbers on the amount of duplication that exists.

We issued a report that highlighted hundreds of investments, providing similar functions across the government. These numbers

¹The prepared statement of Mr. Powner appears in the Appendix on page 57.

are staggering. For example, annually the Federal Government has invested in 780 supply chain systems totaling \$3 billion, 660 human resources systems totaling \$2.5 billion, and 580 financial management systems totaling \$2.7 billion. Again, these are annual expenditures. We recommended that Federal agencies ensure that these IT investments are not duplicative as part of their annual budget submissions.

Mr. Chairman, following that review, we reported on our deeper look into investments at the Departments of Defense, Homeland Security, and Energy. Specifically, we looked at over 800 investments at these three agencies associated with human resources, IT, and supply chain management. We found 37 investments in 12 categories that were duplicative. For example, the Air Force had five similar contract management systems, the Navy had four similar personnel assignment systems, and Energy had very similar back-end infrastructure investments. Addressing this duplication is important since Defense and Energy had planned to spend about \$1.2 billion on these investments over a 5-year period. Our report highlighted the details of these investments and made recommendations to eliminate duplication.

I would like to comment here that if auditors could find this duplication within agencies, there is no excuse for IT investment boards and agencies' CIOs not to do the same.

The good news, Mr. Chairman, is that each agency has actions underway to tackle this duplication, and in March of last year, OMB initiated their PortfolioStat initiative to tackle this proliferation of duplicative investments. We currently have a review underway for this Committee where we are evaluating each of the agencies' plans to tackle duplication.

OMB in its most recent memo specifying PortfolioStat guidance States that the results so far have been significant and that there are nearly a hundred opportunities to consolidate or eliminate duplicative IT investments, like mobile and desktop contracts. This initiative is to result in savings of approximately \$2.5 billion through 2015. The latest PortfolioStat initiative is promising if carried out effectively. However, I would like to offer four specific observations regarding it.

No. 1, cost savings are much higher than \$2.5 billion. Our current review shows that agencies collectively are reporting \$2.4 billion in potential savings, and this is without four agencies reporting, including the Departments of Defense and Justice (DOJ). Clearly, DHS is the gold standard here. Their estimated cost savings are \$1.3 billion, accounting for more than half of the reported savings.

No. 2, metrics and transparency are needed to be successful, and our latest data center report shows that the Administration can do a much better job in these areas.

No. 3, CIO authorities need to be strengthened at many agencies if CIOs are to carry this out. We are currently learning that not all CIOs have authority over commodity IT, which is not a very high bar.

And, No. 4, over time, portfolio management needs to be expanded beyond commodity IT and include all IT investments if we truly want the \$80 billion effectively managed.

In summary, Mr. Chairman and Dr. Coburn, many of the initiatives over the past several years have improved transparency. They have also resulted in better management of large IT acquisitions and technology operations, and there has been some elimination of duplication. However, each agency needs more leadership, and also there needs to be more leadership out of OMB if we are truly to do this right over time.

Dr. Coburn and Chairman Carper, this concludes my statement. Thank you for your leadership on this topic, and I would be pleased to respond to your questions.

Chairman CARPER. Good. Thanks very much for that statement, David.

I am going to come back to you and just ask you to start off. Let us go back in time. Eighteen years ago, Bill Cohen, a Senator, sat in this room and talked about the legislation that ultimately became the Clinger-Cohen law. Just think out loud for us what their vision was. What was their vision all those years ago?

Mr. POWNER. Well, there were two large areas in that bill. The vision was to give CIOs more authority, to have them report to the agency head and for them to have a seat at the management table. I do not think that has happened.

The other big vision was IT investment management. It was to create a governance process on how we choose investments and manage those investments on an annual basis. And that is clearly what Steve is doing with his PortfolioStat initiative. But we have some agencies that do a decent job on their IT investment management. We took the Internal Revenue Service (IRS) off the High Risk List this year. They have a pretty solid governance process. I think DHS was trying to do things, and that is why they have the high reported savings on PortfolioStat. But that was the vision, to have a real strong leader and to effectively govern the IT investments.

Chairman CARPER. All right. I was talking with someone the other day about the role of the executive branch versus the role of the legislative branch, and one of the things we do, we legislate and try to create policy, with input from the executive branch, but we do not execute. That is the role of the executive branch. And a big part of our role is to come back from time to time and do oversight to see how are they doing with respect to this vision laid out all those years ago by Bill Clinger and Bill Cohen. How well are we meeting that vision, measuring up to that vision?

When you think—and there are some bright spots here. This is not all doom and gloom, as you suggest. We have a couple of bright spots that are represented here by Mr. Szykman and Mr. Baitman. But in terms of why significant parts of this vision have not been realized and what the Administration needs to do further and what we need to do further to better ensure that the bigger pieces have been realized, give us some good advice here today.

Mr. POWNER. This goes back to many years when we were at the Subcommittee holding hearings on this. I think one of the keys is transparency. We have fought for years and this Committee was essential on getting an accurate list of troubled projects so that we could do something about it. It goes back to the Management Watch List and the High Risk List, and that was not always trans-

parent. We now have the Dashboard. And, Dr. Coburn, I agree with you. DOD, what is on there for DOD is not accurate. But you have other agencies that—

Chairman CARPER. Say that again about DOD.

Mr. POWNER. It is not accurate what DOD is currently reporting. I mean, they are reporting no red investments, and, in fact, they have red investments. We highlighted that in a report a year ago, and we think something should be done about that. You cannot fix a problem on your acquisitions if you do not acknowledge that you have a problem. And it is just important that we have accurate information. Steve has a great process in place, the TechStat process that tackles a lot of these red and yellow investments. We need more of that.

So I think it starts with transparency. Also, you need effective leadership. But then there needs to be follow-through. Over the years we have seen many good plans, but we never drive them to closure.

Chairman CARPER. OK. In terms of leadership, Dr. Coburn and I have been working with Sylvia Burwell to try to help make sure that we have a leadership team at OMB in place. And a guy who has come out of this Committee has been nominated by the President to be the Deputy OMB Director. I think his name was hotlined yesterday. I do not know if he got through in order to be confirmed. But Sylvia has been pretty much, in the month or so she has been in place, not running the show but, I mean, there is no confirmed Deputy OMB Director, there is no confirmed Deputy for Management, there is no one confirmed to run the regulatory part of the House at the Office of Information and Regulatory Affairs (OIRA). And they got Danny Werfel over there running the IRS instead of being in our control. There are just huge leadership challenges. One of the Administration's responsibilities is to nominate good people, and one of our responsibilities is to vet them when they do, and if they measure up, to get them confirmed.

Let me come, if I could, to either of our witnesses. I will go back in time. Let me put this in some context. In my old role as Governor, I used to say to my cabinet from time to time, when we were dealing with a particular challenge, I would say, "Somebody in some State, some Governor, has faced this challenge, and they have dealt with it effectively. Our challenge in Delaware was to find out who had done it and to go out there and see if that result, their methods were transferable, exportable to us and could be right-sized in what we could learn from them.

Commerce, the Department of Health and Human Services, you all are doing something right here, and the reason why we asked you to come today and testify is because we think you set an example for our other agencies, certainly for the Department of Defense but for others as well.

What is it about your two agencies that have enabled you to stand out in the crowd here, to receive not brickbats but some bouquets for a change?

Mr. SZYKMAN. I think where I want to start is just by saying that I cannot overstate the importance of senior leadership support. Of anything that I could conceivably take credit for accomplishing over the past 3 years, I would not have been able to do it without sup-

port from the chief financial officer (CFO) of the Department, Scott Quehl, who left back in January, and then Dr. Rebecca Blank, who at varying times was the Acting Deputy Secretary—Deputy Secretary and Acting Secretary.

The support from leadership at that level has been critical in not just changing policies but really driving and assessing outcomes. I mentioned earlier our internal performance management process, our balanced scorecard process, and holding all of the bureaus accountable from the senior levels at the Office of the Secretary through that process has helped ensure that the entire community, not just CIOs in the department-wide IT community, but senior career people, chief operating officers, chief financial officers, and bureau chiefs have been very strongly supportive and aligned with the priorities coming out of the Office of the Secretary. So I think the—

Chairman CARPER. But it all starts with leadership, doesn't it? It all starts with leadership.

Mr. SZYKMAN. It does.

Chairman CARPER. Yes, OK. Mr. Baitman, go ahead, and then I will turn it over to Dr. Coburn.

Mr. BAITMAN. Well, I will say ditto, it always starts with leadership and I think that is foundational.

One of the things that we are doing at HHS that I mentioned in my opening remarks is the new governance structure that we are putting in place. We recognize that we did not have an enterprise-wide view of investments, and because of that there was redundancy, there was waste.

The new governance structure that we are putting in place—and we are right in the midst of doing that right now—is going to give us a view where we can sit down with business leaders and technologists and say, these are the systems that we are spending our money on. Is there a better way of doing this? Is there an opportunity to take these multiple systems, consolidate them, and move to a better place as we modernize.

I think that it gets back to the issue of transparency. When you know what you have, you can actually manage it.

Chairman CARPER. All right. Thanks. Dr. Coburn.

Senator COBURN. Well, thank you. Steve, I think you have done a good job at OMB, and I appreciate you coming out of the private sector and serving the country.

My real concern is, as I said in my opening statement, how do we empower CIOs, and I was really worried as you—the decision came out of OMB to not mandate that the CIO was head of your latest program, and so we have, what, five agencies where we did not make the CIO head of the PortfolioStat. In other words, we have five agencies where the Secretary decided not to make the Chief Information Officer head of it. And my thought is that what we have done is disempower the CIOs in those agencies as we are going to do this. Because if you go back to quote Mr. Szykman or Mr. Baitman, leadership was the key, and buy-in, and Mr. Baitman has experience at a couple of agencies. At one he had buy-in and at one he did not. And so consequently one of them is a mess, and the one that is getting better, he has management buy-in.

So would you comment on that decision? Rather than really strengthen CIOs, what you all did is allow Secretaries the capability to not utilize that.

Mr. VANROEKEL. Well, I am not really sure about the decision in particular on PortfolioStat. CIOs, of course, are central to the leadership team to execute on that. Two points.

One is the first memo issued by my office when I got this job in 2011 was specifically on CIO authorities. It was M-11-29, basically reminding agencies of their obligation to empower CIOs, especially in the area of commodity IT and other things. Connecting the dots to today and going back into the past, as Senator Carper has referenced, the Clinger-Cohen Act actually begins by saying "the head of agencies shall," and it is very specific about empowering the head of the agency, the Secretary, the Deputy Secretary, Chief of Operations, et cetera, to take ownership for the IT resources and to focus on that.

What I have found in PortfolioStat and my agenda when conducting these face-to-face meetings was really to teach agencies how to run a private sector investment review board, how to get all the C-level executives together in a room and understand, to meet the mission of their agency, to serve the American people, to reduce, maniacally reduce duplication, and to save money. That is a motion across all of the executives, not just the CIO. You have to have tight alignment with the human capital person who is thinking about expertise. You have to have the acquisition officer sitting at the table thinking about how they make that happen and realize the duplication and drive that out of the system.

And so the convening of PortfolioStat, I do. I sit across the table from the Deputy Secretary, and they are flanked by all their C-level executives, and then we have that discussion on how they are going to realize this across the myriad of management initiatives they do in their agency.

Senator COBURN. The point is that the vast majority of the agencies did use their CIO to do this, but in your guidance, the National Science Foundation (NSF) did not, Social Security Administration (SSA) did not, USAID did not, the Veterans Administration (VA) did not, Treasury did not, DOJ did not, the United States Department of Agriculture (USDA) did not, and the Department of Transportation (DOT) did not. So my point is, my opening statement, what you have is a couple examples here where leadership matters and bought in and we have given authority, but we have to also give the authority to Chief Information Officers to actually make the difference. And what you all put out did not mandate that. Where you could have mandated it so that you would have empowered the CIO everywhere, instead you empowered in 12 or 13 agencies. I know there are other ways to skin a cat, but my preference would have been to empower CIOs.

Let me go to my list. Let me ask, David, do you have any criticisms of having somebody other than the CIO in charge of PortfolioStat?

Mr. POWNER. I think when it comes to IT investment management, the CIO should be the key executive with the support of those other C-level executives. When I saw the PortfolioStat process being rolled out, I think what it did was it helped those CIOs

get a seat at the table where they did not have one. And I think to Steve's credit, I mean, that is part of what—there was an acknowledgment that a lot of them did not have that authority.

Senator COBURN. Yes, I agree.

Mr. POWNER. And I think in that sense, I think that was the whole purpose, to try to elevate their position within the agency with having Steve sitting there saying we have got duplication, let us admit it, let us tackle it the right way and go about it. So I think that was good. And, again, I think the key is now let us followup on that. We have these 100 opportunities, 2.5, it could be double that amount if you throw DOD in there.

Senator COBURN. Well, if I just added up what he indicated in his testimony, it was well in excess of \$30 billion. The way you get rid of trillion dollar deficits is a billion dollars at a time. So if we just did the recommendations, that if we could actually execute what GAO has outlined, you are talking \$300 billion over the next 10 years, and it is ripe.

Just a couple of little questions. On the H.R. stuff that you are consolidating, is that a fixed-price contract?

Mr. BAITMAN. We are actually outsourcing it to another shared service provider in the Federal Government, the Department of Agriculture's National Finance Center, which is in New Orleans. So it is basically a fixed-price contract in that you get charged for the number of seats that they are taking on.

Senator COBURN. OK. So you know what the cost is.

Mr. BAITMAN. We do.

Senator COBURN. And so you do have a comparison.

Mr. BAITMAN. And, in fact, we are estimating roughly \$6.5 million a year in continual savings.

Senator COBURN. Great. And one other question, Steve. So you have the CIOs of the different agencies come together and share some of the things that Simon has mentioned in terms of here is where—in other words, is there a learning process between the CIOs across the Federal Government so that they can take the good work that Simon has done or Frank has done and share it with other people?

Mr. VANROEKEL. Yes, sir. We convene the CIO Council every month. Every other month we focus on cybersecurity specifically and then the off months we convene. I also host an executive committee that gets together. It is the largest agencies. It is a smaller group, and we meet on a very regular basis.

The other thing, actually 2 weeks from now, I am hosting something we now call "CIO University," which is getting new CIOs in the government together. We do this at the National Defense University to sit down for a deep dive for a day, bring in a myriad of professionals across different disciplines—acquisition, finance, procurement, or procurement acquisition—all those to teach these agencies best practices and get them hitting the ground running on this.

We have a lot of turnover in the IT ranks in government, so I think it is important to convene on a very regular basis. Part of the CIO University work we shipped last year something we call "CIOipedia," which is an online resource for government CIOs to

take advantage of to learn to quickly search and dive into best practices and to take that forward as well.

Senator COBURN. Is part of the reason we are having turnover because we cannot compete in the IT field for CIOs?

Mr. VANROEKEL. I think that is a big part of it, and there is so much demand in the U.S. economy.

Senator COBURN. Is that something we should legislate on to give agencies more flexibility in terms of payments to be able to be competitive in the IT field?

Mr. VANROEKEL. I think, the uniqueness we have in the Federal Government is not necessarily pay. I think from the incentive structure that exists in the private sector versus here, the thing we have in the Federal Government is really the breadth of the experience. If you come in as the CIO of the Department of Veterans Affairs, your ability to affect a very large budget, a very large staff, and things like that is unparalleled in the world and will build skills for you, and muscle, that you maybe never had.

I think we need to actually work on that, and as we think about CIO authorities and really—my vision of CIO authorities is the central CIO should really be the hub for all the commodity computing. There should be one help desk. There should be one e-mail system, one way to buy a computer, one way to get mobile. And that CIO should also then provide services to the CIOs sitting on the periphery.

Senator COBURN. Right.

Mr. VANROEKEL. I want the CIO of the Federal Aviation Administration (FAA) to wake up every day thinking about flight safety, and I want them to think about flight safety when they go to bed at night. I do not want them to wake up and think: Is the e-mail up and running? How are BlackBerrys going? I have to acquire this. What is the throughput on my help desk? That should be done elsewhere, and we should focus the professionals on the mission at hand and get the centralization happening to root out duplication and drive everything in a do-one, use-often methodology.

Senator COBURN. OK. Tom, I will come back.

Chairman CARPER. Let me just go back to one of the points that Dr. Coburn was raising with you, and that is, whether or not Federal agencies have the flexibility to hire the talent that they need. We had a tough time in State government in Delaware retaining IT personnel, and what we ultimately did, gosh, in this last decade, is we took them out of the merit system, and we said to the agency, pay people what you need to pay them in order to be able to attract and retain good talent.

Just to followup on Tom's question, is that a problem or not in the Federal Government? It sounds like it is maybe not as much as I might have thought.

Mr. VANROEKEL. At the top ranks, I do not think it is much of a problem. We have a turnover rate of about 18 to 24 months, which is pretty average I think in the Federal Government for some senior positions. It is below that I think we have some of the issues. If you look at cybersecurity in particular, the private sector is able to attract talent at a rate that is much higher than the Federal Government. We are doing things to mitigate that, working with Homeland Security on new training to train the people that

are on staff and to drive that forward. But with technology jobs in this economy growing at 4X any other category, it is putting a strain on the ability for us to bring and retain talented people across the myriad—throw into that, sequester impacts and furloughs and things that are causing other issues. My biggest concern with the sequester and furloughs is actually the talent drain that we are beginning to see now, and if we continue, I think will drive forward.

Chairman CARPER. OK. I do not think we have talked much about what kind of—I talked about lessons learned from the Department of Commerce, from the Department of Health and Human Services, from the rest of our Federal agencies. How about the private sector? What are some lessons learned that we can take from them, particularly some of the larger enterprises, one of which you worked for a number of years? I will just start with you, Steve, if you would, just lessons from the private sector that we have learned, that we are acting on, and maybe some that we ought to.

Mr. VANROEKEL. In the private sector, I was part of a team—my last job at Microsoft was part of a team that was in the server division and had you spun the team off the day I left, it would have been a very large software company on its own right. And we had, under the 4 or 5 years I was there, 26 consecutive quarters of double-digit growth. I think we were doing things right.

The amazing thing for me was we never grew our budget. Our spend on marketing, on product development, and all that stayed very flat, if not declined, because the dollars we were generating on the balance sheet were going to fund other aspects of the mission. It was funding new emerging businesses to expand the portfolio to affect the stock price and things like that. And that mentality does not necessarily exist in government. If you go and do the hard work to find savings or to drive your costs down, that return on investment often is not realized where you sit. It goes somewhere else, and there is not this aggregate sort of notion of the mission to think about how am I driving value for my entire department that is going to bring value to the American people, et cetera. And so you tend to have people that, when they get something, they put their arms around it, and they fiercely defend their budget or their ability to—you take things away from them. And so I think the current fiscal environment, we have to look at two things. One is the forces acting on these groups. The current fiscal environment helps us a lot, cybersecurity helps us a lot to create the mechanisms to have those conversations. And the second thing is to really think hard about the incentive structures. What incentivizes these groups inside these agencies to do this hard work, to provide a better return?

And so I think to get there, because to date that has largely been an ideology discussion, two people doing the same thing in the Department, they just have to—they are never going to work it out on their own on which one should stop doing it and which one should be doing it. We need data, we need analytics, we need to be informed on how to understand who is getting the best return on investments (ROI), who is getting the best result, and how do we then create the right structures to eliminate that.

So PortfolioStat gets us part of the way there. I, as part of PortfolioStat, stood up a very modest small group inside my team to actually get me data and analytics. That is what you are now starting to see, and enhancements in the Dashboard and the reports that come out of our PortfolioStat work.

The President's 2014 budget actually proposes a similar effort that I proposed to actually expand that evidence gathering to programs and grants so we can actually look beyond IT and to think about how can we get real data and analytics to understand what works and then pour our dollars into what works and eliminate the duplication on things that are not working. And so I think we have big potential there if we do it right.

Chairman CARPER. Anybody else? David Powner. Anybody else on lessons we might learn from the private sector?

Mr. POWNER. Well, in the private sector, if you look at governance and how they oversee their portfolio of investments, you would never have a situation where you have this duplication that exists. And the other thing, when their program is in trouble, governance boards get after it. They cannot let this linger for a long period of time. And everyone knew that you had to escalate issues and report accurately. That is what we do not have here. We do not have the governance that is really needed, and that goes back to Clinger-Cohen, what was envisioned, what Steve is trying to do.

One other comment, too, is in the private sector you tackle things incrementally. We talk about agile development now like it is something new, but that is something that I did in the late 1990s, going small in development. We still try to do too many big bang approaches when we tackle these acquisitions.

Chairman CARPER. Let me stick with that for just a second. A lot of times when I get to the end of a hearing, I will ask what are the takeaways for us in terms of a to-do list for us on this side of the dais. And just to followup on what you just said, what are some things that we need to be doing that we are not doing. We get a lot of advice to do oversight, and we do quite a bit of that. Maybe not enough, but we do a lot. But what should be our takeaways from this?

Mr. POWNER. Well, I think this is a good start because I think this PortfolioStat process has—there is great opportunity here, 2.5 billion plus how ever many billion when everyone reports this. And I think this is a good place to start, that we drive this to closure and we eliminate duplication here. But then there are other things going forward. I think using the Dashboard to still tackle those troubled projects is really needed. We still have those failures at DOD that just occurred, and those are things we need to avoid.

Chairman CARPER. OK. Dr. Coburn.

Senator COBURN. Steve, let us talk about the Dashboard for a minute and DOD. TechStat works, does it not? And the fact that DOD has no programs, everything is green for DOD, which means they are ducking having TechStat work on 20 to 30 programs that are in trouble. How do we fix that?

Mr. VANROEKEL. Because I am a very data-driven person and when personalities are involved or personal inputs or ideology is involved in assessing programs, I do not warrant that as a triggering event. We do not use red, yellow, green as the event that says we

should go TechStat. We look much deeper. Are things on budget? Are they on schedule? All of that, that systems report, that technology reports into us are the things we use to go in and look at investments. Just asking someone to self-assess their program—

Senator COBURN. Well, let me ask the question another way. When was the last time TechStat has been applied to a DOD program?

Mr. VANROEKEL. We do TechStats on—I am actually very actively involved in the joint work of DOD and VA on the electronic health care system, and there is an ongoing TechStat right now. I have actually got meetings here on the Hill this afternoon to talk more about that. So that is the most recent one.

One of the things that the system was not reporting to me is, as you can imagine from a behavioral insights standpoint, people have the ability to go in and change the delivery—the deadlines on their schedule, to change their budget allocations on the IT Dashboard. And prior to my arrival, we had no visibility into that. And so if you saw something green, it looked on budget, on schedule, et cetera, it looked like everything was good. One of the features I added under my watch was a triggering event that would tell us every time someone went in and re-baselined any of their metrics. So now when you go to the IT Dashboard, you can actually see on this date someone went in and changed their due date; on this date someone reallocated their budget in some way to this or that project. That then creates a triggering event for us.

Another key thing that I have driven relative to the Dashboard is—we are a very modest team over in OMB doing this level of oversight. Of course, we partner with Dave in GAO a lot on thinking broadly about reforming Federal IT. But we do not scale across the entire Federal Government. And so we have trained over 1,000 people to conduct TechStat reviews, and what you are starting to see and what we are encouraging through PortfolioStat and other mechanisms is that TechStat has become a regular order of business, that when things are going awry, when things are triggering, then they send in, they parachute in the TechStat people to look at these investments and run our methodology against it.

That being said, I still get involved with TechStats and step in on ones that are important.

Senator COBURN. One of the things that I have noticed, 3 years ago I outlined an Air Force program, an IT program, said we ought to cancel it. We did not cancel it. We canceled it this year and paid an \$80 million cancellation fee.

One of our problems in purchasing IT—and the reason I asked about fixed-price contracting—is when you have contracting other than fixed price, what happens is either the person that is making the decision or the company that is not performing, there is no consequences. And in the private sector, if you contract for something and somebody does not perform, you hold them accountable.

Now, you either do that privately or you take them to a civil court and get money damages for not performing under a contract. The other thing they do in the private sector is the person who made the blunder does not have a job anymore.

And so how do you incorporate that into what you are trying to do in terms of guidance? I have a son-in-law that is very good at

this stuff. He travels all over the country. He is a fixer for a big firm. And what he tells me is business is not much better than we are about this nebulous area of IT, and so they are kind of held up, too, in not knowing what they are going to get or maybe not knowing what they want when they start a contract.

How do we get a handle on that?

Mr. VANROEKEL. I think the other phenomenon you see is that planning costs suck up the entire initial allocation of funding, and we have very expensive three-ring binders sitting around on shelves in this town that people paid planning costs for.

I think the way we get around it is, I love to use the analogy, the football analogy of, how many—you or I could easily throw a football to someone a few yards away with a high level of—

Senator COBURN. Very few, in my case.

Mr. VANROEKEL. But with a high level of assurance, I could hit someone that is that close. There are very few elite quarterbacks who can throw a 50-, 60-yard pass and hit someone with a high level of accuracy, especially on the move.

