AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

WASTING INFORMATION TECHNOLOGY DOLLARS: HOW CAN THE FEDERAL GOVERNMENT REFORM ITS IT INVESTMENT STRATEGY

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

JANUARY 22, 2013

Serial No. 113–5

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

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

U.S. GOVERNMENT PRINTING OFFICE

79–790 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 OVERSIGHT AND GOVERNMENT REFORM

DARRELL E. ISSA, California, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
PATRICK T. MCHENRY, North Carolina
JIM JORDAN, Ohio
JASON CHAFFETZ, Utah
TIM WALBERG, Michigan
JAMES LANKFORD, Oklahoma
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
PATRICK MEEHAN, Pennsylvania
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
DOC HASTINGS, Washington
CYNTHIA M. LUMMIS, Wyoming
ROB WOODALL, Georgia
THOMAS MASSIE, Kentucky
DOUG COLLINS, Georgia
MARK MEADOWS, North Carolina
KERRY L. BENTIVOLIO, Michigan
RON DESANTIS, Florida

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
JACKIE SPEIER, California
MATTHEW A. CARTWRIGHT, Pennsylvania
MARK POCAN, Wisconsin
TAMMY DUCKWORTH, Illinois
DANNY K. DAVIS, Illinois
PETER WELCH, Vermont
TONY CARDENAS, California
STEVEN A. HORSFORD, Nevada
MICHELLE LUJAN GRISHAM, New Mexico
VACANCY

LAWRENCE J. BRADY, *Staff Director*
JOHN D. CUADERES, *Deputy Staff Director*
ROBERT BORDEN, *General Counsel*
LINDA A. GOOD, *Chief Clerk*
DAVID RAPALLO, *Minority Staff Director*

CONTENTS

	Page
Hearing held on JANUARY 22, 2013	1

WITNESSES

The Honorable Tom Davis, A former Representative in Congress from the State of Virginia	
Oral Statement	6
Written Statement	9
Mr. Steven Vanroekel, Federal Chief Information Officer, Office of Management and Budget	
Oral Statement	15
Written Statement	17
Mr. David A. Powner, Director, Information Technology Management Issues, General Accountability Office	
Oral Statement	22
Written Statement	24
Mr. Douglas Bourgeois, Vice President and Chief Cloud Executive, U.S. Public Sector Division, VMWARE	
Oral Statement	72
Written Statement	75
Mr. Michael Klayko, Advisor and Former CEO, Brocade Communications Systems, Inc.	
Oral Statement	88
Written Statement	90
Mr. Chris Niehaus, Director, U.S. Office of Civic Innovation, Microsoft Corporation	
Oral Statement	96
Written Statement	98

APPENDIX

The Honorable Elijah Cummings, from the State of Maryland, Opening Statement	120
The Honorable John Mica, from the State of Florida, Opening Statement	122
The Honorable Gerald Connolly, from the State of Virginia, Opening Statement	124
The Honorable Matthew Cartwright, from the State of Pennsylvania, Opening Statement	127
Questions for Steven VanRoekel from Tammy Duckworth, Jackie Speier, and Darrell Issa	130
Response to questions from Jeff Rangel to Jackie Speier	140
Response to questions from Microsoft Innovation Policy Ctr. to Darrell Issa, Elijah Cumming, and Jackie Speier	142
Response to questions from David A. Powner	148
Response to questions from Douglas J. Bourgeois	155
Submitted Testimony for House Oversight and Government Reform Committee Hearing from Consortium for Citizens with Disabilities	164
ICT Sector Trade Associations Comments on FITARA	167
Statement for the Record of the Professional Services Council	170
Statement for the Record of The Honorable Robert C. Cresanti, Vice President, SAP America	176

WASTING INFORMATION TECHNOLOGY DOLLARS: HOW CAN THE FEDERAL GOVERNMENT REFORM ITS IT INVESTMENT STRATEGY

Tuesday, January 22, 2013

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
WASHINGTON, D.C.