From a product manager standpoint, we have a lot of product managers in government that can hit the 90-day deliverable. They can hit it, they can deliver on it, they can get it on time, on budget. We have very few product professionals inside the government who can hit the 5-year deliverable, the 4-year deliverable with any level of accuracy way down the road. And so the goal here—and, the things we have been doing inside—and the guidance I have been issuing have been really to the goal of, let us let 2013 mark the end of the multiyear big giant deliverable and break everything down.

Last summer, Joe Jordan, the head of Federal Procurement Policy, and I issued modular contracting guidance. That was the first step to teach the acquisition community how to actually break these big monolithic deliverables down into a lower risk surface so you are not doing these big whale things that are likely to fail, and so trying to get those down.

And then what we have been doing is the open data Executive Order that just came out, the digital strategy in May 2012 and all the moving parts associated with that, all lead us to these small interoperable components that can be reused inside government. We need to build a community around that. We need to build private sector capability there. And so we are putting all the pieces in place to make small and modular—to Dave's point, when he said we were doing this in the late 1990s about modular and agile development, that needs to be the new normal inside government. We can no longer do these 5-year, \$100 million—if I ever see those, those are like an instant TechStat trigger for me, and I go in and I say, OK, what is your 90-day deliverable? We are going to break this thing down. And in the cases where I have done that, they have turned out successful.

Senator COBURN. Yes. So that is called management.

Talking about DOD and TechStat, we have this report, the Integrated, Efficient, and Effective Uses of Information Technology (IEEUIT) Report. How does Congress know what is happening in DOD if it is not ever reported?

Mr. VANROEKEL. The IEEUIT Report reports savings reported from—it is a net we cast, and we ask the agencies to come back and report against our initiatives, and we pull this back in.

A change I made this year is in the 2013 PortfolioStat guidance, one of the things I needed to do is just kind of cleanup my own shop. What I found out is—I was wanting to understand what burden we were putting on agencies, just hit—compliance of OMB guidance. What I found was that we were asking agencies to report over 30 times in a year the—

Senator COBURN. Which consumes resources.

Mr. VANROEKEL. Which consumes a lot of resources. And so I asked the team to print that all out, lay it on the table, let us understand where we duplicate our requests and things like that. We are now down to three. In 2013 with the PortfolioStat guidance, we do three of them. They are basically an information resource plan, a strategic plan, and then I ask them to do quarterly reporting. At the end of every quarter, they are going to report in on savings and metrics against the initiatives we have done. And so that is now ordered to every agency, and we are starting that process. We just got the plans in on May 15, and then the quarterly reports are going to start, and DOD will be one of those as well.

Senator COBURN. I guess I will wait, and we will go on to Kelly.

Chairman CARPER. Senator Ayotte, your timing is pretty good. If you would like to jump in here, you are recognized. Welcome.

OPENING STATEMENT OF SENATOR AYOTTE

Senator AYOTTE. Thank you very much. I want to thank the Chairman and the Ranking Member for this important hearing, and I would ask the witnesses—I wanted to ask Mr. Szykman about the Federal data centers. You had testified that Commerce has been working to consolidate the data centers. But I wanted to know how much of those consolidated centers are actually being used. And the government buys a lot of servers, lots of space for data, and then leaves them mostly empty. And as I understand it, in a 2009 OMB report, the average utilization rate for Federal servers was between 5 and 15 percent. So private sector utilization is often 60 or 70 percent, looking at a cost/benefit analysis. So are we paying for excess capacity? And what is the average utilization rate? Do I have that wrong? And what are the metrics we are using? And can you help me understand how much we are looking at this issue as we continue to invest in this area?

Mr. SZYKMAN. Certainly. I will be happy to answer your question. At the Department of Commerce, I would have to check on precisely what our utilization rates are, and I would be happy to get back to you, but I can tell you without checking the numbers that they are not where they should be in terms of the high percentage of utilization of our servers that we would like to have.

We do have some initiatives that are pushing this forward. For example, within the Census Bureau they have issued a virtualization first policy which requires establishment of virtualized servers before they can create any new physical servers, and this is intended precisely to drive up that utilization rate from low percentages to high percentages. I will be happy to followup with more details.

In general, though, the issue of utilization is an important one. It is not just about the number of data centers but how they are being utilized. And along those lines, I would say that the Department of Commerce has been supportive of where OMB is going with evolving the data center—Federal Data Center Consolidation Initiative, focusing on not just numbers of data centers and closures, but focusing on distinguishing between core data centers, non-core data centers, closing the ones that are non-core, but just optimizing the ones that are core. And that is key because many of the benefits are going to come not just from closing data centers but really optimizing the equipment that is in existence regardless of where that equipment is being housed.

So I think we definitely understand the issue, and we are working on improving, particularly in the utilization area.

Senator AYOTTE. How quickly do you think we could make this happen?

Mr. SZYKMAN. I would say, to be frank, at Commerce things take time simply because we do have decentralized structure within Commerce. And so my office directly manages one of the Department's data centers, and the overwhelming majority of the Department's data centers are being managed at the bureau level. I do know that the bureau CIOs are keenly aware of this issue as well. I mentioned Census has been focusing on increasing utilization. The National Oceanic and Atmospheric Administration (NOAA), which is the bureau where most of our data centers are, they are currently working on a data center consolidation plan to address many of these issues.

Senator AYOTTE. Well, one of the things I hope would just—there is so much, obviously, in this whole area, but we need metrics, we need goals, we need to have results, because we all can sit here and say, well, this is a problem, we are acknowledging it, but until we have—what I would like to see is some metrics on how quickly we can meet them, what is our plan, what are we going to measure in terms of how we get this done.

So I hope that I could get some followup on that because I think that would be helpful to this issue.

Mr. SZYKMAN. Certainly.

Senator AYOTTE. And I also wanted to ask, Mr. VanRoekel, in your written testimony at least—I apologize I was not here for your testimony here today—you state that the CIOs should be empowered, as I understand it. Now, if we empower them, which I want everyone who works for the government to be empowered, and we give them more power within the agencies, I think that we also need to impose greater obligations on them to act on issues of duplication and consolidation as part of their mission. And so how would you—how would we accomplish that? I mean, when you talk about empowering them—and you may have already covered this—what is it that we are going to ask for them to take actual ownership and responsibility for this issue of the duplication and the consolidation of programs doing the same thing? So much of it we see in the Federal Government.

Mr. VANROEKEL. Absolutely, and the empowering nature is really to root out the duplication. That is why we would empower them. Oftentimes—in the private sector, it is unthinkable for a

company to run more than one e-mail system. You just have one and sort of everyone is in the address book and you utilize this as a cost-effective way of doing your e-mail. That is not the norm in the public sector. There are agencies of government that run seven, eight, ten—I have seen more than 20 e-mail systems in an agency. That should be unthinkable.

The reason they are not consolidated into one is often the CIO is not given the authority to go and say the most effective way to do this is to run one. And I think the opportunity here is it begins with commodity computing, things like e-mail. There should be one way of buying a computer. There should be one way of getting a mobile device. And if you saw a couple weeks ago I established sort of what I am calling the “family plan” for government so we start to pool our minutes and things like that to start to save money in the mobile space.

So all of that should be centralized under the authority of the headquarters and the CIO. And then the next step is to let that CIO then provide mission capabilities out to the periphery of the organization. So, say, if the CIO of the Federal Aviation Administration comes to the Department of Transportation CIO and says, “I have an idea that is going to improve flight safety,” that central headquarters CIO can say, “Great. Here is a development environment as a service. Here is a test environment as a service. This is how we will educate our help desk to help with this project,” et cetera, and make rooting out duplication and providing these cross-agency services just the norm. It is how we get to be the most effective and efficient.

I think the other opportunity is to then look at inherently governmental opportunities and to root out duplication there. So getting our payroll systems in government down to one, streamlining our financial management systems across government, doing those things that we can do that are very vanilla across the agencies, and to establish sharing at that level, too.

So all of our policies, our guidance, everything we have been doing has been in this motion to do exactly that.

Senator AYOTTE. Thank you, and I look forward—I thank again the Chairman and the Ranking Member for having this important hearing, and thank you all for being here. And I know that there is much work to be done in this area, and I look forward to working with the leadership of this Committee to address these issues and with all of you.

Thank you.

Chairman CARPER. Thanks for your question. Thanks for joining us. I know you have a lot on your plate, but you were good to come. Thank you.

We have focused a fair amount—and Senator Ayotte just did again at the beginning of her questioning—on the data center consolidation. I want to dwell on it just for another moment, if I could, and ask a question of David. In its recent PortfolioStat guidance, OMB folded the Data Center Consolidation Initiative into the PortfolioStat process, shifting the goal of the initiative away from just closing data centers and instead have agencies—I guess the word is “optimize”—their data center inventory.

I would just like to hear, if I could, your thoughts on OMB's change in the approach with regards to the Data Center Consolidation Initiative.

Mr. POWNER. I think combining the two makes sense, and that is fine to do it that way as long as you have the right metrics on data center consolidation, Senator, to your point. What remains, we need to get the average server utilization rates up.

I think when all this is said and done and we close all these centers and here is what remains, let us go measure average server utilization, and hopefully it is higher than 5 to 15 percent, on average.

Chairman CARPER. How much higher?

Mr. POWNER. Sixty to 70 I think is industry average. You want to build—you need excess capacity. But we are nowhere near the goal of 60 to 70 percent.

Chairman CARPER. Are we moving in the right direction?

Mr. POWNER. I think we are. There were plans—when there were data center consolidation plans, we saw by agency their average server utilization rates. DOD was reporting in the 30s. DHS was in the high teens. So that is fine.

But if you step back, that is fine to focus on optimization, but you cannot lose sight of the savings. We are closing a thousand centers. That is the goal. Now, we found out about an additional 3,000 centers. Many of them are small, in Agriculture and DOD, but there are more than a thousand we can close, and if the server utilization is that low, there is a lot of cost to—there is hardware, there is networking, there are security costs. DOD reported in fiscal year 2014 alone \$575 million in savings with data center consolidation.

Chairman CARPER. We do oversight here on this Committee, but who should we be looking to hold responsible for closing the next thousand or whatever, two thousand—

Mr. POWNER. Agency CIOs and the Federal Chief Information Officer.

Chairman CARPER. All right. Let us talk a little bit about budget control, if we could. I think a couple of years ago, the budget for information technology at the Veterans Affairs Department was consolidated under the Chief Information Officer for that Department. This year the Administration's budget request for the General Services Administration also sought to consolidate most information technology spending under the office of the CIO. The consolidation of spending under the CIO is, I think, clearly one way to empower an agency's CIO.

I would just ask each of you this question: Do you believe that it is necessary for an agency's CIO to have budget authority for IT spending across an agency? And are there other better ways to empower an agency's CIO? Do you want to go first, Steve?

Mr. VANROEKEL. Sure. Thank you. I think it is one way. I think there are a myriad of other things we have to consider and bring into play because it is not the only way.

I think the essence of good IT management in an agency is one where there is coordination across the budget motion and you are watching the dollars flow and you are making sure that there is not duplicative spend and all of that. But you also, as you heard

earlier, need for oversight of senior leadership. We have seen the private sector go through this in the last 15 years where IT went from this very discretionary thing—it was the ability to print or share a document or save a document—to this very strategic thing. It is the way you connect to your customers; it is the way you drive productivity gains in the organization, the way you streamline your operations, control quality, inventory, et cetera. And the public sector has not necessarily gone through that transition yet where IT is this strategic thing and the way we, change outcomes of research that we are doing and keep America safer and drive economic value and benefit and efficiency.

And so as we go through that inflection point, it is going to take a lot of different people than just the CIO watching the checkbook to make that happen. We need the coordinated efforts of acquisition, to Senator—Dr. Carper’s comment on the person not making the decision at the point of execution. We need acquisition at the table. We need the Deputy Secretary’s chief operating officers at the table. We need human capital people training the next generation of professionals in the space, et cetera, to really make that motion happen. And so it has to be a village approach.

Chairman CARPER. “Dr. Carper.” We have become interchangeable parts here. [Laughter.]

It is a good thing. It is kind of scary.

Any other witnesses want to respond to the question that Mr. VanRoekel responded to? Please.

Mr. SZYKMAN. Sure. From my perspective I think the key is not necessarily to centralize the entire organization’s budget into a single budget managed by one individual. From my perspective I think much of the benefit can be obtained by improving visibility and transparency and providing enough authority that the CIO can influence the right types of decisions going on across the organization.

I think from the centralization perspective, the key is a focus on commodity IT. As Mr. VanRoekel had mentioned, agencies do not need to have well over a dozen e-mail systems, which the Department had a couple of years ago. Our largest bureau had over ten alone. They have consolidated down to one, and the rest of the Department is in the process of moving to the cloud.

So that type of proliferation of replication in commodities is unnecessary. But at the same time, there is a lot of mission-related IT, and I would not necessarily argue, for example, that NOAA’s satellite programs should be run out of my headquarters organization when the experts in satellite systems and programs and the people who really connect that to the National Weather Service’s mission are at the bureau level versus the headquarters level. But the transparency and the ability to influence decisions is key.

One other example I just want to touch on, at the Census Bureau in the 2010 decennial census which took place a few years ago, the Census CIO was not directly involved in the management of the IT for the census program. What that meant was that the census program ran their own IT infrastructure. There are already written administrations in place for the 2020 decennial census that states that the decennial program will run on IT infrastructure managed by the Census CIO, not managed by the program themselves, from

an infrastructure perspective. All of the mission-specific application development is still going to be run out of the program. And the other part of the agreements that are in place there provide the Census CIO with actual approval authority over acquisitions that are coming out of the decennial program, and that is something that is also new from how things have been done in the past.

So I think the key is to be able to know how money is being spent and to influence how it is being spent. The centralization of the budgets themselves do not necessarily need to be there to get the outcomes we want.

Chairman CARPER. Well, that is encouraging. I do not know that Dr. Coburn and I will still be sitting here when they are doing the 2020 decennial, but at least there is maybe cause for hope that when it comes around, the cost overruns that we were plagued with this last time will maybe be less of a problem.

I am going to come back and ask one last question, not now but after Dr. Coburn does, but the question I am going to ask, I will just telegraph the pitch. Sometimes at a hearing, especially I think this one lends itself to it, I like to come back at the end of the hearing and just ask you give a closing statement. You can just reflect on something someone else has said, or if there is something you want to reiterate for us, for our takeaways, that would be good. But one more question, and that will be it. And I am going to step out of the room for just a moment and then come right back.

Senator COBURN. I would just make a comment on the census. I am glad to hear those are the kind of decisions—we spent \$500 million on a cost-plus contract that got us nothing on a handheld device for the Census, and nobody was held accountable for it, nobody got canned. The company did not perform. We did not sue the company for not performing. I mean, it was just throwing \$500 million away. That is what happened. We held the hearings here, and everything they were doing you could have done on an Apple iPhone, with no contract. I mean, so putting controls in and making people responsible and accountable is very important, and if the 2020 census is not done online, we ought to shoot ourselves. We can save billions of dollars. And if that is not the Administration's plan and top-down enforcing that this is what we are going to do—we cannot do it all, but all the money we can save on doing an online census is unbelievable. And you can incentivize people to participate. The same thing with the American Community Survey (ACS). It ought to be all online right now. There is no reason why it should not.

The one thing I did not hear from you, Mr. Baitman, in your testimony was metrics, and Senator Ayotte talked about that. Do you all now know where all your inventory is, where all your computers are, where all your servers are? Do you actually know? Do you know in HHS where they are?

Mr. BAITMAN. We have a good idea where they are, but as I said in my opening remarks, I think we are benefiting from PortfolioStat. Last year, when we went through the PortfolioStat process, we realized that there were a lot of gaps in our knowledge base, and at least in the commodity IT area, which is what PortfolioStat last year focused on, we were able to begin to work with our operating divisions to say this is the data that we need

so that we can actually make knowledgeable decisions about allocation of resources and consolidation.

Senator COBURN. So you do not know where all your stuff is right now.

Mr. BAITMAN. I would say we have a better idea than we had a year ago—

Senator COBURN. I know, but the answer is you do not know—I am not being critical. I am just saying we really do not know in HHS where all the servers are.

Mr. BAITMAN. We have a good idea, but not a complete idea.

Senator COBURN. OK. Well, a “complete idea” is you do not know, OK? And that is part of the problem. Information down is great, but if you do not get information back up, you do not get to make the right decision.

Mr. Szykman, when you did all this consolidation in Commerce over the last 3 years, did you use GSA to perform this? Or did you do it with your own people?

Mr. SZYKMAN. We have worked at GSA on some of our contracting activities. For the most part, most of our strategic sourcing initiatives and several of our shared services initiatives have been things that we have done internally. The Department of Commerce does already have its own strategic sourcing contract called NOAALink, which is under NOAA, and we have used that in a couple of cases.

We have also taken advantage of existing acquisitions that were ongoing within some of the Commerce bureaus and expanded them to become department-wide acquisitions. So those were things that we were doing anyway at the bureau level and which have been expanded to now become department-wide contracts, which—

Senator COBURN. So you used GSA some, but—

Mr. SZYKMAN. Correct.

Senator COBURN [continuing]. Basically you ran the show.

Mr. SZYKMAN. That is correct. The one area where we have been holding back and waiting for GSA is in the area of mobile phones and mobile plans. GSA just recently announced the final awards of contracts in that area, and we had been anxiously waiting for those contracts to be available for us. So we do intend on using those as well.

Senator COBURN. Steve, I have one question for you. The estimated savings out of the server consolidations was supposed to be a minimum \$3 billion. Now with PortfolioStat, the estimated savings governmentwide is \$2.5 billion—\$500 million less than what we thought we were going to get. Would you clarify for me—first of all, we ought to be shooting for a whole lot more than that. Clarify that number for me. Second, how much is ghost savings where we are saving the money and then spending it somewhere else within these agencies?

Mr. VANROEKEL. So I have said publicly that I thought the \$2.5 billion in PortfolioStat was the tip of the iceberg and a very conservative assessment. I am being very diligent about making sure that the money we report in is acquired in a very consistent way to make sure that we are not double counting or doing other things across the 2.5. That is why you do not see, as you mentioned earlier, the DOD and—or I think Mr. Powner said DOD and Depart-

ment of Justice and a couple others are not reported in, because they did not come in through the reporting infrastructure we had in 2012. So I decided not to put them in because I want to make sure it is apples-to-apples. In 2013, they are all required to report in this quarterly way, and so we are going to see a very consistent view across the savings. And I think we are going to see even more of that.

There is overlap in some of the data center consolidation work and what we are seeing in PortfolioStat, and we will continue to drive those numbers forward, and I am encouraged by that. I think we are at the tip of the iceberg on where we are going to go with the savings that are associated with that, and these quarterly reports we have been doing for the Appropriations Committees prove out that we are hitting the mark. We are at over \$500 million now reported to the Appropriations Committees on line item savings.

On where do the savings go, my budget guidance for 2014 kind of follows the spirit which I bring to this, which is I asked for a cut-and-invest strategy in budget guidance. I basically ordered government agencies to cut 10 percent of their IT spending. I gave them very specific areas, and I gave them a tool called PortfolioStat to go do that. And then I asked them to reinvest 5 percent of that, so half of it back into the agency to do one of three things. One is employee productivity, so how are you driving efficiency gains inside your organization to root out duplication and other things? Two was customer facing, so how are you building services for your constituents, the American people? And then the other was cybersecurity.

I then asked them to give me 5 percent back of priority add-backs if we saw budget flexibility, if we had Presidential priorities we wanted to fund, I wanted to hear from them what they would spend an additional 5 percent on, and then I can make a value judgment across that.

So we had very good turnout from the agencies on this work, and the notion of depreciation, something we use in the private sector all the time is, one, a balance sheet tool. But I think more importantly it is a cultural tool that basically says that we need to cut from the bottom of the list to give to the top of the list. We need to take from the operating expense (OPEX) column to give to the capital expense (CAPEX) column in order to create a virtuous cycle to make sure we are taking advantage of the latest technology. When we talked about server utilization at these low single-digit percentages, a big problem there is having the capital to go buy new servers and new software in order to do the consolidating and optimization to get the savings that you are going to see long term.

And so I am intending to create, and through my budget guidance, these tools, that notion of depreciation, let us stop what is not working or what is duplicative, and let us take those savings and in some cases pour them back in to get the capital expenditure to do this, because smart investment in technology can scale you in efficiencies and other ways.

Senator COBURN. Just as a little aside, the Federal Government's balance sheet has \$86 trillion worth of liabilities, and all the assets in the United States of America are under \$80 trillion. That is all

the land, the buildings, the businesses, and everything else in this country.

So it is not enough to just cut it and reinvest it. We have to get real dollar savings that flow to the bottom line so that we can quit adding to that imbalance on our balance sheet.

David, I am going to make one final statement, and I would like your comment on it, and I again want to thank each of you for being here, and we will followup with a list of questions that I did not get to ask.

We have, if you count intelligence organizations, far in excess of \$80 billion a year. From your learned position, how much can we save a year in IT? If we did everything Steve would want to do, we copy what Mr. Szykman has done, and the changes that we are starting to see at HHS, if we really executed over the next 5 years, how much money could we really save?

Mr. POWNER. Out of the 80, I think it is safe to say—well, if you look at—and I agree with Steve. With the PortfolioStat initiative and data centers, some of those that go away, that is mutually exclusive from consolidating applications. So I agree there is some overlap there. But I clearly—if there is 2.5 in PortfolioStat and DOD is not in, you could double that with Justice. You can get the \$5 billion there on PortfolioStat, I think that—I do not know what Steve would think of that, but you have \$5 billion there. And if you take away the \$3 billion on data center consolidation, clearly another couple billion. But also, too, I think you need to focus on those troubled projects on the Dashboard. If we got \$10 billion at risk, you could actually rescope some of those and save a fair amount of money there. You could easily get the \$10 billion if you do the math real quickly out of the 80, easily get to 10.

Senator COBURN. All right. Thank you. Thank you all.

Chairman CARPER. And just to followup, David, on Dr. Coburn's question and your response, for us in the legislative branch, especially on an oversight committee, what more do we need to be doing to better ensure that we are as close to that \$10 billion as we can be?

Mr. POWNER. Well, I have comments on the Dashboard Data Center and PortfolioStat, but I want to start with this comment. I think the CIO authority, if we do not fix that, you cannot accomplish these other things. I think the big learning and a big surprise is I agree with Steve that CIOs should—it is a no-brainer to have them have authority over the commodity IT. And we want to eventually move certain agencies where they have input on the mission-critical applications.

But what we are learning on PortfolioStat is CIOs are struggling having authority over commodity IT. Again, that is a low bar, and that is a big problem. So there is this question about do you give them budget authority or not. I know we go back and forth on that. That would be a game changer. But maybe a starting point is budget authority over all the commodity stuff, and then they would control that to begin with. And I am not certain they all have that, so that is a starting point.

And then if you look at the Dashboard Data Center and PortfolioStat, Dashboard it is real clear. You need to fix the reporting inaccuracies, and you need to TechStat the troubled projects.

Data Centers, we need to measure cost savings, and then we need to make sure that server utilization rates are where they need to be on what remains.

And then on PortfolioStat, I think that is heading in the right direction, but I do have one comment on PortfolioStat, is you need to make sure that we have solid baselines on PortfolioStat because we do not want to get into a situation like we are with data centers where we constantly are coming up with new inventories and that type of thing. I think PortfolioStat is a real solid process, but you need a solid baseline, you need to drive that consolidation to closure.

Chairman CARPER. OK. And this is an opportunity now—when Dr. Coburn was leaving, he asked me, Steve, to ask if you might also send to us the IEEUIT report, not just, I guess, to the appropriators, but also to us as the authorizers, if you could, please. Thank you.

OK, closing statements. Steve, if you would like to lead it off, and we will close with David.

Mr. VANROEKEL. Thank you for this important conversation today. It is great to—

Chairman CARPER. No, we thank you.

Mr. VANROEKEL. Thank you. I think the key things I wrote down, sort of the to-do items in the work I think we have to mutually work on between GAO, the legislative and the executive branch, one is the CIO authorities and taking this balanced approach. I think there are areas where we can enable that.

Two is something we did not talk a lot—we talked a little bit about but not in the broadest sense, which is around budget authority and flexibility associated with that budget authority. I think one of the inhibitors we often have in Federal IT and something that I did not in the private sector was you could often incubate a new product or think about something and have a 5-year window in which to really execute against that with some level of certainty of what your budget was going to look like and how you could do that, because oftentimes it takes investment to realize savings, and it takes investment to realize new capabilities.

And so the ability and flexibility in the budget side to create capital budgeting or to get capital to do new things I think is an important one we often overlook in Federal IT. A lot of data centers do not get consolidated and optimized because the people do not have the money to spend to get the work done to get to the end state they want.

And another area we did not talk about today is around the potential of open data and some of the phenomenon we are seeing with big data and other things. I think the bottom line I often carry to the job is teaching agencies that they do not always have to do the end-to-end solution. If you do just part of the solution and make data available, great things happen outside the walls of government to drive the economy, drive jobs, and others. When the U.S. Government opened up global positioning, it almost overnight created \$100 billion in economic value, yearly economic value, for this country, and I think we stand on a treasure trove of that potential for the economy. And so as we do that and as we all have our takeaways of what to do, I think thinking about that in the

context of legislation we write and other things could be something we could help really drive what makes America great, which is innovation.

Chairman CARPER. Thank you. Mr. Szykman.

Mr. SZYKMAN. Mr. Chairman, thank you for talking about this important issue here today. I was happy to be able to be part of the conversation.

I think it is an exciting time of change in Federal IT management. I think there are a lot of opportunities for us to exploit, but we are now having conversations that I think are key to helping things get done. I found it interesting when you quoted earlier Senator Cohen back in the roots of the Clinger-Cohen Act talking about the change in culture and reflecting on the conversation here today, which was not a conversation about technology at all. It is still a big question about how to change culture and change management in Federal IT. So I think we are still struggling with some of the same questions that we were dealing with way back then.

I do think it is important for us to be focused on outcomes, and some of the questions that were discussed today had to do with understanding what other people are doing and learning from them, and certainly learning is important. But in my view, we have a number of people in key positions who really are change agents. And if we really want to get the outcomes that we are hoping to get, I think it is not as difficult to find change agents as it is to enable them to pursue the changes they would like to pursue. And to be able to do that, we need better knowledge on which to base decisions. We need transparency. We need better internal reporting, better inventories, better baselines. And we need to empower the people to make the changes that they want to pursue.

So I think we have a lot of the ingredients for achieving the kinds of change that we would like to see here within the Federal Government.

On the issue of empowerment, I mentioned in my testimony the IT portfolio management policy that we had put in place at Commerce. My approach was not to use that policy to wrestle control away from the bureau CIOs, but to use delegations to further empower those CIOs to manage their portfolios, because ultimately if you do want to hold people accountable for managing portfolios, then you need to be able to make it possible for them to define their portfolios, and you need to give them the ability, the controls and the authority and responsibility, to manage that portfolio to get the outcomes that you want.

The only last thing I would like to mention is that we have had a fair bit of discussion around data centers here, and certainly data centers are an important part of the overall IT portfolio in the Federal Government. But the approach to portfolio management for better efficiency, savings, and outcomes should be a holistic type of approach, and it is not just data centers. There are millions, tens of millions, hundreds of millions of dollars being spent on IT services of other sorts. There is software and licenses. There is equipment. And so the approach to portfolio management I think should extend the discussion beyond just data centers and really take a holistic look at the IT spending portfolio.

Thank you very much.

Chairman CARPER. Thank you, sir. Mr. Baitman.

Mr. BAITMAN. Thank you for the opportunity to be here today. I have thought about these issues. Up until 4 years ago, I had worked exclusively in private industry before taking on the last two government roles that I have had and tried to understand why there are differences. Why do we think that there are redundancies and waste in government when I did not see that in industry? And what I have concluded is that government and industry are inherently different in some fundamental ways. So in a large federated agency like HHS, Commerce, or other organizations, the programs within those organizations have had to address what their mission requirements were and then decide how to invest their dollars in technology over the past few years.

That brings them all to a different State of maturity. No one is actually at the same state within HHS, for example. So when we bring ideas forward for consolidation, when we say, hey, here is a better way of doing it, technology has changed, we can do something smarter, better, cheaper, we look at it and say, "Why don't they want to go along?" And the reason they do not want to go along is because some of them are actually quite sophisticated and others are laggards. It is very difficult to ever develop a single business case that will bring everyone to a better place and everyone will buy into that.

In private industry, you simply look at the bottom line, and you make a decision based upon what is best for the whole enterprise. We do not do that in government. We do not look at what is the bottom line for Health and Human Services. We look at the bottom line for International Business Machines (IBM), where I used to work, and say that new company that we have just acquired through acquisition is running a system that is redundant and we are going to get rid of it, we are going to take that cost off our books. And that is really what the fundamental difference is.

And I think that gets us to a point that Steve made a moment ago, which is capital investment. If we are going to get everyone to a better place, we need to have the capital to invest so that people do not have to look at the business case and say it is not going to help me even if it helps 90 percent of my peers. We need to be able to make that investment to get everyone to a better place and in the end reduce our operating costs.

Chairman CARPER. Those are very good observations. Thank you.

Mr. Powner, one last shot?

Mr. POWNER. Yes, three things: Leadership, transparency, and accountability. I think the CIO authority thing is a big deal, and that needs to be addressed from a leadership point of view. Transparency, we have talked a lot about the metrics that are needed with the Dashboard, with data centers, with PortfolioStat, and so that transparency needs to be very clear, and then where you can really help is holding the Chief Information Officers accountable going forward.

Chairman CARPER. All right. Thank you.

Mr. VanRoekel, I think you mentioned earlier the work that is going on between the Department of Defense and the Veterans Administration with respect to our electronic health records. I am on active duty 1 day, I finish my obligation, my military obligation,

step down from active duty. The next day I am a veteran. And we have had a problem, as you know, with the transfer, interoperability between the two systems. How are we doing there?

Mr. VANROEKEL. The two Departments have been meeting a lot and have come to an agreement that I think is very sound, which is really around record interoperability, the ability for that record to transfer seamlessly from one entity to the other. Today they share information. If you go into a VA hospital and there is an active-duty record on you, you will see a little flashing icon, you pull it up. What happens, though, is that data is—there are two problems with it. One is it is not sequential, so I cannot see if you took a medication or issued a medication in what order, so there is a lot of variability there. It is two separate experiences to see the two, and I have to map them together myself. And two is it is not computable, so we cannot tell if a certain medicine would interact with a certain other medicine, and if issued those two medicines it might hurt you or something, and so it is not—the data is just sort of static and you just look at it.

So the Departments have done some very important things. One is agreed on record interoperability, and what that basically means is, much like if you are running a Yahoo! e-mail account and I am running a Gmail account, you and I can send e-mail back and forth all day long because the two e-mail vendors have agreed on record interoperability. The e-mail record goes back and forth. So that is the important first step.

The second step is they are going to base all this technology on national standards that have been coordinated by the HHS' Office of the National Coordinator in this Administration. They have specified a bunch of national standards for this type of record, and the important thing to note is in the last, I think, 2 weeks, over 50 percent of the doctors in this country are now utilizing those standards. And so if DOD and VA—and, importantly, they have agreed to exchange records in this way, that will create opportunity for those same veterans to go to private sector providers and have their records transferred there as well.

And so the important milestone we have hit is on that level of agreement and that level of interoperability. So I am very encouraged by that. We held a House Veterans' Affairs Committee meeting a couple of weeks ago with the vendor community. I think there were 40 vendors in the room, and they were all in agreement that this approach, standards-based interoperable approach, was the one to do. And so I am encouraged by that and excited to come up and talk to others about it today.

Chairman CARPER. Well, as a veteran myself, a retired Navy captain, I am encouraged by that. I started off the hearing today by quoting former Senator Bill Cohen about his vision and the problems we faced 18 years ago, and I will close not by quoting Bill Cohen again but by quoting a distant relative of Bill Cohen, Albert Einstein. Really distant. But Einstein used to say, "In adversity lies opportunity."

"In adversity lies opportunity." And I quote him from time to time. There was plenty of adversity 18 years ago when Bill Cohen and Bill Clinger were working in these vineyards, and there is still adversity, but there is opportunity as well. And I am really encour-

aged to hear a good example, a live, real-world example of how that adversity—the opportunities about on its way to being realized.

We have a recurring theme in this Committee as we do oversight, and the recurring theme is: How do we get better results for less money in just about everything we do? And it is a culture change. That is what I think Bill Cohen called for all those years ago, culture change. And we still need one. I like to say the road to improvement is always under construction, and the road to culture change is always under construction as well.

You have been very helpful to us today with respect to our obligations in this regard, and just some pretty good reminders as to things that we are doing on our side that make sense and what we need to do more of, and also what the executive branch needs to be doing and how we can help to empower them there.

I asked our staff over here, as we were thinking back about how 18 years ago what was being said then sounds a whole lot like what we are saying in today's hearing. There is an old Led Zepelin album called "The Song Remains the Same." But the important thing is that 18 years from now or 18 months from now, when we gather together for another update on this, the song will not remain the same and we will have some new lyrics, maybe some new music, and some better results that will give us better results for less money.

Our thanks to each of you for joining us today and for your work that you put on display here today and the work of others who work with you. We are grateful for that.

I want to thank our staffs for helping to put the hearing on today, and I am told by our staff over here that the hearing record will remain open for 15 days—that is until June 26th at 5 p.m. sharp—for the submission of statements and questions for the record.

With that, this hearing is adjourned. Thank you.

[Whereupon, at 12:30 p.m., the Committee was adjourned.]

A P P E N D I X

Opening Statement of Chairman Thomas R. Carper

“Reducing Duplication and Improving Outcomes in Federal Information Technology” June 11, 2013

As prepared for delivery:

Good morning. My thanks to our witness and guests for joining us today to examine the Administration’s efforts to identify and eliminate areas of duplication and waste in federal information technology and the role agency Chief Information Officers can and should play in that process. My thanks as well to Dr. Coburn and his staff for their help in putting this hearing together.

The Committee is holding this hearing today because, to put simply, when it comes to information technology, the federal government needs to do a better job of managing its considerable investments. I would like to start my statement with a simple quote:

Poor information [technology] management is, in fact, one of the biggest threats to the government treasury because it leaves government programs susceptible to waste, fraud and abuse.

These insightful words were spoken by Senator William Cohen from Maine at a hearing this Committee held in the summer of 1995 on Senator Cohen’s Information Technology Management Reform Act. That bill is also known as the Clinger-Cohen Act, and I have no doubt all the witnesses on the panel are very familiar with it because it created the position of Agency Chief Information Officer.

The Clinger-Cohen Act was passed almost two decades ago. Back then, a Blackberry was a fruit, a tweet was something that only birds did, and Google was just a really big number. Today, we live in a world of smartphones and tablets, social media and the cloud. Yet the more things change, the more they stay the same. Because despite passage of the Clinger-Cohen Act and the creation of agency chief information officers, our federal government still wastes a tremendous amount of money by poorly managing IT systems and investing in duplicative systems.

In 1996, when Clinger-Cohen became law, the federal government was spending about \$25 billion a year on information technology systems. That’s not an insignificant amount of money, but today we spend more than three times that amount at \$80 billion a year.

I would ask today’s witnesses, with all the money we spend each year on information technology, can we say that we’re getting what we paid for? Can agency managers look at their investments in this area and tell the American people that they’re managing the taxpayer dollars entrusted to them effectively? I’m afraid that the answer to both questions is “no.”

In 2013 we see many of the same problems that Senator Cohen found in 1995 – poor management of information technology systems, wasted and duplicative investments, and

billions of dollars spent on outdated “legacy” systems. Too often, agencies, or components of agencies, seek to develop new solutions first, before assessing existing options for sharing services with other agencies or even within their own agency. As I mentioned before, the more things change, the more they stay the same.

To address these persistent problems, in 2012 the Administration launched a new initiative called “PortfolioStat” which required Chief Operating Officers across government to lead an agency-wide review of their IT systems and eliminate areas of duplication and waste. The Federal CIO then met with each agency to discuss, among other things, potential duplicative systems and investments that did not appear to be well aligned to agency missions. Through this process, agencies identified more than \$2.5 billion in IT spending reductions that could be achieved from FY 2013 through FY 2015.

I am happy to have the Federal Chief Information Officer here with us today to tell us about the first version of PortfolioStat and what the future holds for that initiative. Mr. VanRoekel, I understand you have new responsibilities at OMB, but I am hopeful that, as our Federal CIO, you will stay actively engaged in the PortfolioStat process because I strongly believe that your participation in those meetings with the Chief Operating Officers and other agency leaders is key to getting results.

One of the key takeaways from the first round of PortfolioStat sessions was that the decentralized manner in which many agencies managed their information technology investments lead to “inefficiencies and duplication.” The fact is that despite the Clinger-Cohen Act, agency CIOs are frequently not recognized as the key leaders in managing information technology at an agency. Too often there are many CIOs in a department, and many of them act independently of each other. As a result, departments are unable to take an enterprise-wide view of their investments which results in duplication and missed opportunities to leverage existing systems.

I am very interested to hear from our panel, and especially from Mr. Szykman and Mr. Baitman about their experiences at large decentralized Departments like Commerce and Health and Human Services.

I want to finish my statement with another quote from Sen. Cohen – he sure is a smart guy:

But we must also understand that statutory change is only half the battle. The other half involves changing the management culture at agencies that has traditionally focused on technical performance and bureaucratic process. We must insure that the top levels of agency management understand how information technology can change and improve their agencies. Cultural change is critical to changing the way government approaches its information technology needs.

I end with that quote because it highlights the fact that our job is not done once a bill is passed into law. In many ways that is when the hard work really starts – when we roll up our sleeves and do the oversight necessary to ensure a law is being implemented properly. It is ultimately congressional oversight that lets agency leaders know where our priorities lie and that can help agency leaders break through any resistance there may be to change.

Opening Statement of Senator Tom Coburn**“Reducing Duplication and Improving Outcomes in Federal Information Technology”
June 11, 2013**

As prepared for delivery:

Thank you, Senator Carper, and welcome, all of you.

I think there are four or five problems in front of us, and having done this a number of years, we keep trying to solve the same problems. And here is the crux of it.

We are well intentioned. You are well intentioned. But we do not give people the authority to do what we ask them to do. And even in OMB's recent guidelines, they essentially in four or five areas undercut the Chief Information Officer and agencies by allowing them to place other than our key Information Technology personnel in charge of the programs. That is the first problem I see, and I will go into detail as we go through the questioning.

The second problem is we do not have real transparency and metrics on what we are doing. We do in one Department. It is very rarely we get to really praise DHS. But if you look at what they have done on their data centers, they actually track it transparently, know what they are doing, know how many they have, know how many they have eliminated, and know how much money they have saved. You cannot do that anywhere else in the Federal Government.

So we lack transparency, and we lack good metrics. As a matter of fact, the metrics are changing in the middle of all this, according to OMB.

The other thing is the IT Dashboard is a farce. We have looked at computer programs at the Pentagon, and according to the IT Dashboard, they are doing fine, which is absolutely opposite of what is actually happening in the Pentagon. Half of the money we spend on IT goes through the Pentagon. Half of it is wasted every year. Half of it is wasted every year. And yet the Dashboard shows no problems with the Pentagon's programs, just like the Pentagon shows no problems in improper payments. These problems go back to the Audit the Pentagon Act – you are never going to control the Pentagon until we can have numbers and accountability and metrics to get it done.

The fourth area is just the communication of what is actually happening. Some of our agencies, some represented here today, actually know. But once you actually get to working on this, some of our Secretaries and some of the people inside some of the agencies do not like it because there is accountability coming and our CIOs get thrown out, two of which recently and who were actually doing a good job. But other priorities other than transparency, other than metrics, other than good management take precedence – and this goes back to the first problem, because if you are not going to give CIOs the authority to do what they need to do, then why do you need a CIO?

We have looked at all the issues, and I hope to have a great discussion. But some change ought to come out of this oversight hearing - both in terms of transparency, in terms of giving CIOs the authority they need to actually make the decisions, and in terms of metrics. And actually my compliments to DHS to create a timeline so you can actually see it and manage it, and we can as you see it and manage it.

My final point I would just make is we had expected savings coming out of the data center. Those savings really have not materialized because if we did have savings, we are spending it somewhere else, essentially. And now we are going to consolidate the savings to less than what we had hoped to achieve through the latest iteration of this initiative. We are actually going backwards. The stream is more powerful than our oars. And, you know, with excess of \$80 billion a year spent on IT, of which a conservative estimate, at least a third of it is not effectively spent. We can do better, and, you know, that is \$24 billion. That is 30 percent of the sequester. Everybody talks about the sequester, how hard it is, but there is plenty of money in this government. There is \$250 billion of waste, fraud, duplication, and stupidity, and what we need is to give you all the authority to go after it and to make smart decisions.

I will just end with this: I trust the vast majority of executives in our government. What I do not trust is Congress to treat them like grownups and give them authority and then hold them accountable for it. And hopefully through this hearing today we can make some steps and get some learning through the communication that will allow us to do that.

David has been great through what he has done through the years. And so, almost every question I am going to ask the panel, I am going to ask him what he thinks about it and your answer because what we want is the best. And this is not meant to knock on anybody, but we have big problems, and they are getting worse. They are not getting better. They are getting worse. The effort is being made at OMB. I am not saying it is not. But we can do a far better job than we are doing.

So I look forward to your testimony. Again, I thank you for being here to discuss these things.

Thank you.

**EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503**

June 11, 2013

**STATEMENT OF STEVEN VANROEKEL
U.S. CHIEF INFORMATION OFFICER
ADMINISTRATOR FOR E-GOVERNMENT AND INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET**

**BEFORE THE SENATE COMMITTEE ON HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS**

“Reducing Duplication and Improving Outcomes in Federal Information Technology”

Introduction

Good morning, Chairman Carper, Ranking Member Coburn, and Members of the Committee. Thank you for this opportunity to testify on the Administration’s efforts to manage the Federal Government’s investment in information technology (IT).

Throughout my career, first in the private sector at Microsoft and then in the Federal Government – at the Federal Communications Commission, the United States Agency for International Development, and now the Office of Management and Budget (OMB) – I have witnessed firsthand the power of technology and have seen the incredible impact innovation has on society. As an executive at Microsoft, I focused every day on improving and expanding core services and customer value, while also cutting costs. And as the United States Chief Information Officer, it is no different. I bring that vision with me in my work in this Administration to help drive innovation in Government and provide better service to the American people.

Today’s challenging economic times underscore the need to drive innovation and efficiency in Government. Our IT investments, while constituting a relatively small portion of the Government’s overall annual spending, have widespread positive impacts across agencies and are increasingly central to almost everything the Government does. And while our progress in this area has been significant, more remains to be done. We must ensure that the Government maximizes the return on its investment in Federal IT, drives innovation to meet customer needs, and establishes a trusted foundation for securing and protecting our IT assets and information. Simply put, we must manage our IT investments so they deliver results for our most important customer – the American people.

PortfolioStat Foundation

Sound management is rooted in evidence. This is why in March 2012, OMB initiated PortfolioStat¹ to take an objective, data-driven look across agencies to identify common areas of spending with the goal of reducing duplication and driving down costs. Throughout the summer of 2012, OMB conducted a series of face-to-face sessions with agency leadership, including agency Chief Operating Officers (COOs), Chief Information Officers (CIOs), Chief Financial Officer (CFOs), and Chief Acquisition Officers (CAOs), to examine their IT portfolios, targeting in particular commodity IT investments and back-office systems. Rather than looking at individual investments on a case-by-case basis, the reviews took a broader, more horizontal perspective – spanning agency components and employing both qualitative and quantitative data to benchmark agencies against their peers in commodity IT areas such as email, collaboration tools, identity and access management, web hosting infrastructure, desktop systems, mobile devices, financial management systems, human resources management systems, and grants management systems.

To date, PortfolioStat has yielded nearly 100 opportunities to consolidate or eliminate redundant or otherwise unnecessary IT investments representing more than \$2.5 billion in potential savings that can be achieved from FY 2013 through FY 2015. And we are already seeing results. Agencies have reported approximately \$300 million in realized savings, with more to come.

While we are off to a great start, there is still much to accomplish to ensure that taxpayers receive the greatest value possible from our investments in Federal IT. To bolster our analytical capabilities, we created the Center for IT Management (CITM) under the Integrated, Efficient and Effective Uses of Information Technology Fund (IEEUIT). CITM is charged with the development of tools that leverage Government-wide and agency-specific data sources to support OMB in the identification and elimination of redundant, wasteful, or otherwise low-value investments. It supports the PortfolioStat process by providing in-depth analysis, research, and reporting capabilities, as well as through the establishment of key performance indicators and outcome-oriented measures. We anticipate CITM continuing to support the PortfolioStat process through these robust analyses.

From the outset, PortfolioStat was envisioned as an annual process, and as a tool to support agencies in improving the management of their IT portfolios as well to inform the annual budget process. And given the rapid advances in IT and the ever-increasing pace of innovation, we anticipate that the PortfolioStat process will evolve from year-to-year, with lessons learned from prior years being incorporated to shape and inform our future efforts.

PortfolioStat Evolution

In March 2013, OMB released the guidance for PortfolioStat in FY 2013². The upgraded process streamlines agency data collection, adds analytical capabilities and tools as provided by CITM, and holds agencies accountable for the goals they set in FY 2012.

¹ http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-10_1.pdf

² <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-09.pdf>

Additionally, the guidance consolidates agencies' strategic IT direction and management improvements into one central plan and incorporates additional portfolio management efforts. The FY 2013 PortfolioStat process includes key performance indicators to measure progress and outcomes related to strategic priorities such as: the Administration's Digital Government Strategy; the Cloud First Policy and the Federal Risk Authorization Management Program; the Administration's priority cybersecurity capabilities, and the recently released Executive Order on open data³ and Open Data Policy⁴. As a result, PortfolioStat includes outcome-focused metrics to track agency efforts to implement priority cybersecurity capabilities to provide safe, secure, and effective mission execution and services to the American people, such as continuous monitoring, trusted internet connections, and strong authentication as well as metrics to track agency efforts to consolidate non-core data centers and to optimize the efficiency of core data centers under the Federal Data Center Consolidation Initiative (FDCCI). To measure the optimization of core data centers, agencies are developing metrics that apply to all facets of a data center, including energy, facility, labor, storage, virtualization, and cost-per-operating-system metrics. This work is well under way, and we look forward to seeing our efforts bear fruit as the PortfolioStat sessions are conducted in FY 2013.

PortfolioStat FY 2013 Areas of Focus

The initial PortfolioStat sessions were concentrated on reigning in and rationalizing commodity IT spending. The FY 2013 effort will continue this work, but also focus on providing agencies with tools and approaches to help manage IT as a strategic investment that can improve mission performance agency-wide. Areas of focus for FY 2013 – based in part on the feedback we received from agencies during last year's process – include the need to empower agency CIOs, take a portfolio-wide view of our IT investments, and shift to IT as a service.

- **Empower Agency CIOs** – Technology solutions are most effective when they stem from a strong and equal partnership between business and IT leaders. Program and mission officials bring an understanding of customer needs while CIOs can provide expertise on systems and security considerations. To succeed in this capacity, CIOs should be empowered to exercise leadership in IT governance, spending, security, and program management across the enterprise. To fully support the needs of the agency, CIOs need to be involved from the outset, starting with the strategy and planning efforts, to ensure that the design and implementation of solutions takes advantage of IT best practices. CIOs also need visibility across the agency, both to craft solutions that support the whole enterprise as well as to eliminate redundant applications and reduce wasteful spending. An empowered and effective CIO can help an agency save money and deliver improved solutions.
- **Take a Portfolio-wide View** – Oversight is most effective when it is done across the entire enterprise. This means standing up oversight processes and Investment Review Boards (IRBs) that bring together COOs, Chief Human Capital Officers, CFOs, CAOs,

³ [http://www.whitehouse.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government-](http://www.whitehouse.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government)

⁴ <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf>

program officials, and other key executives to make decisions reflective of the entire agency. Effective governance requires that we get key stakeholders together and foster a collaborative, data-driven environment, focused on making decisions that best achieve mission-oriented outcomes. To support this, we must also establish consistent, data-driven valuation models that enable the objective evaluation of investments based on cost and value-delivered to the public. To this end, the CITM is working to enhance the IT Dashboard's ability to display PortfolioStat results, providing agencies access to valuable portfolio management data.

- **IT as a Service** – Recent advances in technology, such as cloud and mobile computing, are transforming how IT services are delivered and consumed. In shifting to the cloud, organizations no longer need to incur upfront capital costs to stand up new solutions, but can instead procure technology “as-a-service,” only paying for what they need, when they need it. For example, the Department of Agriculture (USDA) plans to consolidate the existing portfolio of component-operated data centers and migrate platforms contained within to the Department’s Enterprise Data Centers in order to achieve cost reductions, improve agility, reduce energy use, improve security, achieve economies of scale, and reduce overall complexity. Through the use of shared services and cloud computing, USDA will achieve a savings of \$46 million in FY 2013.

We are encouraged by the progress seen so far but must continue to push forward. Last year’s PortfolioStat sessions revealed that agency IT portfolios still have opportunities to improve. Some agencies are just beginning to tackle fragmented use of commodity IT and siloed infrastructures, while others are further along, deploying enterprise services on cloud platforms. Consequently, we need to provide agencies with the appropriate tools for driving change.