The committee met, pursuant to call, at 1:08 p.m., in Room 2154, Rayburn House Office Building, Hon. Darrell E. Issa [chairman of the committee] presiding.

Present: Representatives Issa, Mica, Turner, Duncan, Chaffetz, Lankford, Amash, Gosar, DesJarlais, Gowdy, Farenthold, Hastings, Lummis, Woodall, Massie, Collins, Meadows, Bentivolio, Cummings, Maloney, Norton, Tierney, Connolly, Speier, Cartwright, and Duckworth.

Staff Present: Ali Ahmad, Communications Advisor; Alexia Ardolina, Assistant Clerk; Richard A. Beutel, Senior Counsel; Robert Borden, General Counsel; Molly Boyl, Parliamentarian; Lawrence J. Brady, Staff Director; Caitlin Carroll, Deputy Press Secretary; John Cuaderes, Deputy Staff Director; Adam P. Fromm, Director of Member Services and Committee Operations; Linda Good, Chief Clerk; Michael R. Kiko, Staff Assistant; Mark D. Marin, Director of Oversight; Laura L Rush, Deputy Chief Clerk; Scott Schmidt, Deputy Director of Digital Strategy; Rebecca Watkins, Deputy Director of Communications; Peter Warren, Legislative Policy Director; Krista Boyd, Minority Deputy Director of Legislation/Counsel; Ashley Etienne, Minority Director of Communications; Jennifer Hoffman, Minority Press Secretary; Carla Hultberg, Minority Chief Clerk; Elisa LaNier, Minority Deputy Clerk; Lucinda Lessley, Minority Policy Director; Dave Rapallo, Minority Staff Director; Mark Stephenson, Minority Director of Legislation; and Cecelia Thomas, Minority Counsel.

Chairman ISSA. The committee will come to order.

The Oversight Committee exists to secure two fundamental principles. First, Americans have a right to know that the money Washington takes from them is well spent. And second, Americans deserve an efficient, effective government that works for them. Our duty on the Oversight and Government Reform Committee is to protect these rights. Our solemn obligation is to hold government accountable to taxpayers, because taxpayers have a right to know what they get from the government.

Our obligation is to work tirelessly in partnership with citizen watchdogs to deliver the facts to the American people and bring genuine reform to the Federal bureaucracy. This is our mission.

Today we advance that mission statement in the area of information technology, which is at the heart of whether the Federal government knows where the waste, fraud, and abuse is; knows or can be expected to deliver an efficient and honest return for every dollar contributed by the Federal taxpayers. To that extent, we have three panels today. This is not a controversial hearing within this committee. But it may be controversial outside of this dais.

In just the last 10 years, government spending on IT has risen by $46 billion. Even in Washington, that is a lot of money. We now spend $81 billion in 2012. As is the case government-wide, spending decisions were often not based on performance results. Program failures and cost overruns plague three-quarters of all large Federal IT programs. Federal managers say that 47 percent of their budget goes to maintain obsolete or deficient IT resources.

Estimates suggest that as much as $20 billion of taxpayer money is wasted each year. But let us understand, in this case it is not the waste of the $20 billion, it is what that $20 billion could do properly applied to our transparency into our government. The leveraging of $20 billion to save $200 billion is why it is essential that we fix this part of government that seems to be so broken.

We have built an IT infrastructure that is bloated, inefficient, and actually makes it more difficult for the government to serve its citizens in some cases. With more than $81 billion spent each year on Federal information technology, Americans are not getting anywhere close to what they would expect to get for their money.

Just last month, the Air Force announced that a $1 billion logistics system had failed and was being shut down. It was a logistics system that was needed. It will still be needed. We will still need to make these improvements.

I want to join with all those who realize that few of our programs that fail, fail because they weren't wanted or needed, they fail for other reasons. And that is what this committee is determined to get to the bottom of and change the system.

Often quoted in Washington is Albert Einstein saying, more or less, that if you keep doing the same thing over and over and expect a different result, that is the definition of insanity. We will not allow the Federal government to continue doing things over and over again that, in fact, more money has not made work better. It is our choice now to listen to all the parties who will come to bear to this committee. People who understand government procurement, of course; people who understand the private sector and what works there.