Conclusion

We are at a unique point in our history. As the economy recovers, advances in technology – such as cloud computing and mobile technologies, to name just two – provide new opportunities for transforming how we live and function as a society. And so we must endeavor to harness our underused assets to create new services for the American people that were until recently unimaginable. Rather than use the current fiscal environment as an excuse to do less with less, we must use this as an opportunity to efficiently reduce waste and invest in innovation. Our efforts to date in implementing PortfolioStat reveal that there is tremendous opportunity to improve IT and these types of changes will continue to drive better service, greater efficiencies, and more vigilant security. There has never been a more crucial time to make smart investments in information technology.

I appreciate this committee’s interest and continuing support. Thank you again for the opportunity to appear before the committee today and I look forward to answering your questions.

###

**Statement of Dr. Simon Szykman,
Chief Information Officer
U.S. Department of Commerce**

**Before the Committee on Homeland Security and Governmental Affairs
of the United States Senate**

on Reducing Duplication and Improving Outcomes in Federal Information Technology

June 11, 2013

Chairman Carper, Ranking Member Coburn and members of the Committee, I am pleased to have been invited here today to discuss with you ongoing efforts at the U.S. Department of Commerce (Commerce) aimed at eliminating duplication and improving outcomes associated with the Department's information technology (IT) investments.

I have been the Chief Information Officer (CIO) at Commerce for slightly over three years. I spent over three years prior to that as the CIO at the National Institute of Standards and Technology (NIST), and in the six plus years I have spent in a CIO role, I have spent much of my time working to improve efficiencies and governance in the organizations I have supported. Over the past three years, Commerce has taken a variety of steps to strengthen governance relating to its IT investments, as well as to improve the efficiency and effectiveness of IT spending at Commerce.

Governance

Commerce has made significant advances in strengthening governance, both generally and specifically in the IT area, in recent years. Since 2010, Commerce has established an Office of Program Evaluation and Risk Management, an Office of Privacy and Open Government, and an independent cost estimation function in the Office of Acquisition Management.

Each of these functions has had implications for how IT is being managed at Commerce. The Office of Program Evaluation and Risk Management provides senior level oversight for Commerce's most critical programs. These programs, which have included IT investments, benefit from enterprise risk management run out of the Office of the Deputy Secretary. The new independent cost estimation function, while not focused solely on IT investments, has supported decision-making related to IT, including Commerce's satellite programs.

Commerce has also significantly improved how it conducts oversight of IT investments through existing mechanisms such as the Commerce IT Review Board (CITRB), TechStat reviews, and the Federal IT Dashboard review and rating process. While these functions are aimed at supporting Department-level oversight generally, they provide greater visibility, as well a venue for improving efficiencies. For example, discussions at several CITRB meetings for investments at the National Oceanic and Atmospheric Administration (NOAA) have provided an opportunity to press for moving from IT-related services that existed in organizational silos to NOAA-level enterprise services for capabilities that include data storage and dissemination. Similarly,

bureau-level portfolio reviews have included discussions of assessing opportunities for some of the smaller bureaus to move from independently-managed services to cross-organization shared service models.

Policy

In early 2012, then Commerce Deputy Secretary Dr. Rebecca Blank recognized the importance of CIO authorities in the quest for greater efficiencies in Commerce's IT spending. She issued a memorandum directing the Commerce CIO, to work in consultation with the Commerce bureaus to develop an IT Portfolio Management Policy. The policy, developed with input and consensus from all of Commerce's organizational units, was issued by Acting Secretary Blank in June of 2012.

The policy includes sections covering Enterprise Architecture; Service Catalog and Governance; IT Budget Formulation, Investment and Acquisition Review; and IT Workforce Management. The provisions in this policy give the Commerce CIO a greater role in setting Department-wide architecture standards, identifying and implementing shared services, supporting Department-level budget formulation, reviewing IT investments, and managing the IT workforce at Commerce.

A memo I subsequently issued delegates several of these authorities to bureau-level CIOs to better empower them to manage IT portfolios at the bureau level. As a result of these increased and delegated authorities, for example, the CIO role in IT acquisition reviews at the larger bureaus is being strengthened and several IT service organizations that had previously not been under the respective bureau CIO's management authority have been or are being considered for realignment under bureau CIOs, either in their entirety or by formally giving bureau CIOs a portion of the performance review of the heads of those organizations.

The new policy and related delegations have provided significant new support for several of the efficiency initiatives that I will be discussing today.

Shared Services and Infrastructure Consolidation

The IT Portfolio Management Policy mentioned above has also led to a broad push into shared services, both within and across bureaus. Within bureaus, NIST is centralizing mobile application development into an internal center of excellence for these services. At the Census Bureau, the Office of the CIO is now operating enterprise services for content management and collaboration; storage, data backup and recovery; project management; and a database server "farm," all of which are available to support programs and offices across the bureau. NOAA is in the process of consolidating its high performance computing infrastructure from one of lab-centric computing to a remote shared service computing model. This model will be more cost-effective than independently managed infrastructures and will provide significant increases in research and development, as well as operational supercomputing capabilities. Following the consolidation of 19 different email systems into a single cloud-based system at NOAA last year, NOAA is now in the process of consolidating dozens of help desks into one national service desk that will support all of NOAA.

Moving on to cross-bureau shared services, within Commerce's Herbert C. Hoover headquarters building, one of the Commerce bureau's video teleconferencing service has been leveraged into a cross-bureau shared service that serves all of the bureaus in the building. Work is in progress to carry out a service desk consolidation of several of the help desks in the headquarters building that are currently operated and managed independently by different bureaus. Several security-related shared services are also under development.

In some cases, implementation of cross servicing models is extending beyond individual services and incorporating a complete suite of IT services. As of the beginning of this fiscal year, the Minority Business Development Agency, a Commerce bureau located in the headquarters building, transitioned the full portfolio of IT infrastructure, services and staff to the headquarters Office of IT Services, managed by my office. A similar transition of IT services is underway for the Economic Development Administration (EDA). While EDA has not transitioned its full suite of services, several commodity services including network operations, desktop support, service desk, and email, are now being received through shared services offered by my office, rather than being managed independently within EDA.

At the Department-wide level, Commerce's Enterprise Continuous Monitoring Operations (ECMO) initiative, currently in early implementation stages, will deploy a single security continuous monitoring infrastructure across the entire Department of Commerce. Through this capability – Commerce's first operational security function – my office will for the first time have near-real-time situational awareness of the state of security across Commerce's entire IT infrastructure. Next year we are expecting to establish for the first time an enterprise security operations center, which will provide Department-wide analytical capabilities to leverage continuous monitoring data, providing better capabilities to identify and react to cyber security incidents.

In addition to these shared services initiatives, data center consolidation efforts are also under way across Commerce. In the headquarters building, several independently-managed bureau-specific data centers have been consolidated into a single enterprise data center that is available to support all of these bureaus' needs. Bureaus are now supporting one another's data center needs, with NIST locating equipment in a NOAA data center, and the International Trade Administration having relocated its equipment from a separate leased facility to the Census Bureau. In FY 11 and FY 12, Commerce met the data center consolidation/closure it had established in our initial data center consolidation plan. Over time, as we have worked to improve our inventory, additional data centers that had not been identified when the initial plan was developed have been uncovered, and Commerce has been developing a draft of an updated consolidation plan to include these newly-identified data centers. Additionally, Commerce is supportive of the Office of Management and Budget's decision to no longer solely focus on data center closures. The new emphasis on optimization of core data centers, as well as consolidation of non-core data centers, will help ensure that the data centers which remain open are optimized to meet the diverse, but critical mission needs that Commerce bureaus carry out.

These are only some examples among numerous shared services and infrastructure consolidation efforts that are going on at Commerce. These efforts are enabling organizations to replace

services or infrastructure that were previously managed independently by different organizations, often duplicatively and at times outside of the management of Commerce or the bureau-level CIOs, with services that are centrally managed in a more cost-effective manner.

Strategic Sourcing

I'd now like to describe Commerce's use of strategic sourcing as another mechanism to improve the efficiency of our IT spending. In 2011, Commerce had over 100 different contracts for purchasing desktop and laptop personal computers (PCs). With 12 bureaus, it's clear from that figure that, even within bureaus, the purchasing of PCs had not been consolidated to leverage the government's buying power. In response to the opportunity presented by more efficient purchasing, the Office of the Chief Financial Officer established an emphasis on strategic sourcing within Commerce's Office of Acquisition Management. Working in collaboration with bureau acquisition organizations and Commerce's CIO and IT community, a contract was put in place in January 2012 which has produced savings of between 30% and 35% for every desktop and laptop purchased.

It should be noted that the benefits of this strategic sourcing contract go beyond the direct cost savings. There is also the secondary benefit to Commerce's acquisition organizations, which now do not have to spend time and resources to put in place dozens of largely duplicative contracts for the same commodity IT purchases. This frees up time of acquisition staff to focus on local and/or unique acquisitions, which often meet mission-specific needs rather than common commodity requirements.

Since that time, several other Department-wide strategic sourcing vehicles have been put in place at Commerce. We have established a trio of blanket purchase agreements for the three most common endpoint protection (i.e., antivirus) software tools, and have Department-wide contracts in place for cloud-based email, mobile device management, PDF (Portable Document Format) document generation software, and a cyber security continuous monitoring tool. Work is in progress to carry out additional strategic sourcing efforts for other services, networking equipment, and software.

Assessing Outcomes

I have met regularly with the Commerce Deputy Secretary and Acting Secretary to provide regular updates on Department-wide efficiencies initiatives. In order to maintain a Department-wide focus on implementation of improvements in IT portfolio management, my office and Commerce's bureaus have also been asked to include reporting on IT priorities in our quarterly performance updates, which have been taking place via meetings between the Acting Secretary and senior bureau leadership. These quarterly balanced scorecard reports track outcomes-oriented measures and have covered a range of initiatives, including updates on implementation of shared services and strategic sourcing initiatives, implementation of bureau-level IT portfolio management improvement plans, and improvements to Commerce's IT security.

Conclusion

I'm pleased to have had the opportunity to discuss with you today the evolution in IT portfolio management at the Department of Commerce that has been taking place over time. Although we have several accomplishments that we are proud of, and numerous related activities that are in progress, we recognize that many more opportunities for improving efficiencies lie ahead of us. With support from the Office of the Secretary and the Office of the Chief Financial Officer and Assistant Secretary for Administration, we intend to press forward aggressively to pursue these opportunities.

Although we have already begun to document tangible savings realized from the initiatives described above, these benefits are merely representative of more fundamental changes to IT portfolio management at Commerce. Commerce's leadership has worked together to successfully take on one of the most significant challenges facing senior IT leadership – the need for greater empowerment to support decision-making needed to drive efficiencies and improve effectiveness of IT spending at Federal agencies. The policies, plans, and initiatives that have been instituted have created a foundation for sweeping changes to how IT portfolios and investments are being managed at Commerce. The results of these efforts are only starting to be realized, and the ultimate impacts are expected to continue to materialize and grow in the future.



Testimony of

Frank Baitman

Deputy Assistant Secretary for Information Technology and

Chief Information Officer

U.S. Department of Health and Human Services

Before the

U.S. Senate Committee on Homeland Security and Government Affairs

June 11, 2013

Good morning, Chairman Carper, Ranking Member Coburn and members of this Committee. My name is Frank Baitman, and I am the Deputy Assistant Secretary for information Technology and Chief Information Officer (CIO) at the U.S. Department of Health and Human Services (HHS). I am honored to join you here today.

Under the leadership of Secretary Kathleen Sebelius, HHS is committed to the effective and efficient management of our information resources in support of our public health mission, human services program, and the United States health system. Our information technology (IT) portfolio is sizable, including support for a number of grant programs that provide IT resources to state, local, and tribal governments in support the programs administered by HHS. The portfolio also supports everything from commodity IT to our broad portfolio of mission systems. IT is mission-essential to everything we do at HHS, and it is essential that we manage IT as carefully as any other aspect of our programs.

HHS is a large department with a diverse set of missions. Our operating divisions include: the Administration for Children and Families, the Administration for Community Living, the Agency for Healthcare Research and Quality, the Centers for Disease Control and Prevention, the Centers for Medicare and Medicaid Services, the Food and Drug Administration, the Health Resources and Services Administration, the Indian Health Service, the National Institutes of Health, and the Substance Abuse and Mental Health Services Administration. We manage our IT portfolio through a federated governance structure. The vast majority of the Department's IT resources are directly tied to appropriations made to our programs and operating divisions and our governance reflects this reality. Program-level IT decisions are governed and reviewed by our operating divisions.

At the Department-level, we have established three IT steering committees (ITSC) to bring together IT and program leaders from across the Department. These ITSCs take a functional view of our IT investments in health and human services IT, scientific research IT, and administrative and management IT along with our IT infrastructure, respectively. Collectively, these steering committees provide Department-wide oversight of our IT portfolio.

Efforts to Eliminate Duplication

In an IT portfolio as large and varied as HHS's there is inevitably the potential for spending that appears duplicative or inefficient. We are constantly looking to identify these cases and determine where we can consolidate investments, systems, or acquisitions to meet the Department's needs more effectively.

Use of shared services is one way we avoid duplication within our IT portfolio. HHS is both a supplier and consumer of shared IT services. HHS operates a number of shared IT services supporting grants management, including Grants.gov, the government-wide platform for finding and applying for grants, and GrantSolutions.gov and Electronic Research Administration (eRA), two government-wide shared services platforms that support general grants management and extramural research grants management activities, respectively. Another example is in the area of shared acquisition—the National Institutes of Health's (NIH) IT Acquisition and Assessment Center (NITAAC) administers a number of

government-wide acquisition contracts that can be used by any Federal agency to acquire information technology products, services and solutions. A third example is the Program Support Center (PSC), a shared service center within HHS. The PSC provides shared services, including shared IT systems, to customers within HHS and across the Federal Government.

Data Center Consolidation

One way we are successfully increasing the efficiency of the Department's IT portfolio is by consolidating data centers. In 2010, HHS identified over 200 data centers across the Department, and we developed a plan to close or consolidate roughly one quarter of them. Today, we are on our way to achieving this goal and have closed or consolidated almost 30 data centers since the Federal Data Center Consolidation Initiative (FDCCI) began.

We are excited about the evolution of the FDCCI – the new emphasis on optimizing core data centers which provide a better mechanism to elevate the efficiency and service delivery of HHS's critical data center assets. Ultimately, this policy, when compared to a count-driven view of our inventory, will drive better mission delivery to the taxpayer. At a department with as diverse a range of missions as HHS, the focus on efficiency over count positions us to make decisions about our data center inventory that make the best use of our limited resources.

Cloud Computing

Cloud computing is another area that promises to transform how we approach IT at the Department. Decisions to move our systems to the cloud are generally motivated by cost savings, better performance, and more efficient maintenance, but the move also provides a path to keep our systems continuously modernized. In addition to these factors, by leveraging cloud platforms we take advantage of flexible, scalable, highly available tools that allow us to deliver services that meet the American public's expectations – comparable to their interactions with business.

At the same time, we recognize that the promises of the cloud come with challenges – specifically, how to appropriately secure and protect the systems and information we move to the cloud. I'm happy to say that the Federal Risk and Authorization Management Program (FedRAMP) is proving to be an effective framework for addressing these challenges. A few weeks ago, HHS became the first agency to grant an Agency Authorization to Operate (ATO) for a cloud service provider through the FedRAMP process. In so doing, we made that provider's services available to the entire Federal Government, and we built a replicable and effective process that we plan to use for other vendors in the coming months.

The ability to leverage this process will enable continuing adoption of cloud solutions at HHS. Already, we have moved a number of systems and applications, including the grants-management system GrantSolutions.gov and the Food and Drug Administration's MedWatch+ system. Moving MedWatch+ in the cloud has reduced hosting costs by about 87% including just over \$1 million in hardware costs. We continue to consider cloud solutions as we evaluate new investments and the

modernization and enhancement of existing systems, and I anticipate that our use of the cloud will continue to grow as more providers receive FedRAMP security authorizations.

PortfolioStat

The PortfolioStat process has been a valuable tool to focus our efforts to look at our IT portfolio across the Department. We continue to work through this year's PortfolioStat with the Office of Management and Budget (OMB), but I can say that we learned some valuable lessons in the first PortfolioStat.

First and foremost, the PortfolioStat process highlighted some places where we had challenges in assembling a Department-level view of some of our commodity IT activities. The lessons learned from that exercise, coupled with OMB's simplification of the data collection process, are already providing us more timely information across the Department.

Second, the PortfolioStat provided a channel to discuss and prioritize Department-wide IT consolidation activities such as one of our more significant current activities, the Hire-to-Retire IT modernization program. Through the Hire-to-Retire program, we are moving the IT systems and activities supporting our core human resources, payroll, and time and leave functions to a shared service provider – effectively outsourcing a commodity activity, and getting to a better solution than we have in house, while realizing substantial operation cost efficiencies. By the conclusion of the Hire-to-Retire program, we will sunset at least 10 legacy systems, and we will have consolidated multiple conflicting HR data sources into a single authoritative system of record. In addition to the Hire-to-Retire program, we are also evaluating consolidation of our existing six email systems and moving email services to a cloud email provider, as other agencies have done, and looking at other opportunities to consolidate systems and acquisition of IT products and services.

Role of Agency Chief Information Officers

I understand that the role of department-level CIOs in driving all these efforts and in the direct management of departments' IT portfolios is an ongoing subject of discussion. As the current CIO of HHS and former CIO of the Social Security Administration (SSA), and with years of experience in private-sector IT, I have a perspective on this discussion informed by experience with a variety of governance structures.

First, regardless of the organization, IT leaders need to work in partnership with business or program leaders. If just the IT experts or just the business experts always have the final say, inefficiencies may follow. There are two questions relevant to every IT investment decision: what are we trying to accomplish and how (technically) will we deliver that outcome? The question of "what" should be answered first by the business – but the question of "how" is where IT needs to be empowered to provide solutions. At HHS, we have leveraged the TechStat process, on top of our existing stage-gate review model to bring business and IT decision makers together to achieve more efficient outcomes. Two recent HHS TechStats have resulted in project-level cost savings and cost avoidance of almost \$6 million dollars in FY 2012.

Second, regardless of the organization, there needs to be an enterprise-level IT perspective. Few effective private-sector organizations have subdivisions with total autonomy in the management of IT for any meaningful period. To operate as an enterprise requires someone to take the enterprise view. This is as true in IT as it is in program policy.

As the CIO at HHS, my job is to make sure that we effectively and efficiently manage our information resources. To be successful in that job, we need to maintain a governance structure that supports a strong business-IT partnership and ensures a place in decision making for the enterprise view.

Thank you for the opportunity to appear here today. I welcome your questions.

United States Government Accountability Office



Testimony
Before the Committee on Homeland
Security and Governmental Affairs,
U.S. Senate

For Release on Delivery
Expected at 10:30 a.m. EDT
Tuesday, June 11, 2013

INFORMATION TECHNOLOGY

OMB and Agencies Need to Focus Continued Attention on Eliminating Duplicative Investments

Statement of David A. Powner, Director
Information Technology Management Issues

GAO Highlights

Highlights of GAO-13-685T, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

With the federal government poised to reportedly spend at least \$82 billion on IT in fiscal year 2014, the magnitude of these expenditures highlights the importance of avoiding duplicative investments to ensure the most efficient use of resources. In a series of reports over the last few years, GAO has identified federal programs or functional areas where unnecessary duplication, overlap, or fragmentation exists. In particular, GAO has identified opportunities to reduce duplication and the cost of government operations in critical areas, such as federal data centers and IT investment management.

To help address IT duplication, OMB launched the PortfolioStat initiative. As part of this initiative, agencies are required to conduct an annual review of their IT investments and make decisions on eliminating duplication, among other things.

GAO was asked to testify on the results and recommendations from its selected reports that focused on IT duplication. To prepare this statement, GAO relied on previously published work.

What GAO Recommends

GAO has issued numerous recommendations to OMB and selected agencies to utilize existing transparency mechanisms and report the steps taken to avoid making duplicative investments.

View GAO-13-685T. For more information, contact David A. Powner at (202) 512-9288 or dpowner@gao.gov.

June 2013

INFORMATION TECHNOLOGY

OMB and Agencies Need to Focus Continued Attention on Eliminating Duplicative Investments

What GAO Found

GAO has identified a number of issues related to information technology (IT) duplication across the federal government. For example, GAO has previously reported that hundreds of investments provide similar functions. Specifically, agencies reported 1,536 information and technology management investments, 777 supply chain management investments, and 622 human resource management investments (see table).

Number of IT Investments Governmentwide by Primary Function		
Selected category of investment	Number of investments	Expenditures (\$ in millions)
Information and technology management	1,536	\$35.476
Supply chain management	777	3.327
Human resource management	622	2.406

Source: GAO analysis of the Office of Management and Budget's IT Dashboard, exhibit 53 data as of July 2011.

GAO further reported that while the Office of Management and Budget (OMB) and federal agencies have undertaken several initiatives to address potentially duplicative IT investments, such as consolidating similar functions through "line of business" initiatives, most of OMB's recent initiatives had not yet demonstrated results. Further, agencies were not routinely assessing operational systems to determine if they were duplicative. GAO recommended that OMB require federal agencies to report the steps they were taking to ensure that their IT investments were not duplicative as part of their annual budget and IT investment submissions. OMB agreed with the recommendation.

In addition, GAO reported on potentially duplicative investments at selected federal agencies. More specifically, although the Departments of Defense and Energy used various investment review processes to identify duplicative investments, GAO found that 37 of its sample of 810 investments were potentially duplicative. These investments accounted for about \$1.2 billion in total IT spending for fiscal years 2007 through 2012. For example, GAO identified four Department of the 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 functions. GAO recommended that the agencies report on the progress of efforts to identify and eliminate duplication, where appropriate; the agencies agreed with the recommendations.

In part to address duplicative IT investments, in March 2012 OMB launched PortfolioStat. Specifically, PortfolioStat is designed to assist agencies in assessing the current maturity of their IT portfolio management process, making decisions on eliminating duplication, and moving to shared solutions in order to maximize the return on IT investments across the portfolio. In March 2013, OMB reported that through this effort, agencies had identified and committed to nearly 100 opportunities to consolidate or eliminate commodity IT investments. OMB also believes that PortfolioStat may save the government \$2.5 billion by 2015. GAO has ongoing work looking at PortfolioStat, including determining whether agencies are completing key actions.



U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

Chairman Carper, Ranking Member Coburn, and Members of the Committee:

I am pleased to be here today to discuss duplicative information technology (IT) investments and the Office of Management and Budget's (OMB) PortfolioStat initiative. As reported to OMB, federal agencies plan to spend at least \$82 billion on IT in fiscal year 2014. Given the scale of such planned outlays, it is important that federal agencies avoid duplicative investments, whenever possible, to ensure the most efficient use of resources.

Over the past few years, we have issued a series of reports that have 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 In particular, we identified opportunities to reduce duplication and the cost of government operations in several critical IT areas, including avoiding investing in duplicative and unnecessary systems and underutilized federal data centers.

To help address IT duplication, in March 2012 OMB launched PortfolioStat, which requires agencies to conduct annual reviews of their IT investments and make decisions on eliminating duplication, among other things. According to OMB, PortfolioStat has the potential to save the government \$2.5 billion over the next 3 years.

You asked us to testify on the results and recommendations from our selected reports that focused on IT duplication.² Accordingly, my testimony specifically discusses our past work reporting on duplication,

¹GAO, *2013 Annual Report: Actions Needed to Reduce Fragmentation, Overlap and Duplication, and Achieve Other Financial Benefits*, GAO-13-279SP (Washington, D.C.: Apr. 9, 2013); *2012 Annual Report: Opportunities to Reduce Duplication, Overlap and Fragmentation, Achieve Savings, and Enhance Revenue*, GAO-12-342SP (Washington, D.C.: Feb. 28, 2012); and *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: Departments of Defense and Energy Need to Address Potentially Duplicative Investments*, GAO-12-241 (Washington, D.C.: Feb. 17, 2012); and *Information Technology: OMB Needs to Improve Its Guidance on IT Investments*, GAO-11-826 (Washington, D.C.: Sept. 29, 2011).

overlap, and fragmentation across the federal government and OMB's efforts to identify and address potentially duplicative IT investments through PortfolioStat. 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 provides a reasonable basis for our findings and conclusions based on our audit objectives.

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.³ 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. As reported to OMB, federal agencies plan to spend more than \$82 billion on IT investments in fiscal year 2014, which is the total expenditure for not only acquiring such investments, but also to operate and maintain them.

Opportunities to Reduce Duplication and Achieve Cost Savings Exist in Critical IT-related Areas

Over the past several years, we have reported that overlap and fragmentation among government programs or activities could be harbingers of unnecessary duplication.⁴ 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. Many of the government programs or activities with opportunities to reduce duplication and the cost of government operations are related to critical IT areas, including the following:

³OMB, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Washington, D.C.: December 2010).

⁴GAO-13-279SP, GAO-12-342SP, and GAO-11-318SP.

-
- *IT Dashboard.* Given the importance of transparency, oversight, and management of the government's IT investments, in June 2009 OMB established a public web site, referred to as the IT Dashboard, that provides detailed information on approximately 700 major IT investments⁵ at 27 federal agencies, including ratings of their performance against cost and schedule targets. The public dissemination of this information is intended to allow OMB; other oversight bodies, including Congress; and the general public to hold agencies accountable for results and performance. As of August 2012, 190 of the federal government's approximately 700 major IT investments—totaling almost \$12.5 billion—were in need of management attention.
 - *Federal data centers.* As federal agencies have modernized their operations, put more of their services online, and increased their information security profiles, they have demanded more computing power and data storage resources. According to OMB, the number of federal data centers grew from 432 in 1998 to more than 2,000 in 2010. The growth in the number of federal data centers, many offering similar services and resources, has resulted in overlap and duplication among the centers. In addition, according to OMB, in August 2009 the average utilization rate for servers ranged from 5 percent to 15 percent.
 - *IT investment management.* OMB and agencies need to address potentially duplicative IT investments to avoid investing in unnecessary systems. In fiscal year 2011, there were approximately 7,200 reported investments (includes major and nonmajor investments) totaling at least \$79 billion. The Department of Defense (Defense) reported the largest number of IT investments (2,383 investments at \$37 billion), followed by the Department of Energy (Energy) (876 investments and \$2 billion).

⁵According 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.

-
- *Geospatial investments.* The federal government collects, maintains, and uses geospatial information—information linked to specific geographic locations⁶—to help in decision making and to support many functions, including national security, law enforcement, health care, and environmental protection. Many activities, such as maintaining roads and responding to natural disasters—floods, hurricanes, and fires—can depend on critical analysis of geospatial information. Multiple federal agencies may provide services at the same geographic locations and may independently collect similar geospatial information about those locations. In August 2012, the Department of the Interior estimated that the federal government invests billions of dollars in geospatial data annually and reported that duplication among investments is common. Better coordination among these agencies could help reduce duplication of geospatial investments and provide the opportunity for potential savings of millions of dollars.
 - *Cloud computing.* As an emerging approach to delivering IT services, cloud computing provides on-demand access to a shared pool of scalable computing resources. According to OMB, cloud computing has the potential to address IT inefficiencies by providing services both more quickly and at a lower cost. OMB further noted that IT services costing billions of dollars annually could potentially be migrated to cloud computing. Accordingly, agencies have reported saving millions of dollars from implementing cloud-based solutions. In particular, the Department of Homeland Security (DHS) reported that its implementation of enterprise content delivery services avoids an estimated \$5 million in costs annually.
 - *Enterprise architecture.* An enterprise architecture is a modernization blueprint that is used by organizations to describe their current state and a desired future state and to leverage IT to transform business and mission operations. In light of the importance of developing well-defined enterprise architectures, we issued a seven-stage enterprise architecture management maturity framework that defines actions

⁶For example, entities such as houses, rivers, road intersections, power plants, and national parks can all be identified by their location. In addition, phenomena such as wildfires, the spread of the West Nile virus, and the thinning of trees because of acid rain can also be identified by their geographic locations.

needed to effectively manage an architecture program.⁷ The alternative, as our work has shown, is the perpetuation of the kinds of operational environments that burden most agencies today, where a lack of integration among business operations and the IT resources supporting them leads to systems that are duplicative, poorly integrated, and unnecessarily costly to maintain.

OMB Initiated Recent Major Initiatives for Reducing Duplication and Achieving Cost Savings

OMB has implemented a series of initiatives to manage IT more effectively, reduce duplication, and achieve cost savings. These efforts include the following:

- *TechStat reviews.* In January 2010, the Federal Chief Information Officer (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. Subsequently, OMB empowered agency CIOs to hold their own TechStat sessions within their respective agencies. As of April 2013, OMB reported that it had led 79 sessions that resulted in improvements to or termination of IT investments with performance problems. According to the former Federal CIO, the efforts of OMB and federal agencies to improve management and oversight of IT investments have resulted in almost \$4 billion in savings.
- *Federal Data Center Consolidation Initiative.* In February 2010, the Federal CIO established the Federal Data Center Consolidation Initiative to address the growing number of federal data centers. This initiative’s four high-level goals are to promote the use of “green IT”⁸ by reducing the overall energy and real estate footprint of government data centers; reduce the cost of data center hardware, software, and operations; increase the overall IT security posture of the government; and shift IT investments to more efficient computing platforms and technologies. OMB believes that this initiative has the potential to provide about \$3 billion in savings by the end of 2015.

⁷GAO, *Organizational Transformation: A Framework for Assessing and Improving Enterprise Architecture Management (Version 2.0)*, GAO-10-846G (Washington, D.C.: August 2010).

⁸“Green IT” refers to environmentally sound computing practices that can include a variety of efforts, such as using energy efficient data centers, purchasing computers that meet certain environmental standards, and recycling obsolete electronics.

-
- *PortfolioStat reviews.* In March 2012, OMB launched the PortfolioStat initiative, which requires agencies to conduct an annual agency-wide IT portfolio review to, among other things, reduce commodity IT⁹ spending and demonstrate how their IT investments align with the agency's mission and business functions.¹⁰ PortfolioStat is designed to assist agencies in assessing the current maturity of their IT investment management process, making decisions on eliminating duplicative investments (such as geospatial information), and moving to shared solutions (such as cloud computing) in order to maximize the return on IT investments across the portfolio. While OMB's TechStat reviews are intended to examine IT performance at the specific project or investment-level, PortfolioStat reviews are intended to examine the portfolio as a whole and draw on the agency's enterprise architecture to help identify and eliminate areas of duplication and waste. OMB believes that the PortfolioStat effort has the potential to save the government \$2.5 billion over the next 3 years by, for example, consolidating duplicative systems.

**GAO Has Previously
Reported on IT Investment
Management at Selected
Agencies**

During the past few years, we have reported on IT investment management—an important mechanism for identifying and analyzing duplicative investments—at key agencies. For example, in July 2011, we reported¹¹ that the Internal Revenue Service (IRS) had established most of the foundational practices needed to manage its IT investments, but that additional improvements were needed. Specifically, the agency had executed 30 of the 38 key practices identified by GAO's Information Technology Investment Management framework¹² as foundational for successful IT investment management, including all the practices needed to provide investment oversight and capture investment information. For

⁹According to OMB, commodity IT includes services such as IT infrastructure (data centers, networks, desktop computers and mobile devices); enterprise IT systems (e-mail, collaboration tools, identity and access management, security, and web infrastructure); and business systems (finance, human resources, and other administrative functions).

¹⁰OMB, *Implementing PortfolioStat*, Memorandum M-12-10 (Washington D.C.: Mar. 30, 2012).

¹¹GAO, *Investment Management: IRS Has a Strong Oversight Process But Needs to Improve How It Continues Funding Ongoing Investments*, GAO-11-587 (Washington, D.C.: July 20, 2011).

¹²GAO, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity*, GAO-04-394G (Washington, D.C.: March 2004).

instance, IRS had defined and implemented a tiered governance structure to oversee its projects and had several mechanisms for the boards to regularly review IT investments' performance. However, we reported that, despite these strengths, IRS could improve its investment management process in two key areas. First, IRS did not have an enterprisewide IT investment board with sufficient representation from IT and business units that was responsible for the entire investment management process, and as a result may not have been optimizing its decision-making process. Second, IRS did not have a process, including defined criteria, for reselecting (i.e., deciding whether to continue funding) ongoing projects. We concluded that, given the size of its IT budget, IRS could be spending millions of dollars with no assurance that the funds are being used wisely. Accordingly, we made recommendations to IRS to, among other things, assign responsibilities for implementing the investment management process to optimize decision making, and define and implement a process for deciding whether to continue funding ongoing projects; the agency concurred with our recommendations.

More recently, in July 2012, we reported¹³ that DHS was making progress in developing and implementing a new IT governance process that focused on portfolio management and eliminating duplication. Specifically, we found that DHS had developed a new governance framework and that the associated policies and procedures were generally consistent with recent OMB guidance and with best practices for managing projects and portfolios identified in GAO's Information Technology Investment Management framework.¹⁴ For example, DHS's new governance framework included the establishment of portfolio governance boards to oversee functional portfolios with the goals of eliminating duplication and leveraging services and programs across the department. However, the agency had not yet finalized most policies and procedures and was not fully using best practices for the implementation. Accordingly, we made recommendations to DHS to, among other things, strengthen its new governance process and related IT management capabilities; the agency agreed to implement the recommendations.

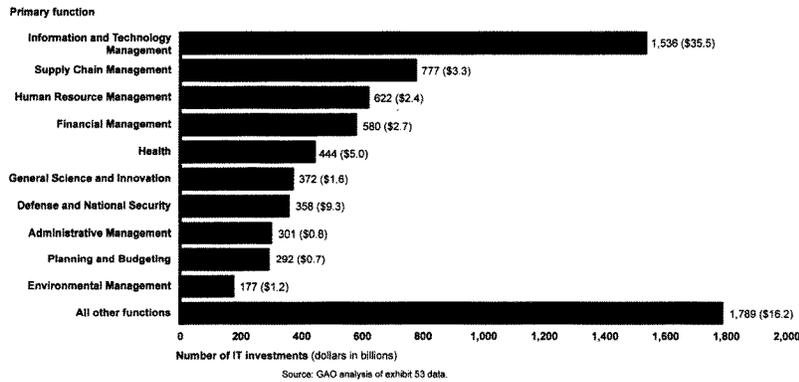
¹³GAO, *Information Technology: DHS Needs to Further Define and Implement Its New Governance Process*, GAO-12-818 (Washington, D.C.: July 25, 2012).

¹⁴GAO-04-394G.

OMB and Agencies Have Taken Steps to Reduce Duplicative IT Investments, but More Remains to Be Done

In September 2011, we reported¹⁵ that, although OMB's guidance to federal agencies on how to categorize IT investments allowed for analysis of investments with similar functions, it did not go far enough to allow identification of potentially duplicative investments. Specifically, since the fiscal year 2004 budget cycle, OMB had required agencies to categorize their IT investments according to primary function and subfunction. 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 1 depicts, by primary function, the total number of investments within the 26 federal agencies that report to the IT Dashboard, as of July 2011.

Figure 1: Number of Government IT Investments by Primary Function, as of July 2011



We also found that the at least \$79 billion in IT investments for fiscal year 2011 did not include IT investments by 58 independent executive branch

¹⁵GAO-11-826.

agencies, including the Central Intelligence Agency and Securities and Exchange Commission, or by the legislative or judicial branches. A closer look at the investments for the 26 agencies also revealed that some agencies excluded systems that fit the definition of an IT investment, such as space systems and systems that are in research and development.

Further, we reported that, while OMB guidance stated that an investment needs to be mapped to a single functional category within the Federal Enterprise Architecture,¹⁶ IT investments could fit into more than one category. For example, an agency could identify an inventory system as a financial management system or a supply chain management system. Thus, if an organization planned to develop an inventory system and searched for potentially duplicative investments in a group labeled as financial management systems, it would miss seeing potentially duplicative systems categorized as supply chain management systems. As an example, we cited our May 2009 finding that a Defense financial management system was identified in a different functional category—supply chain management.¹⁷ We noted that because Defense had categorized the system as supply chain management, the cost of this system was not included in OMB's estimate for financial management systems.

Finally, we reported that OMB and federal agencies had undertaken several initiatives to address potentially duplicative IT investments. For example, OMB had efforts under way to consolidate similar functions through its "line of business" and Federal Enterprise Architecture initiatives and had eliminated duplicative systems identified during its TechStat sessions. In addition, several of the agencies we evaluated had established guidance for ensuring new investments were not duplicative with existing systems. However, we found that most of OMB's recent initiatives had not demonstrated results. Further, several agencies did not

¹⁶The Federal Enterprise Architecture 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.

¹⁷GAO, *Financial Management Systems: OMB's Financial Management Line of Business Initiative Continues but Future Success Remains Uncertain*, GAO-09-328 (Washington, D.C.: May 7, 2009).

routinely assess legacy systems to determine if they were duplicative. We concluded that, until agencies routinely assess their entire IT portfolios to identify and remove or consolidate duplicative systems, such duplication will continue to exist.

Accordingly, 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 agreed with our recommendation and has since taken action to implement it. Specifically, in March 2012, the OMB issued a memorandum to federal agencies regarding implementing PortfolioStat reviews. As previously mentioned, these reviews are intended to assist in ending the investment in duplicative IT investments. In addition, as part of this effort, OMB is requiring agencies to document their cost savings and cost avoidance due to consolidation beginning in their fiscal year 2014 budget submissions.

**Selected Federal Agencies
Have Potentially
Duplicative Investments**

In February 2012, we reported¹⁸ that although Defense, Energy, and DHS utilized various processes to prevent and reduce investment in duplicative programs and systems, potentially duplicative IT investments existed. Specifically, each of the agencies we reviewed had IT investment management processes in place that were, in part, intended to prevent, identify, and eliminate unnecessary duplicative investments. For example, Defense's *Information Technology Portfolio Management Implementation* guide required the evaluation of existing systems to identify duplication and determine whether to maintain, upgrade, delete, or replace identified systems. Similarly, Energy's *Guide to IT Capital Planning and Investment Control* specified 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 were to 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.

¹⁸GAO-12-241.

Even with such investment review processes, of the 810 investments we reviewed,¹⁹ we identified 37 potentially duplicative investments at Defense and Energy within three Federal Enterprise Architecture categories (Human Resource Management, Information and Technology Management, and Supply Chain Management).²⁰ These investments accounted 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 Defense and
- 6 potentially duplicative investments totaling approximately \$8 million at Energy.

The 37 investments comprised 12 groups of investments that appeared 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 Energy that were each responsible for managing the backend infrastructure at three different locations. We also identified four Department of the Navy (Navy) personnel assignment investments—one system for officers, one for enlisted personnel, one for reservists, and a general assignment system—each of which was responsible for managing similar assignment functions. Additionally, the Department of the Air Force had five investments that were each responsible for contract management, and within the Navy there were another five contract management investments. Table 1 summarizes the 12 groups of potentially duplicative investments we identified by purpose and agency.

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

²⁰Within the three selected functions, we narrowed our review to the following seven subfunctions: 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
Defense	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
	Defense Enterprisewide	Civilian Personnel Management	2	\$504
Energy	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 independently identified several duplicative investments and systems. Specifically, DHS officials 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 also identified 38 additional systems that they 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 existed for a number of reasons, including decentralized governance within the departments and a lack of control over contractor facilities. For example, Energy investments for the management of back-end infrastructure were for facilities which Energy oversaw but does not control. In addition, Defense officials indicated that a key reason for potential duplication at 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 was the miscategorization of investments. Among the 810 investments we reviewed, we identified 22 investments where the selected agencies assigned incorrect Federal Enterprise Architecture primary functions or subfunctions. Specifically, we identified 13 miscategorized investments at Defense, 4 at Energy, 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 subfunction, but DHS agreed that this investment should have been assigned to the Human Resources Development subfunction.

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

Therefore, we recommended in our report that Defense and Energy utilize existing transparency mechanisms, such as the IT Dashboard, to report on the results of the departments' efforts to identify and eliminate, where appropriate, each potentially duplicative investment we have identified, as well as any other duplicative investments. In response, Defense and Energy stated that they agreed with our recommendations. In addition, Energy's Office of the CIO stated that the agency was committed to increasing its IT investment oversight.

To Address Duplicative IT
Investments, OMB
Launched PortfolioStat

In March 2012, OMB launched the PortfolioStat initiative, which requires agencies to conduct an annual agency-wide IT portfolio review to, among other things, reduce commodity IT spending and demonstrate how its IT investments align with the agency's mission and business functions.²¹ PortfolioStat is designed to assist agencies in assessing the current maturity of their IT portfolio management process, making decisions on eliminating duplication, and moving to shared solutions in order to maximize the return on IT investments across the portfolio. According to OMB, while TechStat reviews examine IT performance at the specific project or investment-level, PortfolioStat reviews examine the portfolio as a whole and draw on the agency's enterprise architecture to help identify and eliminate areas of duplication and waste. OMB believes that the PortfolioStat effort has the potential to save the government \$2.5 billion over the next 3 years by, for example, consolidating duplicative systems.

As part of this initiative, OMB required agency Chief Operating Officers to lead a PortfolioStat review on an annual basis—working in coordination with CIOs, Chief Financial Officers, and Chief Acquisition Officers. Such an effort is appropriate given the numerous investments performing the same function, as we reported in February 2012.²² For example, as noted previously, 26 major federal agencies had planned to spend \$2.7 billion on 580 financial management systems in 2011. According to OMB, agencies were required to designate a lead with direct reporting authority to the Chief Operating Officer for implementing the PortfolioStat process and OMB requirements by April 2012, and develop a baseline of their commodity IT investments by June 15, 2012. Using this portfolio data, agencies were asked to consolidate commodity IT spending under the agency CIO, hold a PortfolioStat session by July 31, 2012, with key stakeholders, and submit a final plan to consolidate their IT portfolio by August 31, 2012, including outlining at least 3 years of agency consolidation activities and migrating at least two duplicative commodity IT services by December 31, 2012.

Subsequently, in March 2013, OMB issued a memorandum documenting additional guidance to help strengthen the PortfolioStat initiative and noted that the results from PortfolioStat so far had been significant—including that agencies had identified and committed to nearly 100

²¹OMB, Memorandum M-12-10.

²²GAO-12-241.

opportunities to consolidate or eliminate commodity IT investments.²³ Among other things, OMB's memorandum describes plans to strengthen the initiative by integrating PortfolioStat and the Federal Data Center Consolidation Initiative,²⁴ streamlining agency reporting requirements, and establishing guidance for conducting PortfolioStat sessions in fiscal year 2013. For example, to improve the outcomes of PortfolioStat and to advance agency IT portfolio management, OMB's memorandum consolidated previously collected IT plans, reports, and data calls into three primary collection channels—an information resources management strategic plan,²⁵ an enterprise road map,²⁶ and an integrated data collection channel.²⁷ Agencies' draft versions of their strategic plans and enterprise road maps were due to OMB in May 2013, as well as their first integrated data collections. The integrated data collections are to be updated quarterly beginning in August 2013 and the strategic plans and road maps are to be updated after Congress receives the President's budget for fiscal year 2015.

We recently reported²⁸ and testified²⁹ on, among other things, OMB's efforts to integrate the Federal Data Center Consolidation Initiative with

²³OMB, *Fiscal Year 2013 PortfolioStat Guidance: Strengthening Federal IT Portfolio Management*, Memorandum M-13-09 (Washington, D.C.: Mar. 27, 2013).

²⁴OMB established the Federal Data Center Consolidation Initiative, under the direction of the Federal CIO, in February 2010 to reduce the size of the federal data center inventory and improve the efficiency, performance, and the environmental footprint of federal data center activities.

²⁵OMB, *Management of Federal Information Resources*, Circular A-130 (Washington, D.C.: Nov. 30, 2000). According to OMB Circular A-130, an agency's information resources management strategic plan should describe how information resources management activities help accomplish agency missions, and ensure that information resource management decisions are integrated with organizational planning, budget, procurement, financial management, human resources management, and program decisions.

²⁶OMB, *Increasing Shared Approaches to Information Technology Services* (Washington, D.C.: May 2, 2012). The enterprise road map is to include a business and technology architecture, an IT asset inventory, a commodity IT consolidation plan, a line of business service plan, and an IT shared service plan.

²⁷The integrated data collection channel will be used by agencies to report structured information, such as progress in meeting IT strategic goals, objectives, and metrics, as well as cost savings and avoidances resulting from IT management actions.

²⁸GAO, *Data Center Consolidation: Strengthened Oversight Needed to Achieve Cost Savings Goal*, GAO-13-378 (Washington, D.C.: Apr. 23, 2013).

PortfolioStat and found that key performance metrics were not yet fully defined. More specifically, OMB's March 2013 memorandum³⁰ stated that, to more effectively measure the efficiency of an agency's data center assets, agencies would also be measured by the extent to which their data centers are optimized for total cost of ownership by incorporating metrics for data center energy, facility, labor, and storage, among other things. However, we found that although OMB had indicated which performance measures it planned to use going forward, it had not documented the specific metrics for agencies to report against. OMB's March 2013 memorandum indicates that these would be developed by the Data Center Consolidation Task Force,³¹ but did not provide a time frame for when this will be completed.

Further, our report noted that OMB's integration of the Federal Data Center Consolidation Initiative with PortfolioStat also included a modification to the previous data center consolidation goal of closing approximately 40 percent of the total number of agency data centers. Specifically, OMB stated an agency's data center population will now be placed into one of two categories—core and non-core data centers—but for which the memorandum did not provide specific definitions. OMB further stated that its new goal is to close 40 percent of non-core data centers but, as noted, the definition of a core and non-core data center was not provided. Therefore, the total number of data centers to be closed under OMB's revised goal could not be determined.

We also reported that, although OMB had previously stated that PortfolioStat was expected to result in savings of approximately \$2.5 billion through 2015, its March 2013 memorandum did not establish a new cost savings goal that reflected the integration of the Federal Data Center Consolidation Initiative. Instead, OMB stated that all cost savings goals previously associated with the Federal Data Center Consolidation Initiative would be integrated into broader agency efforts to reshape their IT portfolios, but did not provide a revised savings estimate. We

²⁹GAO, *Data Center Consolidation: Strengthened Oversight Needed to Achieve Billions of Dollars in Savings*, GAO-13-627T (Washington, D.C.: May 14, 2013).

³⁰OMB, Memorandum M-13-09.

³¹The Data Center Consolidation Task Force is comprised of the data center consolidation program managers from each agency. According to its charter, the Task Force is critical to supporting collaboration across the Federal Data Center Consolidation Initiative agencies, including identifying and disseminating key pieces of information, solutions, and processes that will help agencies in their consolidation efforts.

concluded that the lack of a new cost savings goal would limit OMB's ability to determine whether or not the new combined initiative is on course toward achieving its planned objectives. As a result, we recommended that OMB track and annually report on key data center consolidation performance measures, such as the size of data centers being closed and cost savings to date. OMB agreed with our recommendation.

We have ongoing work looking at OMB's PortfolioStat initiative, including determining whether agencies completed key required PortfolioStat actions, evaluating selected agencies' plans for making portfolio improvements and achieving associated cost savings, and describing OMB's plans to improve the PortfolioStat process.

In summary, while OMB and agencies have taken steps to improve their ability to identify and categorize IT investments, duplicative IT investments still exist at federal agencies. Because these investments account for billions of dollars in spending, it will be important for OMB and agencies to implement our prior recommendations to better ensure that duplicative investments are identified and eliminated.

To help agencies better address duplicative IT investments, OMB established PortfolioStat as a means of assisting agencies with the assessment of the maturity of their IT investment management processes and eliminating areas of duplication and waste. OMB recently released additional guidance that expanded this important initiative's scope and reported that significant progress had been made to date, including more than 100 opportunities to consolidate or eliminate commodity IT investments. Moving forward, it will be important for OMB to be transparent on agencies' progress against key performance metrics, such as cost savings, in order to ensure that the PortfolioStat initiative is meeting its established objectives.

Chairman Carper, Ranking Member Coburn, and Members of the Committee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

**GAO Contact and
Staff
Acknowledgments**

If you or your staffs have any questions about this testimony, please contact me at (202) 512-9286 or at pownerd@gao.gov. Individuals who made key contributions to this testimony are Dave Hinchman (Assistant Director), Justin Booth, Kate Feild, Rebecca Eyer, Valerie Hopkins, Sabine Paul, Colleen Phillips, Bradley Roach, Jonathan Ticehurst and Kevin Walsh.

June 25th 2013

Statement of Vance E. Hitch

Former Chief Information Officer Of The Department Of Justice.

For the Record of the Senate Committee on Homeland Security and Government Affairs.

"Reducing Duplication and Improving Outcomes In Federal Information Technology"

Introduction

I am pleased to submit my statement for the record on how to make information technology (IT) more efficient and effective in the Federal government. My observations are based on more than 40 years of experience in IT, including more than 9 years as the Chief Information Officer (CIO) of the Department of Justice (DOJ). Since retiring from DOJ in July of 2011, I have continued to be active in Federal IT, working part-time for Deloitte Consulting and serving as a SAGE (Strategic Advisor for Government Executives) CIO with the Partnership for Public Service. As a citizen and as an IT professional, I have a passion for "good government" and I firmly believe that IT can and should play a leading role in helping government deliver smarter more cost effective services.

I am proud of what I accomplished during my tenure at DOJ. I viewed my role as a key change agent for the Department and helped lead DOJ through two major generations of IT transformation. In the years immediately following the tragic events of 9/11/2001, I envisioned and led the Law Enforcement Information Sharing Program (LEISP) to provide appropriate information sharing and "connecting the dots" within the Department and across the entire Law Enforcement community. Also, starting in approximately 2007, I created a Department wide Cyber Security Program to detect and prevent cyber incidents from compromising the integrity of DOJ's data and infrastructure. As the CIO for DOJ for over nine years, I was by far at the time the longest serving CIO of a major cabinet agency. A key driver for me in staying that long in a difficult and, at times, seemingly thankless position was to see these major transformations involving scores of projects through to substantive completion (spanning planning, design, development, conversion, rollout, and operational support on a national and/or enterprise basis). My lingering regret is that these transformations, as well as the other enterprise projects we pursued during my tenure, took longer and were more costly than I would have liked due to many of the issues described below.

Core Reasons for Federal IT inefficiencies

Certainly, the Federal government and major agencies like DOJ are among the largest and most complex organizations in which to implement IT. In 2011 alone, Federal agencies spent nearly \$80B on IT. Based on my years at DOJ and my private sector experience, I am convinced that this huge base IT spend can be leveraged more effectively to improve mission accomplishment and enlightened management. Likewise, I believe government can and should be more efficient to get more capability /results for each IT dollar spent and /or to cut IT costs where prudent. However, to accomplish these objectives, Congressional and Executive leadership need to clarify and strengthen the role of agency CIO and to hold those in that position accountable for results.

Much of the Federal government's IT spending goes into the maintenance of a highly inefficient, highly duplicative, fragmented technology infrastructure. Hundreds (if not thousands) of separately managed help desks, networks, email systems, and office systems mean that government misses many opportunities for economies of scale. Also, because the technology infrastructure is reflective of the government's underlying business structure, efforts to address those inefficiencies have fallen short of their intent. In addition, investments we do make in new technology solutions are not consistently successful. While there have been notable successes (e.g. DOJ's National Digital Exchange or NDEX) far too many of our IT projects to run into trouble. The reasons for inefficiencies in government IT are many; I will highlight a few: (1) Organizational complexity and cultural resistance to change cause Government IT projects to be more costly and more risky than similar private sector projects. Even successful projects take way too long, at best deferring benefits, at worst being out-dated when implemented. (2) While the private sector treats IT projects as investments, Federal Budgets and Appropriations treat all IT as cost line items, often delaying projects and deferring potential savings and benefits. (3) Budget process delays and uncertainties add to the risk and the delivery timelines. (4) Distributed management control of IT (accompanied by lack of clear accountabilities) can lead to redundant, stove piped systems; lack of enterprise IT portfolio visibility and accountability; and failure to take advantage of economies of scale. (5) Critical IT skillsets, both management and technical, are extremely difficult to acquire due to lengthy hiring, training and contracting processes.

Role of CIO - Current State

Starting with the passage of Clinger-Cohen 1996, the policy framework for effective IT management was put in place. The position of Chief Information Officer was identified and chartered to make CIOs of cabinet agencies responsible to their agency heads for the efficient and effective acquisition and management of IT. Clinger-Cohen specifically includes as CIO responsibilities developing an integrated IT architecture for the entire agency and promotion of efficient and effective design and operation of all IT management processes including improvements to work processes.

Also, through the efforts of multiple Administrations, many best practices have been established in Federal IT policy by OMB. These include, among others, requiring agencies to put in place (1) An agency wide enterprise architecture; (2) Common e-government applications to drive more efficient citizen involvement and visibility; (3) Plans for leveraging Lines of Business applications for selected common business functions across government; (5) Policies for cloud 1st adoption when evaluating new technology needs. (6) A digital government strategy (established in 2012) to direct agencies to enable systems to provide appropriate access to data by key stakeholders, including citizens; and (7) Data Center Consolidation Initiative to reduce duplicative capabilities and assets. While each of these efforts have provided/will provide some incremental improvements, their results have not been transformative. By and large, these initiatives were instituted by OMB as "unfunded mandates" with inadequate and/or no specific funding support. CIOs are expected to accomplish them within the existing IT funding sources, many of which CIOs don't control. Thus, CIOs can lead the charge but can only be held accountable for "best efforts". Likewise, projected savings / efficiencies are difficult to nail down and account for in "hard" dollar reductions to specific budgets.

I believe the shortfall in IT effectiveness in Government is due in large part to a lack of consolidated technology management and budget control – fundamental aspects of Clinger-Cohen and other elements of the IT policy framework at the agency level. I also believe that a strong CIO, as envisioned by Clinger-Cohen, is key to effective IT management and necessary to overcome the extraordinary complexities and challenges of Government IT. But Clinger-Cohen is implemented differently in each Cabinet agency. As currently implemented across the Federal Government: (1) CIOs rarely report directly to their Agency heads, they usually report to the Chief Financial Officers or occasionally the Chief Management Officers (2) CIOs often do not control their agency IT budgets. IT budget items are usually parceled out across different appropriations; and the CIO often does not have visibility or control of IT budgets managed at the component level. (3) Many CIOs have no direct organizational ties to the "CIOs" of components within their agencies and have minimal role in their selection or evaluation.

Role of CIO – "Empowered" State

In my view, the key element that is missing to the detriment of cost effective, mission enabling IT programs, is the empowerment of the agency CIO with budget control over all IT at their agencies and the full support of the agency leadership. This would require implementation of the following concepts into agency policy and practices: (1) IT is an enterprise asset under the management control of the CIO. (2) IT includes both mission support and administrative applications and technologies. (3) IT budgets include infrastructure, development, operations and maintenance, and workforce elements (4) The CIO has the authority to start, stop, cancel and transfer IT budget resources with the concurrence of the Agency head as needed for the effective implementation of the overall IT program. (5) The CIO will establish an appropriate Governance process to receive input from and to report progress to key Stakeholders. (6) All IT must be clearly identified in component budgets and programs, and a consolidated IT view of budgets and costs must be implemented, whether through actual consolidation or summarized reporting. (7) The CIO must be included in all substantive budget negotiations relating to the IT budget. (8) The CIO must have strong reporting ties to the Agency Executive or Deputy to provide ongoing visibility and support of IT priorities. (9) The CIO must have a strong role in the recruitment, hiring, evaluation, and promotion of key IT personnel across the agency including its large components. (10) The CIO must be incented and rewarded for "good government" activities such as saving costs, prudent technology innovation, and technology refreshment. This may require the implementation of new business models (e.g. technology working capital funds). (11) Finally, there has been an ongoing debate over whether an "empowered" CIO should be a political appointee or a career civil servant. Although there are strong arguments on both sides, I favor making the CIO a 6 to 8 year tenured appointment. I believe this would elevate the position, attract highly experienced executives, and provide greater continuity to Federal IT efforts.

Portfolio and Other Management Processes.

Portfolio as implemented by OMB over the past 2 years is to be applauded; it is definitely a step in the right direction. Portfolio is intended to identify and prioritize enterprise IT initiatives and gain support for them from agency and OMB leadership. The inclusion this year of the Data Center Consolidation Initiative efforts is also an excellent move because of the difficult decisions and tradeoffs that must be made in each agency. While I am totally supportive of Portfolio, my experience leads me to ask 2 questions. Improvements may be needed to address each of the following questions affirmatively:

(1) Does the agency IT portfolio represent a forward looking vision or does it represent a 'dated' view of the legacy environment with natural extensions? I believe that Portfolio should require a "ground up" refreshed agencywide IT Strategic Plan be performed periodically. It should be based on the agency business/strategic plan and should make sure the agency is leveraging modern technology to effectively accomplish its mission and management.

(2) Does the IT portfolio include all significant IT programs and spend? I know how difficult it is to identify and capture good information on IT costs, including shadow IT (expended on behalf of IT initiatives but funded elsewhere). Because IT responsibilities have been diffused, most financial and management systems do not capture and track IT costs and initiatives as discrete entities. The OMB IT Dashboard implemented several years ago helps at a macro-level to provide visibility of major initiatives. However, the detailed agency feeder mechanisms are very immature, ad hoc, and are often neither comprehensive nor accurate. I believe that CIOs "empowered" as described earlier in this statement, should be tasked to define, design, and implement improved IT management processes and systems that accurately identify and track IT costs and activities for all IT functions and services (e.g. operations, development, maintenance, etc.). I believe that IT Systems Management (ITSM) Improvements should be defined as a project and included in Portfolios as appropriate.

Conclusion

Clinger-Cohen has been in place for seventeen years, and incremental improvements in IT management have been initiated by many Administrations. Yet there remains a significant performance gap between the Federal government and the private sector in cost effectively deploying IT to mission and business functions. I believe that Congressional and Executive actions are appropriate and necessary to achieve transformative improvements in Federal IT effectiveness and efficiency. Such actions could include:

- (1) Strengthening the role of the agency CIO and holding "empowered" CIOs accountable.
- (2) Building on the Portfoliostat process to require: (a) Periodically refreshed, forward looking IT Strategic Plan for each agency, and (b) IT Systems Management improvements as needed to assure comprehensive capture and monitoring of agency IT costs.



PARTNERSHIP FOR PUBLIC SERVICE

OURPUBLICSERVICE.ORG
1100 New York Ave NW Suite 200 East Washington DC 20005

SAGE: REMARKS FOR THE RECORD, "REDUCING OUTCOMES AND IMPROVING OUTCOMES IN FEDERAL INFORMATION TECHNOLOGY"

1. DO YOU BELIEVE THAT IT IS NECESSARY FOR AN AGENCY CIO TO HAVE BUDGET AUTHORITY FOR IT SPENDING ACROSS AN AGENCY? ARE THERE OTHER WAYS TO EMPOWER AN AGENCY CIO?

Budgetary authority is absolutely crucial for CIOs to be able to actually reduce duplication and wasteful, inefficient spending. Because the budget is the document by which strategic decisions are made and operational and implementation accountability are too diffused across the federal government and within agencies. Without control of the budget, CIO authority is significantly diminished and the ability of the CIO to 'play' in the decision-making process. In addition, budgetary authority, including the ability to control infrastructure (data centers, telecommunications, desktop support, etc.), would give CIOs the ability to get out in front and shape outcomes, as opposed to simply trying to stop bad projects, and to promote savings through shared services and collaboration.

2. HOW IMPORTANT IS IT FOR A DEPARTMENT-LEVEL CIO TO HAVE VISIBILITY INTO THE INFORMATION TECHNOLOGY SYSTEMS AND APPLICATIONS THAT COMPONENTS ARE RUNNING

Visibility is critical in many areas and functions of IT to ensuring that progress is being made in optimizing and creating common Enterprise Architecture within agencies, increasing effectiveness, and reducing cost. In addition, there are core capabilities within the IT sphere that require daily reporting and visibility to the CIO, including safety of life and cybersecurity (with agencies like to offer their own ideas on the most critical capabilities. This does not need to be intrusive, but can be a N/SOC network attached device monitoring approach that will locate infrastructure anomalies and can be used in a "Departmental POAM process" to make changes to further strengthen the architecture, share resources and enhance the security posture of the Department.

3. HOW IMPORTANT IS THE PARTICIPATION OF AGENCY LEADERSHIP IN IMPLEMENTING CLINGER-COHEN AND EMPOWERING THE CIO'S OFFICE?

Agency leadership has the ability to play a major role in implementing Clinger-Cohen and empowering agency and bureau-level CIOs. However, the CIO is not just a technical position, but a strategic one. For the CIO to be truly effective, it must be an individual who can communicate and navigate organizational politics, as well as someone who is mission-focused and respected by his or her peers. Without these qualities, the authority of the position is bound

to be diminished. Agencies would be best served to include IT infrastructure in the portfolio of either the Secretary or Deputy Secretary, so that they can provide a unified approach to management activities (especially around budget formulation or audit time). Clinger-Cohen's ties to the CFO Act allow a natural opportunity to raise IT management to the level of other C-suite management activities. A simple change to the CFO Act would incorporate IT Management into the best management practices approach that is already required of OMB Circular A-123.

4. WHAT ARE THE BIGGEST CHALLENGES THAT AGENCY CIOs FACE IN CONDUCTING EXAMINATION OF IT SPENDING ACROSS DEPARTMENTS?

The two biggest challenges are access to in-depth data on IT spending and time management. Most CIOs can ask the right questions but lack access to program-by-program, project-by-project spending data that would tell them what is happening on a daily basis. This data is relatively easy to get, though sometimes vendors can be reluctant to share it. Additionally, all program spending that does not meet FISMA's definition of a "major system" falls outside of the Departmental IT review process. These expenditures should be included in each yearly budgetary review planning process.

Time management has been flagged as another issue. Many CIOs simply spend too much time triaging failed or struggling project and can be overwhelmed by the most critical problems. This leaves little time for strategic thinking and looking for IT infrastructure-enhancement opportunities, and makes CIOs less effective.

5. WHAT ARE YOUR OPINIONS OF THE PORTFOLIOSTAT PROCESS?

PortfolioStat is effective at setting expectations and holding people accountable for the outcomes of their projects. It should continue to stay focused on uncovering challenges and bringing in support where needed, rather than becoming a "gotcha" or a compliance exercise. However, it is important to remember that PortfolioStat is only reflective of the past and not the future. It does not show what is planned for a project and whether that dovetails with departmental or administration priorities. It is the ability to look into the future goals for a project that will allow program managers and the CIO to develop plans for corrective action and save significant time and money.

6. WHAT DOES THE CONGRESS, THE ADMINISTRATION AND OUR AGENCIES NEED TO DO TODAY AND OVER THE NEXT FEW YEARS, TO MAKE SURE THAT, 20 YEARS FROM NOW, WE ARE NOT STILL CONFRONTING THE SAME PROBLEMS THAT WE FACE TODAY?

There are a number of potential answers to this. Centralizing authority in the CIO and raising its profile so that CIOs (at least for agencies that are part of the CIO council) are reporting directly to the Deputy Secretary and are on par with the Departmental CFO and other C-suite executives. Agencies must also eliminate proprietary, customized solutions for IT needs and replace them with open-architecture, standards-based, modular systems that promote the use of shared services across the organization. OMB should also promote a unified IT and budgetary review of agencies and encourage agencies to give the Departmental CIO approval

of the IT budget proposal and approval of IT expenditures across the agency. Congress and the administration should also consider finding ways to allow for the removal of poor-performers much more quickly.

While these options will help enhance CIO authorities and ensure that the continued issues that hinder agency IT acquisition outcomes will be reduced and, eventually, eliminated, problems will always arise in any large project. The administration should continue to promote the use of the PortfolioStat process as a way to avoid unpleasant surprises and take on problems before they get out of hand. And along with Congress, the administration should need to increase the standing and visibility of the program management role. This is a key role that needs to have its own job series, standards of performance, and career ladder potential.

7. ON JUNE 10TH THE WALL STREET JOURNAL RAN AN ARTICLE ABOUT THE PROMINENT ROLE THAT CIOs PLAY IN DATA GOVERNANCE AT PRIVATE SECTOR COMPANIES. WHAT DO YOU SEE AS THE APPROPRIATE ROLE OF AN AGENCY CIO IN "DATA GOVERNANCE" AND IN IMPLEMENTING THE ADMINISTRATION'S OPEN-DATA POLICY? WHAT DO YOU SEE AS THE CHALLENGES IN COMPLYING WITH THE OPEN-DATA POLICY?

The Departmental CIO needs to have responsibility for overall data governance policy and oversight. A focus on data openness is the best way for agencies to stay plugged into their mission, promote transparency, and provide enhanced benefits to the nation (acknowledging the need for protection of personal information and privacy).

The biggest challenge right now lies in bureaucratic resistance to open-data and "data governance". While data governance is probably best accomplished at the sub-agency level, many senior officials are highly protective of data and hesitate to share across the agency or with the public. As of now, the CIO does not have enough enforcement authority to push senior executives to share their data, or to punish those who are not doing their job.

**Post-Hearing Questions for the Record
Submitted to Steven L. VanRoekel
From Senator Tom Coburn**

**“Reducing Duplication and Improving Outcomes in Federal Information Technology”
June 11, 2013**

1. In August 2011, OMB issued guidance to clarify the role of agency CIOs, and specifically directed CIOs to reduce duplication. However, subsequent OMB guidance issued in March 2012 says agency Chief Operating Officers (COOs) are directly responsible for the implementation and outcomes of Portfolio Stat. Since Portfolio Stat allows agencies to evaluate the maturity of their IT portfolios in order to, among other things, reduce duplication, why did OMB task somebody other than CIOs directly with this responsibility?

The PortfolioStat 2013 memorandum¹ describes noteworthy management practices agencies should strive to emulate. One of the best practices cited is ‘Strengthening IT Portfolio Governance.’ The memorandum states, “[s]trong oversight of spending through the use of effective investment review boards (IRBs) that include Chief Operating Officers (COOs), CIOs, Chief Human Capital Officers (CHCOs), Chief Financial Officers (CFOs), Chief Acquisition Officers (CAOs), Performance Improvement Officers (PIOs), program officials, and other key executive decision makers is essential for efficient and effective IT portfolio management.” The Government’s IT investments make up a relatively modest portion of total Government spending, but have far-reaching impacts and touch upon almost every aspect of Government activity. The Office of Management and Budget (OMB) believes this level of executive sponsorship -- at the Deputy Secretary level -- is a direct reflection of our belief that IT is a strategic asset that can dramatically improve productivity and the way agencies execute their mission. The convening function possessed by agency Deputy Secretaries is to bring together senior management across an organization in an integrated and holistic fashion.

2. There are approximately 240 CIOs at the 24 major agencies. At the Department of Transportation, for example, the chief CIO must contend with no less than 35 sub-organization CIOs. Does the volume of CIOs obscure lines of authority and makes it difficult to hold individuals accountable for waste or security weaknesses?

Proper governance structures, policies and procedures and management, including the CIO having visibility and ability to influence their agency’s entire IT portfolio, are critical to holding individuals accountable.

According to Department of Transportation, as of August 1, 2013, the Department has 13 CIOs.

¹ <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-09.pdf>.

3. In recent years, there have been reports of CIOs leaving their agencies seemingly under conflict. Is legislative reform needed to strengthen the role of the CIO?

OMB believes that current statutes afford agency CIOs the proper authorities to ensure IT is used as a strategic asset to improve agency service delivery. However, over time, these authorities have not been implemented in a consistent and effective manner across agencies. To address, OMB has established policy, including OMB-M-11-29, which strengthens the role of the CIO by stating that, "Agency CIOs must be positioned with these responsibilities and authorities to improve the operating efficiency of their agencies. In addition to their statutory responsibilities through the Clinger-Cohen Act and related laws...agency CIOs shall have a lead role in governance, commodity IT, cybersecurity, and program management." OMB does not believe legislative reform is an effective tool to change culture or poor leadership.

4. OMB has estimated that TechStats will result in savings totaling \$4.4 billion over the projects lifecycle. The most recent IEEUIT report issued in May 2013 only lists five TechStat sessions totaling \$10.5 million in cost avoidance and \$53 million in cost savings. To date, how many TechStat sessions have been conducted?

OMB has conducted 79 TechStats. Agencies have reported conducting more than 450 TechStats.

5. If more TechStat sessions have occurred than are listed in the IEEUIT reports, why are more projects not detailed?

The IEEUIT report only details TechStat sessions that have yielded savings. Not all TechStat sessions, whether conducted by OMB or agencies, result in quantifiable savings.

6. Will OMB pledge to provide the IEEUIT reports directly to the authorizing committee?

The Consolidated and Further Continuing Appropriations Act, 2013 (P.L. 113-06) requires OMB to submit quarterly reports to the House and Senate Committees on Appropriations which identify the savings achieved by OMB's government-wide IT reform efforts. We request that you work directly with these Committees to obtain copies of the reports.

7. If savings are being realized, why aren't they listed in IEEUIT? If the results of Tech Stat sessions are listed elsewhere, why are they not being communicated on the document that is transmitted to Congress each quarter?

All Federal IT reform savings reported to OMB since the inception of the IEEUIT fund on

December 23, 2011, are reported to Congressional Appropriations Committees in the quarterly *IEEUIT Report*.

8. If the actual number of data centers is far higher than 3,000 as revealed by testimony of the GAO during the hearing, do you still believe the goal of closing 1,253 by 2015 is sufficient, or should be increased? Isn't there a lot more duplication and potential savings than your current goals suggest?

As part of PortfolioStat in 2013, the Federal Data Center Consolidation Initiative (FDCCI) was integrated into PortfolioStat. As these efforts converge, agencies will continue to focus on optimizing those data centers that are pivotal to delivering taxpayer services, while closing duplicative and inefficient data centers. To do so, under PortfolioStat, agencies are currently designating their data center population in to two categories, core and non-core data centers. The core data centers will be optimized across a suite of total cost of ownership metrics while the Government will consolidate 40 percent of the non-core population. Should the number of the non-core data centers change, then the 40 percent target will change to parallel that. At this point, OMB believes the 40 percent policy goal is appropriate, when coupled with the shift to optimize the Government's core data centers.

9. Given the fluctuations in the number of data centers identified by Federal agencies, if agencies aren't certain of their inventory, how can we have any reasonable assurances that agencies' complete inventory is secure?

A key tenet of the FDCCI since its origination was an iterative, continual process by which FDCCI participating agencies, known as the FDCCI Task Force, would annually update their asset inventories on June 30th of each fiscal year. The increase in number of data centers reported by agencies resulted from the 2012 change in the definition of a data center, from above 500 square feet and meeting Uptime tiering criteria to data centers of all sizes and types. The integration of the FDCCI and PortfolioStat enables the Federal Government to have a more comprehensive analysis of resources used, efficiencies realized, and also helps to better protect Government assets.

Since the FDCCI began in 2010, OMB has expanded the definition of a data center to include data centers of all types and sizes. As a result, we saw an increase in the number of data centers agencies reported. The higher number of data centers cited by GAO during the hearing on June 11th reflects this change in methodology and improved reporting by agencies, not a large increase in the actual number of data centers. Under PortfolioStat, agencies are categorizing their data center populations into core and non-core data centers and examining how optimizing these assets will improve agency mission service delivery. Through this work, the Administration

made significant progress in improving the efficiency and effectiveness of data centers and will continue to work to make progress in this area in the months and years ahead.

10. OMB's May 2013 PortfolioStat memorandum established guidelines for categorizing data centers as either "core" or "non-core," and stated the 40 percent closure goal will now apply only to non-core data centers. Does this mean it is no longer a goal of OMB to close 1,253 of the 3,133 data centers you've identified?

The current policy goal for non-core data centers is to close 40 percent of those data centers identified and reported by agencies. As agencies finalize these figures through PortfolioStat, the Government will establish a new target for non-core data centers. OMB expects that the goal for closing non-core data centers will increase. Additionally, as the number of non-core data centers increases, the Government's target will increase/decrease in a commensurate fashion. The use of a percentage rather than a hard number allows the goal to increase as agencies identify and report more data centers.

11. In July 2010, when OMB defined "data center" as any room used for the purpose of processing or storing data that is larger than 500 square feet, it identified 2,094 data centers. After expanding the definition to include facilities of any size, OMB identified 3,133 data centers. Of the 420 data centers reported closed in December 2012, do you know how many are larger data centers—as opposed to 'server closets'? Given the relevance of the size of closed data centers to cost savings, why is this information not published on data.gov as recommended by GAO?

As of May 2013, agencies reported 484 data centers closed. The square footage of these is:

# of Data Centers	Square Footage
31	Other
54	< 100
131	< 250
89	< 500
155	< 5,000
24	≥ 5,000

Other data centers include those where square footage has not been reported by the agency or for which square footage is not germane, such as the case with a cloud service provider. OMB is working with the FDCCI Program Management Office (PMO) at GSA, as well as the FDCCI Task Force, to improve data quality and ensure this information is reported on Data.gov by the October 2014.

12. What oversight role will the FDCCI Task Force and GSA, respectively, have over data center consolidation given its integration with PortfolioStat?

OMB's role and responsibilities with respect to the FDCCI fall under the following E-Gov Office activities: (a) lead, coordinate, and oversee development of IT and electronic government related policy; and (b) provide oversight to agencies in the management of the Federal IT portfolio.

The FDCCI PMO, housed in GSA's Office of Citizen Services and Innovative Technologies, works with OMB as an execution partner for the FDCCI. OMB is the lead partner and sets the broader policy direction of the FDCCI. The GSA PMO:

- Supports OMB in the planning, execution, management, and communication of the FDCCI;
- Coordinates communications about the initiative, including receiving responses to data calls and responding to agency questions about procedures and deadlines;
- Develops, manage, and provides training on the data center total cost of ownership model;
- Provides agencies with practical tools, templates and guidance to effectively plan and execute their strategies to optimize and consolidate data centers;
- Collects and disseminates data related to the FDCCI inventories, plans and closure updates; and
- Completes other tasks necessary to support OMB in the planning, execution, management, and communication of the FDCCI.

The Data Center Consolidation Task Force is comprised of the data center consolidation program managers from each agency. It serves as a "community of practice" for agency CIOs and data center program managers to share best practices from this effort and enhance optimization and consolidation effectiveness.

Per the May 2013 GAO report, OMB is establishing a mechanism to ensure that the established responsibilities of designated data center consolidation oversight organizations are fully executed.

13. Please explain why the PortfolioStat savings estimate is smaller than the initial savings goal of the Data Center Consolidation Initiative. If OMB's original goal was to save \$3 billion by the end of 2015 from data center consolidations, why is the overall savings estimate for Portfolio Stat not higher than \$3 billion? How does Congress know what savings are attributable to data centers under Portfolio Stat efforts, and what savings are attributable to other things?

The two savings estimates should be viewed separately; however, they are not mutually exclusive. For example, of the \$2.5 billion in planned PortfolioStat savings between FYs 2013 – 2015 identified by agencies, \$750 million of that was for servers and mainframes, which are located in a data center. Some FDCCI savings may come from PortfolioStat and some savings identified in PortfolioStat may come from data center consolidation.

14. During the hearing, you mentioned a process by which agencies are allowed to keep 5 percent of savings that are realized from IT reform efforts, and that OMB retains a portion of savings as well. Please describe this incentive program in greater detail. Was guidance issued by OMB to institute this policy? If so, please provide a copy of this guidance.

OMB provided directions to agencies via the Fiscal Year (FY) 2014 Budget Guidance memorandum M-12-13, which was released on May 18, 2012.² Additional detailed reporting guidance can be found on page 27 of the FY 2014 *Guidance on Exhibits 53 and 300 – Information Technology and E-Government*.³

15. Now that the IT Dashboard is in its fourth year of operation, what are the Dashboard's strengths and weaknesses from OMB's perspective?

Strengths of the IT Dashboard include a wealth of available information on Federal IT investments, an intuitive and flexible user interface which has helped provide improve public insights, and historical trend data. A limitation with the IT Dashboard, and an issue previously discussed, is that it relies on agencies to report accurately and in a timely manner. However, in a number of successive engagements, GAO has reported that data quality has improved over time, resulting in part from improved system validations and oversight activities undertaken by OMB.

16. DOD is responsible for nearly half of Federal IT investments yet has not a single project listed in the red zone in the IT Dashboard. Has OMB ever approached DOD to ask why their ratings do not appear to be accurate or in keeping with the spirit of IT Dashboard?

Agency CIOs are accountable for assigning a rating that is consistent with OMB guidance and reflective of an investment's current status. It is important to note that the CIO rating is not the sole indicator of risk or performance of Federal IT investments, and OMB uses numerous other

² The memo states, "Your agency's 2014 budget submission should also continue to look for ways to spend Federal dollars on IT more efficiently. Unless your agency has received different guidance from OMB, your 2014 budget submission should achieve an agency-wide 10 percent in IT spending, compared to the average spending on IT from FY 2010 through 2012, and include an explanation of how, at the investment and account level, you would achieve this reduction. Your budget submission may also propose where you would reinvest the savings from identified cuts in innovative IT solutions that would produce a favorable return on investment within 18 months or demonstrably improve citizen services or administrative efficiencies. OMB will provide additional guidance on how agencies should reflect this information in their budget submissions."

³ http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy14_guidance_on_exhibits_53_and_300.pdf.

metrics and data points, from the IT Dashboard and other sources, to gain an overall picture of investment performance.

17. Under the IT Dashboard, projects categorized as “minor” projects constitute roughly half of Federal IT investments, roughly \$35 billion. Does the Dashboard contain sufficient information on “minor” projects? Does OMB have plans to expand the amount of information available on “minor” projects?

OMB created the “major” investment distinction in recognition of the fact that some investments are larger and more complex than others and it makes sense to focus more deeply on those investments in our oversight role. OMB believes that there is sufficient information available on “non-major” investments, and under current authorities may request additional detail for those non-majors that may require greater scrutiny. While there are no immediate plans to significantly expand the amount of information available for non-majors, every year OMB re-evaluates data collected in the Exhibit 53 and if appropriate, makes adjustments to data reported. For example, in recent years, OMB has begun collecting additional information for each investment such as contact information and cloud computing adoption.

18. Federal agencies have been found by the GAO to be inconsistently reporting Federal IT investments. For example, some agencies were found to count research and development (R&D) systems as “IT investments” while others do not. While OMB has issued guidance to help agencies report their IT investments, GAO stated in testimony before the House in January 2013 that “this guidance did not ensure complete reporting or facilitate the identification of duplicative investments.”⁴ What is OMB doing to improve the consistency and accuracy of reporting by agencies?

OMB acknowledges that in select cases, agencies have opted not to report certain types of investments that would appear to fit the definition of “IT investments.” OMB believes that the definition provided is sufficient to capture all Federal IT spending, and that any non-reporting is non-compliant with policy. OMB, on a continual basis, through TechStats, PortfolioStats, the budget development process and other means, works with agencies to improve the consistency and accuracy of agency reported data.

19. In OMB’s 2012 annual review of agencies’ compliance with FISMA, OMB rates the Social Security Administration at 98 percent compliance – a stand-out agency, the second-highest score in Federal Government. But the SSA Inspector General found the agency’s IT security was riddled with serious problems – “great enough to constitute a significant deficiency under FISMA,” and urged SSA to take “immediate action.” How can the IG find SSA’s systems so dangerously vulnerable, and OMB find them one of the best in government?

⁴ See GAO-13-297T and GAO-11-826.

The Federal Information Security Management Act (FISMA) requires the Director of OMB to summarize the results of the evaluations conducted under section 3543(a)(8) in its annual report to Congress. OMB does not assign the compliance scores. Under FISMA, agency inspectors general (or an independent auditor) conduct independent annual evaluations. Section V of OMB's FY 2012 FISMA report to Congress is a summary of the Inspector General (IG) findings and includes scores provided by the IG community.

The Social Security Administration's (SSA) overall performance and compliance on security measures identified in the FISMA report was determined by its IG, based on independent assessments conducted by third-party auditors. While overall performance and compliance in these areas remains high, the IG also identified specific weaknesses with the agency's management and oversight of access controls. We understand that SSA has developed and already begun to implement specific plans of action to eliminate the weaknesses identified by the IG.

20. How much money has this administration spent on securing Federal civilian agency networks over the last five years?

OMB reports this information in the annual *FISMA Report*, delivered to Congress each March 1. These figures are:

- FY 2009 -- \$6.8 billion⁵
- FY 2010 -- \$12 billion⁶
- FY 2011 -- \$13.3 billion⁷
- FY 2012 -- \$14.6 billion⁸
- FY 2013 -- Will be included in the FISMA Report submitted to Congress in March 2014.

The large increase between FY 2009 and 2010 is a function of improved reporting and data quality, rather than a nearly 100 percent increase in spending, as FY2009 was the first time OMB worked with agencies to collect this information.

21. Who at OMB is responsible for ensuring the administration's cybersecurity efforts improve? Who should be praised for progress, and held accountable for lapses?

Given the importance of cybersecurity, multiple offices inside OMB, including the Director, Deputy Director and Deputy Director for Management, as well as multiple resource management offices, the Electronic Government and Information Technology Office and the Office of Federal Procurement Policy, ensure the Administration's cybersecurity efforts improve. Furthermore,

⁵ http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY09_FISMA.pdf.

⁶ http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY10_FISMA.pdf.

⁷ http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy11_fisma.pdf

⁸ http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma_0.pdf.

every agency in the U.S. Government has a role to play in cybersecurity whether in simply securing its own network or more wide ranging responsibilities. Because of the diverse and nature of authorities and responsibilities, cybersecurity truly requires a whole of Government approach. Consistent with its statutory policy, budget and oversight roles, OMB also works closely with agency leadership to ensure high visibility is given to cybersecurity and to improving the Government's cybersecurity capabilities.

###

**Post-Hearing Questions for the Record
Submitted to Steven L. VanRoekel
From Senator Claire McCaskill**

**“Reducing Duplication and Improving Outcomes in Federal Information Technology”
June 11, 2013**

1. In your opinion, what can be done to ensure that the Department of Defense more accurately reports its troubled investments in the IT Dashboard?

OMB believes that the criteria provided for the Evaluation by agency CIO are sufficiently clear and broad to yield accurate and meaningful responses from all agencies. On an ongoing basis, OMB stresses with all agencies the importance of timely reporting and the quality of data reported on the IT Dashboard, and follows up with agencies in specific cases where data appears to be inaccurate. Additionally, agencies have access to a data quality report on their IT Dashboard reporting, which provides a snapshot of areas which the agency should address and correct in future reporting cycles. To that end, improving transparency is an ongoing, continual effort. Oversight from OMB, in addition to Congress and GAO, assists with delivering accurate and timely information to the public.

2. All of the witnesses at the hearing agreed that the authorities of department Chief Information Officers required strengthening and clarification over commodity IT investments, at the very least. However, none spoke of the potential coordination across agencies. What role, if any, should the General Services Administration play in commodity IT purchases to maximize the purchasing power of the Federal Government and coordinating efforts across departments in commodity IT purchases?

In December 2012, OMB released M-13-02, *Improving Acquisition through Strategic Sourcing*.⁹ This memorandum created the Strategic Sourcing Leadership Council (SSLC), on which GSA is a key member. It called on the SSLC to develop five strategic sourcing opportunities. Given its unique mission and vantage point, GSA was also called upon to create five additional opportunities in FYs 2013 and FY 2014. Thus, in addition to GSA working collaboratively with all agencies to develop a set of strategic sourcing opportunities, GSA will develop at least 10 on its own for agencies to leverage.

Additionally, the Federal Strategic Sourcing Initiative (FSSI) Wireless is a great example of strategic sourcing in action. Under this program, GSA established blanket purchase agreements (BPAs) with four large wireless providers, AT&T, Sprint, Verizon and T-Mobile. These BPAs, known colloquially, as the Federal Government’s ‘wireless plan,’ allow agencies to aggregate

⁹ http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-02_0.pdf.

their acquisitions in such a way that they are able to achieve unprecedented levels of scale which impacts pricing. Agencies are also creating pools of capacity which helps to avoid overages and translates into future savings. Finally, the administrative burden has been significantly reduced, which frees up resources to focus on the mission. This is the area in which GSA expertise can uniquely be brought to bear. Wireless services are well-defined commodity areas with a limited number of offerors. Other great opportunities are represented by large volume desktop publishing software and mapping software.

Additionally M-13-02 called on GSA to provide additional transparency for prices paid for common goods and services. OMB is working with GSA to establish a core capability that can collect and support the analysis of prices paid for a large number of different commodities. GSA should be in a position in which they can help support contracting officers at agencies with data to validate independent government cost estimates as well as the fair and reasonable component of evaluating offers.

3. Strategic sourcing for IT commodities provides an opportunity to leverage the purchasing power of the entire Federal Government for resources that are needed at every agency. Yet during the hearing, only Mr. Szykman made any mention of strategic sourcing. In your opinion, what legislative or oversight actions should be taken to increase the implementation of strategic sourcing of IT commodities and services?

Over the last several years, there have been concerted efforts by the Administration to better leverage the purchasing power of the entire Federal Government for commodities common to every agency. Agencies assembled to specifically identify opportunities for strategic sourcing, and commodity IT represented a significant portion of that vision. Commodity teams were established to consider new opportunities to leverage spending and to deliver better value to the taxpayer.

As reflected in GAO Report 13-417, *Leading Commercial Practices Can Help Federal Agencies Increase Savings When Acquiring Services*, differing market conditions may require unique strategies for each commodity area. OMB has found that the Federal efforts are consistent with these commercial practices. In some instances, when there are a large number of offerors, agencies are working to focus acquisition actions on a limited number of contracts to leverage the scale of the Government's investment. In other examples, in which there are few offerors, agencies are working to refine a standard set of requirements.

To better ensure that agencies do not overpay for services or capabilities, OMB makes strategic sourcing a part of agency discussions in PortfolioStat, objective, data-driven sessions which identify common areas of spending with the intent of reducing duplication and lowering

costs.¹⁰¹¹ One of the key areas for engagement with agencies is in commodity IT. OMB uses information from agency IRM Strategic Plans, Enterprise Roadmaps and the quarterly Integrated Data Collection to identify specific opportunities for improvement with each agency. During PortfolioStat sessions, discussions focus on these and other issues and work with the agency to establish performance goals to better manage commodity IT.

###

¹⁰ http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-10_1.pdf.

¹¹ <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-09.pdf>.

**Post-Hearing Questions for the Record
Submitted to Steven L. VanRoekel
From Senator John McCain**

**“Reducing Duplication and Improving Outcomes in Federal Information Technology”
June 11, 2013**

1. The Clinger-Cohen Act of 1996 requires the Director of OMB to report to Congress on “the net program performance benefits achieved as a result of major capital investments made by executive agencies for information systems and how the benefits relate to the accomplishment of the goals of the executive agencies.” But, on January 22, 2013, the Government Accountability Office’s Director of Information Technology Management Issues, David Powner, testified to the House Committee on Oversight and Government Reform on the OMB’s failure to meet its reporting requirements as required by Clinger-Cohen.

- Why was the reporting of risky IT investments discontinued in 2010?

Please see answer to question 3.

2. In fiscal year 2013, the Federal Government is expected to invest about \$74 billion on IT and \$82 billion in 2014. In today’s challenging fiscal climate, the Government cannot afford to have taxpayer dollars wasted or otherwise abused in connection with these investments. OMB, in particular, must not allow high-risk programs, such as the Air Force’s Expeditionary Combat Support System (ECSS), to squander increasingly scarce IT funding.

Since 2005, ECSS spent over \$1 billion in taxpayer funding. But, ultimately, the Department of Defense cancelled the program in December 2012 with little to show for it. While ECSS’s cost overrun is troubling, I am also concerned that other programs may be funded today while performing at similarly critical risk levels.

- Since 2005, what was the risk level associated with the ECSS program?
- At any time, did OMB meet with the Air Force to discuss ECSS’s risk level?

Please see answer to question 3.

3. How will OMB reinstate its legal obligation for the reporting of risky IT investments and assure transparency of these reports for the agencies and taxpayers funding them?

The OMB is committed to fulfilling its responsibilities established by the Clinger-Cohen Act of 1996 and the E-Government Act of 2002. Initiatives such as the IT Dashboard, TechStat

accountability sessions (TechStat) and PortfolioStat are strengthening OMB's visibility into, and oversight of, agencies' IT investments.

In April 2009, then Federal Chief Information Officer (CIO) Vivek Kundra, testified before the Senate Homeland Security and Government Affairs Committee (HSGAC) that OMB would be undertaking a major shift in our approach to overseeing IT investments. Specifically, Mr. Kundra testified that OMB would be moving away from the static lagging indicators represented by our management watch list and high risk list, and replace these lists within two months with more dynamic leading indicators of investment risk and performance.

Accordingly, on June 30, 2009, OMB launched the IT Dashboard, a public website bringing unprecedented transparency and frequency to information on billions of dollars in Federal IT investments. The IT Dashboard requires a host of new agency inputs and serves as a centralized portal to share detailed information for all major technology investments. The platform provides a more streamlined and standardized approach to the previous policy, which required each agency to post these reports on their websites.

Through the IT Dashboard, Federal agencies and the public have the ability to view details of Federal information technology (IT) investments online and to track their progress over time. The IT Dashboard displays data received from agency Exhibit 53 and Exhibit 300 reports, including general information on over 7,000 Federal IT investments and detailed data for over 700 of those investments that agencies classify as "major." Agency CIOs are responsible for evaluating and updating select data on a regular basis, which is accomplished through interfaces provided by the IT Dashboard.

The IT Dashboard shines light onto the performance and spending of IT investments across the Federal Government. If a project is over budget or behind schedule, anyone can discern by how much money and time, and will also be able to identify the person responsible for managing the project. The IT Dashboard gives the public access to the same tools and analysis that the Government uses to oversee the performance of the Federal IT investments. The transparency and analysis features of the IT Dashboard make it harder for underperforming projects to go unnoticed, and easier for the Government to focus action on the projects where it's needed most.

In order to better align its initiatives with the principles established by the Clinger-Cohen and E-Government Acts, is the requirement for agency CIOs to provide risk assessments (referred to as "Evaluation by Agency CIO" in [Circular A-11, Exhibit 300]) for all major investments, which are then shared publicly on the IT Dashboard. Requiring CIOs to rate investment risk and placing their major investment evaluations on the IT Dashboard were deliberate moves to empower and drive accountability to agency CIOs, and a move away from OMB's prior practice of scoring agencies on their compliance with reporting requirements. CIOs are required to use

the following criteria¹² to establish their rating, and should update the rating as soon as new information becomes available which impacts the assessment of a given investment:

Evaluation Factor	Supporting Examples
Risk Management	<ul style="list-style-type: none"> • Risk Management strategy exists • Risks are well understood by senior leadership • Risk log is current and complete • Risks are clearly prioritized • Mitigation plans are in place to address risks
Requirements Management	<ul style="list-style-type: none"> • Investment objectives are clear and scope is controlled • Requirements are complete, clear and validated • Appropriate stakeholders are involved in requirements definition
Contractor Oversight	<ul style="list-style-type: none"> • Acquisition strategy is defined and managed via an Integrated program team • Agency receives key reports, such as earned value reports, current status, and risk logs • Agency is providing appropriate management of contractors such that the Government is monitoring, controlling, and mitigating the impact of any adverse contract performance
Historical Performance	<ul style="list-style-type: none"> • No significant deviations from planned cost and schedule • Lessons learned and best practices are incorporated and adopted
Human Capital	<ul style="list-style-type: none"> • Qualified management and execution team for the IT investments and/or contracts supporting the investment • Low turnover rate
Other	<ul style="list-style-type: none"> • Other factors that the CIO deems important to forecasting future success

Evaluation ratings are based on a five-point risk scale, as follows:

Evaluation (By Agency CIO)	Color
5-Low Risk	Green
4-Moderately Low Risk	Green

¹² These criteria are available at ITDashboard.gov/faq.

3-Medium Risk	Yellow
2-Moderately High Risk	Red
1-High Risk	Red

Overall, OMB believes agencies are providing fair and accurate assessments of these investments. However, there are cases where other information available on certain investments is inconsistent with the agency rating. Where appropriate, OMB contacts the agency directly to address those inconsistencies. It is important to note that there is no one single indicator for investment risk or performance, and that the evaluation by an agency CIO is one of several key data points illustrated to provide OMB with a multi-dimensional assessment of investment risk and performance. Trend data on investment risk, previously available on the IT Dashboard, is now also available in the Fiscal Year (FY) 2014 President's Budget, consistent with GAO's recent recommendation cited in your letter.

In March 2012, OMB established PortfolioStat, engaging directly with agency leadership to assess the effectiveness of current IT management practices and address opportunities to improve management of IT resources. These sessions led agencies to take certain actions to curb wasteful spending. Through PortfolioStat, OMB has candid discussions with agency leadership, reinforcing many of the basic principles laid out in Clinger-Cohen and E-Government Acts, such as capital planning and investment control, IT governance, reinforcement of CIO authorities and responsibilities, information security, and many others.

As a result of PortfolioStat, agencies identified \$2.5 billion in commodity IT expenditures, such as combining multiple email systems and eliminating duplicative mobile or desktop contracts, to eliminate or consolidate between FYs 2013 – 2015. OMB reported some of these savings in the last report on the Integrated Effective and Efficient Uses of Information Technology (IEEUIT), submitted on a quarterly basis to the Senate and House Appropriations Committees. The most recent report IEEUIT report from July 24, 2013 includes \$1.37 billion in savings from the last five fiscal quarters.

Shortly after the launch of the IT Dashboard, OMB took advantage of the more frequent collections of investment performance data to help identify and confront some of the highest risk investments in Government through TechStat accountability sessions. These investments included the Department of Defense's (DoD's) Expeditionary Combat Support System (ECSS), which was one of a handful of reviewed investments that went through multiple TechStat sessions. The results from the ECSS TechStat sessions were itemized in a corrective action plan agreed to by the agency to address what were then acknowledged deficiencies. The corrective actions ranged from recommended resource reductions to specific budget actions such as apportionments and administrative controls, consistent with authorities laid out in the Clinger-

Cohen and E-Government Acts. Additionally, your letter also inquired about the Marine Corps' Global Combat Support System (GCSS-MC). The OMB did not conduct a TechStat related to GCSS-MC; we would refer questions regarding that investment to the Marine Corps.

Due to the scope and size of DoD's ECSS investment, the largest enterprise resource planning (ERP) implementation ever attempted, it was always considered high-risk and closely watched by OMB. Early in the life of the program, in 2005, the Air Force began experiencing delays in the implementation of the system, pushing development and initial operating capability out by years. One such delay beyond DoD's direct control was a contract protest lasting from 2005 through 2007. In addition, the DoD and the Air Force, and a subsequent GAO report 11-53 (October 2010), indicated that projected lifecycle costs appeared to be growing and had never been baselined. At the launch of the IT Dashboard, DoD identified the investment as a "Medium Risk" or 3 out of 5.

In early 2010, just months into the development of ECSS Release 1, OMB engaged directly with officials representing the Department of the Air Force and DoD to highlight its concerns about the effectiveness of the ECSS implementation, including the management of risk. The discussions culminated in two TechStat sessions with OMB in addition to several DOD level reviews. After evaluation of the program through these review sessions, DoD made the decision to terminate the program in December 2012. OMB believes that its continuous direct engagement - through the TechStat process - played a critical role in identifying implementation weaknesses and in ultimately terminating the program.

4. As the Senate debates cybersecurity, once of the central issues will be how to best protect government civilian networks, particularly those that fall under the preview of the Federal Information Security Management Act (FISMA).
 - In your view, what tools does your office rely on to ensure department and agency compliance with the FISMA?

OMB uses a number of mechanisms. For example, we rely on information submitted by agencies as part of the FISMA reporting and annual budget processes. OMB also conducts oversight reviews (e.g. PortfolioStat and CyberStat accountability sessions) in which we discuss agencies' cybersecurity status and plans, and we meet with agencies as part of the budget planning process to review progress in particular areas. Lastly, the Administration works with agencies to update -- on a quarterly basis -- the cybersecurity Cross Agency Priority (CAP) Goal, developed under the GPRA Modernization Act of 2010 (the progress of which is displayed on Performance.gov).

- In your view, are there steps that can be taken to improve the effectiveness of the FISMA and ultimately, compliance?

A key step to improving effectiveness of Federal information security includes shifting to continuous monitoring to protect Federal information and information systems. Continuous monitoring, one part of the National Institute of Standards and Technology's (NIST) 3-tiered Risk Management Framework approach, is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

In addition to strengthening the underlying information technology infrastructure through the application of state-of-the-art architectural and engineering solutions, the implementation of continuous monitoring is essential to keep pace with the dynamic cybersecurity threat landscape and improve the effectiveness of safeguards and countermeasures employed to defend Federal information and information systems.

In support of continuous monitoring, the General Services Administration is working with the Department of Homeland Security to establish a Government-wide acquisition contract (GWAC) which agencies can leverage to deploy and implement continuous monitoring capabilities. The GWAC will provide a consistent, Government-wide set of continuous monitoring solutions to enhance the Government's ability to identify and respond to the risk of emerging cyber threats, and capitalizes on strategic sourcing to minimize the costs associated with implementing continuous monitoring.

- In light of recent events, what is your office doing to ensure that the FISMA, and applicable regulations, are in place to ensure government contractors are complying with the FISMA requirements?

The requirements in existing law apply to information regardless of whether that information is hosted on Federal systems, or systems hosted by non-Federal entities on behalf of the Federal Government. Additionally, OMB policy and NIST standards and guidelines apply regardless of where the information is hosted and agencies must report status as part of the FISMA reporting process. The Federal Acquisition Regulation, for example, section 39, includes requirements for contractors to safeguard Federal information. As OMB and DHS work to update the annual FISMA metrics, we will determine if additional information needs to be collected to better gauge agency compliance with FISMA requirements.

- Does the FISMA need to be amended to better deal with ensuring government contractor security? If so, please explain.

FISMA requires agencies to identify and provide information security protections for information collected or maintained by or on behalf of an agency, and information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. Essentially, the security requirements are the same regardless of where information is hosted by a Federal agency or an entity on behalf of the Federal Government.

###

**Post-Hearing Questions for the Record
Submitted to Mr. Simon Szykman
From Senator Tom Coburn**

**“Reducing Duplication and Improving Outcomes in Federal Information Technology”
June 11, 2013**

1. *According to agency data, Commerce has closed 30 data centers as of December 2012, yet OMB has not reported any cost-savings for HHS in its quarterly IEEUIT report submitted to Congress. Why is this?*

A: Commerce has been documenting savings and cost avoidance associated with our data center consolidation activities. These savings come from a combination of lower facility costs and reduced operations and maintenance costs. However, a comprehensive accounting of all savings is difficult for a variety of reasons, including difficulties in establishing baselines against which to document savings. For example, within the Herbert C. Hoover headquarters building, several bureau data centers were consolidated into a single facility over the past couple of years. However, those previously existing data centers were very small facilities that were not individually instrumented to track power consumption (which is paid centrally for the entire building), so we are not able to accurately calculate power savings associated with the consolidation. Additionally, unlike the closure of a leased facility where savings associated with space costs are easily determined, in the case of these small facilities in the Commerce headquarters building, the rooms were simply repurposed by bureaus for other uses. Thus, although the new facility operates more efficiently than the proliferation of smaller ones that existed previously, the benefits associated with the space consolidation are only indirect (bureaus having space to repurpose) rather than directly linkable to cost savings.

Nevertheless, Commerce has been working where possible to identify tangible savings in the form of both hard savings and cost avoidance associated with some of our data center activities. Although these savings assessment efforts are not comprehensive (as described above), we have documented \$100K in savings and \$16.2M in cost avoidance in FY 2012, \$8.5M in savings and \$12.3M in cost avoidance in FY 2013, and are projecting \$8.6M in savings and \$19.2M in cost avoidance in FY 2014.

2. *As CIO, do you believe you have a comprehensive count of data centers under the Department of Commerce's control? If not, please explain why not?*

A: I believe that Commerce has been significantly improving its inventory of data centers over the past couple of years and that the current inventory captures the Department's major data center facilities. In March 2012, the Office of Management and Budget expanded the definition of a data center to include data centers of all types and sizes. Since then, Commerce has been diligently working to ensure the contents of its data center inventory are complete and verifiable. At this point, Commerce's inventory has not been fully validated as complete. While the recent increase in data center numbers at Commerce could at first

glance be a source of concern, the increase is not due to construction or operation of more data centers but rather a more accurate accounting of the facilities that were already in place. Thus the increase is an indicator that we are doing a better job at inventorying our facilities than we previously had done in the past.

3. *As CIO, are you able to verify the data centers that components report to you? If so, please describe this verification process.*

A: Due to the fragmented nature of information technology (IT) investments throughout the Department, most of which are based on bureau-specific needs, budgets, and governance structures, the Department CIO currently has a limited role in observing operational facilities managed by Commerce bureaus. As such, the CIO maintains no direct visibility or management control over bureau data centers in this role. The Department OCIO is working to drive data center consolidation within Commerce. The Department's inventory, however, has been developed via reports from bureaus on their investments and, because management control resides at the bureau level, at this time, the Department CIO does not independently verify the reports.

4. *If you do not have a comprehensive count of data centers, how can you assure the security of these centers?*

A: Under the Federal Information Security Management Act (FISMA), every information system controlled, managed, or operated, by or on behalf of Commerce, is required to implement security controls and conduct ongoing risk management according to a comprehensive risk management framework established by the National Institute of Standards and Technology (NIST). While I recognize that as Commerce CIO I have some responsibility for the security of all Commerce systems, the direct responsibility and accountability for management of Federal information systems lies at the level of individuals and organizations that own those systems.

Specifically, under FISMA and according to NIST guidance, each Federal information system has an Information System Security Officer who is responsible for ongoing management of the security of that system, as well as a System Owner (who is responsible for development and management of a system, including its system security plan), and an Authorizing Official (who is responsible ensuring that a system operates at an acceptable level of risk, accepting risk, allocating resources needed to ensure security, etc.).

Commerce policy establishes baseline security requirements for all Commerce systems, and helps to ensure that they are managed appropriately by requiring testing of security controls according to various schedules, ongoing monitoring of security controls, and periodic reauthorization to provide a valid authority to operate (from a security perspective) for those systems. Commerce uses a central data management system for tracking data associated with Commerce's FISMA systems, enabling my office to track the authority-to-operate status of Commerce systems, as well as whether system managers are completing identified risk remediation actions on a timely basis. Because all Commerce information technology (IT) assets are required to be documented as part of a Commerce FISMA system, our cyber

security risk management framework provides my office with visibility into the security of Commerce systems regardless of the organization within which each system resides.

5. *Last September, your Inspector General found that the National Telecommunications and Information Administration had failures in security policy that “jeopardize critical bureau information.” Types of information the IG believed was at risk included law enforcement information, information supporting the protection of elected officials, and proprietary commercial data. Can you explain the deficiencies the IG found, whether they concern you, and whether they still exist?*

A: The deficiencies found were in the completeness of NTIA’s system categorization documentation – based on the Federal Information Processing Standard Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*. Specifically, as you mention, not all of the information collected and maintained by the systems was reflected in the categorization documentation. The IG did not come to the conclusion that the systems were unprotected or vulnerable in any way; the IG was concerned that if NTIA had not properly completed the documentation, required security controls may have been missed.

At the time of the report, I was greatly concerned about the deficiencies. Since that time, I have worked proactively with NTIA’s new Chief Information Officer to understand the issues and to review and understand NTIA’s corrective action plan. NTIA developed a three month schedule for the review and update of categorization documentation for all systems – not just those that had been reviewed by the IG. NTIA opened 26 Plan of Action and Milestones (POA&Ms, i.e., risk remediation actions) to address the issues identified by the IG. As of July 3, 2013, NTIA has completed and closed 20 out of the 26 POA&Ms. Six POA&Ms, all concerning role-specific IT security training, are pending and are on track to be completed by their scheduled completion date of September 30, 2013.

NTIA has completed the documentation of the system categorization from scratch, and has worked hard to identify all of the information types stored in its systems. For example, for one of its systems (the unclassified Spectrum XXI System), the original categorization identified only one information type, whereas in the new documentation NTIA has identified and recorded a total of 46 information types, as well as the security controls required for protection of this expanded inventory of information types.

At this time I am confident that NTIA has worked to remediate the IG findings and, pending the completion of role-based training currently in progress, is on track to fully implement the corrective action plan that was submitted to the IG in response to the audit. It is worth noting that after the update of the categorization documentation, NTIA determined that no additional security controls were needed to protect the information systems.

6. *The IG also noted 44 computer servers on NTIA's network that NTIA did not list on its own inventory, some of which ran on obsolete or unlisted operating systems, creating significant security vulnerabilities. Can you explain how this could be, whether it concerns you, and whether the problem still exists?*

A: At the request of the Associate Administrator for NTIA, I performed an information technology assessment of NTIA in late FY 2011. My findings were that NTIA had critical IT leadership gaps and lacked a defined budget and integrated IT strategy. Service delivery was poor and accountability was limited. NTIA had weak IT processes and documentation in place. I recommended that open IT leadership positions be filled, and that the IT organization be realigned to reinforce its broad IT responsibilities and focus accountability. NTIA implemented a new organization concurrent with hiring a new NTIA Chief Information Officer (NTIA CIO) on April 9, 2012. These events had occurred independently while the FISMA audit was in progress. NTIA also hired a new Deputy Chief Information Officer in July, 2013 and charged him to oversee its Information Assurance program.

I found myself quite concerned based upon my own assessment of NTIA's IT organization and the IG audit when the report was subsequently issued, but the actions taken by NTIA are taking the organization down the right path. The new NTIA CIO and his team have made numerous improvements to the NTIA IT organization in response to recommendations I had made, as well as directly relating to the IG audit findings. NTIA rebaselined all software; deployed a newer operating system (Windows 7) along with other specified/approved software across the organization; completed a physical asset inventory; excessed over 150 pieces of old equipment; and implemented a configuration management database to track hardware and software assets. NTIA also implemented a weekly vulnerability scan review process to identify system vulnerabilities and strengthened its software patching program to remediate them. NTIA has made great strides in improving its IT hardware and software management capabilities and has improved the integrity of its systems.

7. *The IG also found unauthorized files on NTIA computers suggesting that employees were downloading movies and games, possibly in violation of copyright laws. Can you explain how this could be, whether it concerns you, and whether the problem still exists?*

A: This incident was tied to a single computer on the NTIA network. The files in question were owned by the employee and were contained on an unauthorized USB drive connected to the PC. The contents of this drive were in the IG scan results. There was no peer-to-peer software found.

Although isolated to the one individual involved, this was unauthorized behavior that violated DOC policy and was behavior that could have served to threaten or compromise the security of NTIA networks. NTIA developed and published 21 IT policies in 1Q FY13 consistent with Departmental and Federal guidelines that govern IT operations. NTIA's Media Protection Policy, NTIA-IA-12-014, prohibits use of personally owned removable media devices. NTIA now provides users with encrypted devices for transfer of authorized files. In addition, NTIA has severely limited the number of users with elevated privileges to

install software. NTIA also scans for unauthorized software using its configuration management database to identify changes within the NTIA network environment.

8. *This February, the IG reported that the Patent and Trademark Office (USPTO) deployed a wireless network at its Alexandria campus with major security weaknesses and vulnerabilities. In doing so, USPTO "put its critical operational systems at risk," the IG found. Do you agree? How did this happen in your estimation? What steps have you taken to ensure similar failures do not occur in the future?*

A: My office reviewed and concurred with the IG's findings. In this case, it appears that plans associated with deploying wireless technology got out ahead of proper security management processes. The Federal risk management framework established by FISMA allows for the use of technologies in a pilot mode prior to a full production deployment with some security measures not fully implemented. It appears that in the case of the USPTO wireless system deployment, the system moved from a pilot mode to production use prematurely in that it was not fully secured at the time.

This incident did draw attention to the need to ensure compliance with security policies prior to deploying new production wireless networks. To ensure that a similar problem would not be repeated, my own office not only conducted a comprehensive security testing and evaluation process prior to operating a new wireless network that was under development within my operations organization, we even requested that DHS come and do an independent assessment of our wireless infrastructure and were provided with a report that identified a small number of improvements that should be made, but which generally found the network to be well secured.

9. *How much did Commerce spend on IT security in 2012?*

A: Based on the Department's IT OMB Exhibit 53b, the Department spent \$175M on IT security in FY 12, which includes spending on full-time employees, contractors, security tools, testing and training.

10. *Last year, OMB rated Commerce 20 points higher in terms of compliance with FISMA. In other words, you dropped from 81.4 percent compliant in 2011 to 61 percent in 2012. How did your department spend money on IT security, only to drop by 20 points? Who should be held accountable for this lack of performance?*

A: At first glance, the decrease in the FISMA compliance score would naturally lead to concern to external reviewers absent some important context. In this case, however, the apparent drop in performance is the result of prior-years' reporting shortfalls rather than an actual decrease in performance.

As part of the FISMA Report generation process, DHS established a set of 96 attributes. In the case of Commerce, the Office of the Inspector General did not provide a rating for Commerce in all of the categories due to having only assessed a subset of those criteria during their FY 2012 audit cycle. Among the 96 criteria, 14 are attributes/questions that IGs

were asked to score. Of those 14, the Commerce IG responded "N/A" for 8 of them due to a lack of data from not having assessed those criteria in FY 2012. Unfortunately, those questions were improperly scored as zeros in the calculations of the FISMA compliance ratings. In other words, rather than removing those criteria from the scoring due to their not having been assessed by the IG, the compliance calculations were calculated as if Commerce had zero compliance in those areas, which was simply not the case.

If the "N/A" responses had been entirely removed from the calculations rather than being included as zeros, DOC's compliance score for the 14 IG-scored criteria would have been above 80%. The Office of the Inspector General has concurred with the explanation and acknowledges that the incorrect handling of unrated criteria resulted in incorrectly depressing Commerce's score. We would be pleased to facilitate a direct meeting with the IG's staff to discuss the improper calculation if necessary.

Commerce has made significant IT Security improvements in recent years, including eliminating its IT security material weakness in FY 2011. Furthermore, by way of IG recommendation, Commerce implemented an IT Security workforce improvement program, where personnel with significant IT Security roles and responsibilities must be properly trained and obtain a professional security certification (Commerce is the only civilian agency that has implemented this requirement). Commerce has overhauled its cyber security risk management framework, and is in the processes of deploying a Department-wide continuous security monitoring infrastructure. Commerce has also been using a balanced scorecard reporting process to drive improvements in cyber security performance Commerce-wide, resulting in visible performance improvement for metrics such as systems with authority to operate, timely remediation of security risks, and implementation of key security controls. We strongly believe that our performance has been improving in recent years, and that this progress has been recognized in the IG's *Top Management Challenges* reports. Cyber security has been and remains a high priority for Commerce, and we continue to push forward with policies and plans aimed at continuing the trend of improvement.

**Post-Hearing Questions for the Record
Submitted to Frank Baitman
From Senator Tom Coburn**

**“Reducing Duplication and Improving Outcomes in Federal Information Technology”
June 11, 2013**

- **What steps do you believe need to be taken to strengthen the role of agency CIOs, either legislatively or otherwise?**

An Agency CIO needs to be empowered to have an enterprise-level IT perspective. To be effective, the CIO needs to have visibility into all IT spending and early awareness of projects to affect their course. In addition, a strong partnership with business owners is crucial to bridging the gap between the capabilities of technology and the functional needs of program managers.

At HHS, we have worked towards that end by establishing a domain governance structure that supports the business-IT partnership and ensures that decision making is informed by an enterprise-wide view. High-level executive support will ensure the continued success of our efforts.

- **According to agency data, HHS has closed 28 data centers as of December 2012, yet OMB has not reported any cost-savings for HHS in its quarterly IEEUIT report submitted to Congress. Why is this?**

While 28 data centers have been closed, there are ongoing activities involved with the shut-down process to include reallocation of space, decommissioning of utilities, as well as modifications or termination of leasing agreements and services contracts. Savings will be identified and reported as these shut-down-related activities are completed.

- **As CIO, do you believe you have a comprehensive count of data centers under the HHS’ control? If not, please explain why not?**

HHS has an active and ongoing program to identify and categorize our core data centers and to target smaller-footprint facilities for closure and/or consolidation to significantly reduce our overall datacenter footprint. In addition, we are focused on ensuring that our remaining data centers are operated in line with industry standards for efficiency and redundancy.

- **As CIO, are you able to verify the data centers that components report to you? If so, please describe this verification process.**

HHS has a comprehensive reporting process for all the Operating Divisions and the Office of the Secretary. This includes a detailed reporting form that specifies all the relevant attributes of the reported data centers.

- **If you do not have a comprehensive count of data centers, how can you assure the security of these centers?**

HHS has a set of security-related policies and procedures that must be followed before IT assets and systems are allowed to operate on our networks. We also require contractors to adhere to the same requirements in the data centers they own and operate.

- **Last fall, Ernst & Young found HHS does not require suitability background investigations before it grants them access to sensitive Departmental systems and networks. Is that still the case?**

This finding has been addressed by updating both the access policy for these applications as well as the associated waiver process. Adherence to this policy is being monitored on an ongoing basis.

- **What is the status of the auditors' recommendation that HHS begin requiring background checks for such personnel?**

This recommendation is covered in the same updated policy described in the response above.

- **Ernst & Young also found HHS did not have adequate security protecting its system from unauthorized remote access. Did you agree with that finding?**

HHS has put in place the use of Personal Identity Verification (PIV) cards for remote access to systems in addition to the Virtual Private Network (VPN) requirements. These changes have addressed this finding.

- **The auditor also found HHS has no effective process to make sure critical software patches are applied as quickly as possible. Is that still the case?**

OCIO has acquired a patch management tool and is completing the rollout of the technology to address this finding and to ensure consistent application of patches is occurring on IT assets on the network.

- **In a separate review, focused on CMS IT systems, Ernst & Young found that security problems had gone years without being fixed. When combined with new performance pressures on the IT systems, the result could be "unauthorized system access. . . a lack of compliance with policies, and "incomplete and inaccurate processing of transactions." The auditors seem to believe that these security weaknesses could impact CMS' ability to perform its mission. Do you share that concern?**

HHS has addressed this issue directly with CMS through its Risk Management Financial Oversight Board (RMFOB). CMS is providing detailed plans regarding

the resolution of these long standing issues and periodic updates on progress and any delays in their mitigation plans.

- **In its FISMA report released in March, OMB said that during testing your agency caught just 14 percent of intrusions into its networks. That was one of the worst scores in the federal government. Are you concerned by that statistic?**

The report references the outcome of testing for new penetration techniques. We take this testing seriously and work diligently to address each of the unidentified methods post-audit to ensure that we have improved our security posture in response to these techniques. Each year new tests are done, which in turn allows us to further enhance our overall departmental security posture.

- **OMB also found that only 21 percent of HHS computers had an automated capability to detect and block unauthorized software from executing. The government-wide average was 60 percent. Are you concerned by that statistic?**

We currently do not have “White Listing” capabilities at all the Operating Divisions. We are working with the Department of Homeland Security and Continuous Diagnostics and Mitigation (CDM) to acquire tools to implement a solution to mitigate this gap in our toolset.

- **Overall, OMB scored your compliance with FISMA requirements at 50 percent. That was the lowest of any CFO Act agency except for USDA. And it was almost exactly the same as it was the year before. Are you concerned by that?**

We take our FISMA responsibilities seriously, and we are working to improve our information security posture. We continue to seek to improve all of our IT assets and network security challenges on an ongoing basis. Specific examples of our commitment to enhancing our capabilities to deal with these challenges include: 1) creating a Department-level computer security incident response center to coordinate and communicate information security incidents, and 2) establishing a cyber-threat fusion center.

- **How much did your office spend on IT security in 2012? What improvements in performance does HHS have to show for it?**

The HHS Office of the Chief Information Officer invested approximately \$40 million focused on the Trusted Internet Connection Program, the Computer Security Incident Response Center for correlating information security incident response data, and the FISMA program across the Department. HHS has also been a leader in the advancement of the Cloud First strategy issuing the first agency led FedRAMP ATO ensuring that our cloud applications are operating in the most secure environment.

- **Who should be held accountable for this failure of performance?**

HHS has made significant strides on a number of information security fronts to develop an enterprise-level view. These efforts range from governance with the establishment of the CISO Council to operational standardization in our secure enclave architecture. All of these elements have led to a significant increase in our situational awareness and ability to react to threats, but we also recognize that there is work left to do as we continue to improve on all facets of our information security posture.

- **In your testimony you mention that your IT resources are directly tied to appropriations made to programs, and that as a result, program-level IT decisions are governed and reviewed by HHS' operating divisions. As the HHS CIO, what authority do you therefore have over implementation of the IT provisions of the Affordable Care Act? Have you been consulted at all with regard to the federal data hub?**

Within HHS, CMS is leading the implementation of the Affordable Care Act, including the IT provisions. CMS has kept my office informed of the status of their efforts.

- **Given a number of OIG reports on IT vulnerabilities at HHS, are you at all concerned that when the exchanges go live on October 1, patient data or taxpayer dollars will be at risk?**

I am confident that CMS and our partner agencies have taken reasonable steps to mitigate the IT security risks associated with the Marketplaces. Additionally, the Health Insurance Marketplaces do not store patient data, further minimizing risk.



U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

July 18, 2013

The Honorable Thomas R. Carper
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate
Washington, DC 20510

Subject: *Federal Information Technology (IT) Duplication*

This letter is in response to questions you sent us following your committee's June 11, 2013 hearing on reducing duplicative federal IT investments. At the hearing, we discussed results and recommendations from our selected reports that focused on IT duplication.¹ The enclosure provides our responses, which are based on work conducted in support of our previously issued products.

If you have any questions or would like to discuss the responses, please contact me at (202) 512-9286 or PownerD@gao.gov.

Sincerely yours,

A handwritten signature in cursive script that reads "David A. Powner".

David A. Powner
Director, Information Technology
Management Issues

Enclosure

cc: Laura Kilbride, Committee Clerk

¹GAO, *Information Technology: OMB and Agencies Need to Focus Continued Attention on Eliminating Duplicative Investments*, GAO-13-685T (Washington, D.C.: June 11, 2013).

**Post-Hearing Questions for the Record
Submitted to David A. Powner, GAO
From Senator Claire McCaskill**

**“Reducing Duplication and Improving Outcomes in Federal Information Technology”
June 11, 2013**

1. In your opinion, what can be done to ensure that the Department of Defense more accurately reports its troubled investments in the IT Dashboard?

Our October 2012 report on the IT Dashboard noted that opportunities existed to improve the transparency and oversight of investment risk at selected agencies, including the Department of Defense (DOD).² Specifically, we found that, although DOD had reported up to 87 investments on the IT Dashboard between June 2009 and March 2012, none of these investments were rated by the Chief Information Officer (CIO) as being high or moderately high risk. Further, its ratings for certain investments did not appropriately reflect significant cost, schedule, and performance issues reported by GAO and others. Finally, we found that DOD did not apply its own risk management guidance to the ratings, including assessing risks based on a program’s cost and schedule estimates.

To ensure that DOD more accurately reports its troubled investments on the IT Dashboard, we recommended that the department ensure that its CIO ratings reflect available investment performance assessments and its risk management guidance. In addition, we recommended that OMB analyze agency trends reflected in the Dashboard’s CIO ratings, and present the results of this analysis with the President’s annual budget request. Both DOD and OMB concurred with our recommendations. If implemented, such actions could better ensure that DOD is accurately reporting troubled investments on the IT Dashboard.

2. All of the witnesses at the hearing agreed that the authorities of department Chief Information Officers required strengthening and clarification over commodity IT investments, at the very least. However, none spoke of the potential coordination across agencies. What role, if any, should the General Services Administration play in commodity IT purchases to maximize the purchasing power of the Federal government and coordinating efforts across departments in commodity IT purchases?

In September 2012, we reported on the role that the General Services Administration (GSA) had in maximizing the purchasing power of the federal government and coordinating efforts across agencies.³ Specifically, we reported that GSA was responsible for managing a governmentwide strategic sourcing program—known as the Federal Strategic Sourcing Initiative (FSSI)—which was established by OMB in 2005 to identify governmentwide opportunities to strategically source commonly purchased products and services and eliminate duplication of efforts across agencies. Under GSA’s management, we reported that the FSSI program was responsible for assessing opportunities for procuring certain products and services, developing and implementing sourcing strategies to leverage

²GAO, *Information Technology Dashboard: Opportunities Exist to Improve Transparency and Oversight of Investment Risk at Select Agencies*, GAO-13-98 (Washington, D.C.: Oct. 16, 2012).

³GAO, *Strategic Sourcing: Improved and Expanding Use Could Save Billions in Annual Procurement Costs*, GAO-12-919 (Washington, D.C.: Sept. 20, 2012).

governmentwide buying power, and managing the strategic sourcing efforts. We also found that several of the implemented and planned FSSIs were related to IT commodity areas, including telecommunications, commercial off-the-shelf software and services, and wireless rate plans and devices. Finally, we reported that GSA's Program Management Office played an important role in coordinating efforts across agencies by supporting a working group comprised of agency representatives. For example, the working group was responsible for vetting and approving initiatives and sourcing strategies, and establishing the standards, processes, and policies governing FSSI.

We have previously reported that GSA had a role in managing interagency acquisition vehicles, such as governmentwide acquisition contracts (GWAC)—contracts for IT established by one agency for governmentwide use.⁴ Among other things, we found that GWACs were being used to provide a broad range of IT goods and services and resources for agency activities. We also noted that interagency contracts, such as GWACs, had the potential to provide an advantage to the government in buying billions of dollars worth of goods and services, including IT.

3. Strategic sourcing for IT commodities provides an opportunity to leverage the purchasing power of the entire federal government for resources that are needed at every agency. Yet during the hearing, only Mr. Szykman made any mention of strategic sourcing. In your opinion, what legislative or oversight actions should be taken to increase the implementation of strategic sourcing of IT commodities and services?

Our September 2012 report on strategic sourcing identified several challenges that selected agencies faced in implementing strategic sourcing in key spending areas, such as IT commodities and services, and corresponding actions that should be taken to increase its implementation.⁵ Notably, we found that the Departments of Defense, Homeland Security, Energy, and Veterans Affairs leveraged only a fraction of their buying power through strategic sourcing. Although these agencies accounted for 80 percent of the \$537 billion in federal procurement spending in fiscal year 2011, they reported managing about 5 percent or \$25.8 billion through strategic sourcing efforts. Further, we noted that these agencies reported savings of \$1.8 billion—less than one-half of one percent of procurement spending. Other challenges we found at the selected agencies included that most of their strategic sourcing efforts did not address their highest spending areas and most had not fully adopted a strategic sourcing approach. Finally, we reported that a lack of clear guidance on metrics for measuring success had also impacted the management of ongoing governmentwide strategic sourcing efforts, as well as most selected agencies' efforts.

To help address these challenges, we recommended that selected agencies and OMB implement a number of actions. Specifically, to improve agency strategic sourcing efforts, we recommended that selected agencies evaluate the best way to strategically source their highest spending categories of products and services (e.g., by utilizing governmentwide acquisition vehicles, interagency collaboration, agencywide acquisition vehicles); set goals for spending managed through strategic sourcing; and establish metrics, such as utilization rates, to monitor progress toward these goals. In addition, to help ensure that government strategic sourcing efforts further reflect leading practices, we recommended that OMB issue

⁴GAO, *Contracting Strategies: Data and Oversight Problems Hamper Opportunities to Leverage Value of Interagency and Enterprisewide Contracts*, GAO-10-367 (Washington, D.C.: Apr. 29, 2010)

⁵GAO-12-919.

an updated memorandum or other direction to federal agencies that established additional metrics to measure progress toward goals. OMB and selected agencies concurred with our recommendations.

Congressional oversight of these recommendations will increase the likelihood of the implementation of strategic sourcing of IT commodities and services. In addition, legislative action could be useful to ensure agencies establish goals and metrics for their strategic efforts. Legislative action could also assist agencies by requiring the compilation of a price list and catalog containing pricing information by vendor for IT commodities, accessible to executive agencies. This could assist agencies in conducting spend analyses of IT investments by enhancing their ability to conduct price comparisons and make more informed purchasing decisions.