I have often quoted my working in my old company with companies like Circuit City, Best Buy, and Wal-Mart, companies that in some cases were very opaque; in other cases, visual on even my desktop, I could see every store, every product from my company, and whether, in fact, it was selling or not. I not only could see it, but my salesmen could see it. And if something didn't move in one store and moved in another, they knew that they could go and find out why. That doesn't exist in the Federal procurement system. It doesn't exist anywhere in government, and it needs to.

With that, I would like to introduce Mr. Cummings for his opening statement at this time.

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

I want to welcome all of our witnesses here today, including our good friend and distinguished former chairman, Tom Davis, who I just have a phenomenal amount of respect for.

Tom, it is good to see you again.

I think this is an appropriate first hearing for this Congress. This is a good government hearing that gets right to the core of our committee's jurisdiction. Today we are examining Federal spending on information technology. Our committee has jurisdiction over the efficiency and management of government operations and activities, including procurement. It is our responsibility to ensure that the Federal government is spending money wisely and efficiently.

I think all of our constituents would agree that they want to make sure that their tax dollars are spent that way, effectively and efficiently. This includes Federal spending on information technology. The President's fiscal year 2013 budget projected that agencies will spend $79 billion on IT this year. The Government Accountability Office has found that agencies did not have adequate oversight of these investments. In a report last October, GAO found that five major agencies have not been using the proper safeguards to ensure that their investments in the operation and maintenance of IT systems are performing as intended.

As GAO said, and I quote, "Until agencies address these shortcomings, there is increased risk that these agencies will not know whether the multi-billion dollar investments fully meet their intended objectives."

I look forward to hearing from Mr. VanRoekel, the Chief Information Officer, about the progress the administration has made in improving the quality of IT investments, what is being done to improve oversight of those investments, and how overall spending is being reduced.

In particular, I am interested in hearing about the administration's efforts to improve transparency of IT investments. I also look forward to hearing from the industry leaders who can identify the challenges, opportunities we face in our efforts to improve the way that government invests in IT.

And let me say this. As the chairman was speaking, I could not help but think about a few years ago when I sat as the ranking member on the Transportation Committee of the Maritime and Coast Guard Subcommittee. And one of the things that we discovered is that we had a broken procurement process in the Coast Guard. And the Coast Guard literally were buying boats that did not float, radar systems that were supposed to cover 360 degrees that were covering 180 degrees, radios that if they got wet, they did not operate. That was in this country.

But I hope you listened to what the chairman said very carefully. When we are wasting money and not using it effectively and efficiently, I mean, that is money that could be used to do some things that we really do need done. And so that is why this hearing is so important.

You know, I often talk to my staff about hearings and whether we get the value out of hearings. I want the people who address

us this morning to talk about how we can effectively get this done. I mean, it is nice to hear about the problem, but do we need time tables, Tom? I mean, what kind of things can be done so that when the chairman looks back at his legacy and hopefully we all look back at ours, we can say we actually did something and didn't just spend time talking about it.

I am sure the chairman shares any view. And I am hoping that when the folks come up here to testify, you will help us with some roadmaps—that is right, take out your pens, write it down—and so that we can be effective and efficient. Effective and efficient.

Finally, I want to applaud the work of our resident technology expert, Representative Connolly, the ranking member of the Government Operations Subcommittee. Mr. Connolly held a forum in his district last May that explored many of the very same issues we will hear about today. He also has taken the lead in introducing legislation to reduce waste by consolidating Federal data centers.

The administration's efforts on data center consolidation are expected to save the government $3 billion by 2015. I believe it is time to modernize the way the government does business. This will require strategic investments in technology. But we should not overlook the importance of strategic investments in our workforce. Our acquisition community needs to have the tools necessary to effectively oversee increasingly complex systems from beginning to end. These professionals ensure that the government is a smarter consumer.

And with that, I yield back.

Chairman ISSA. I thank the gentleman.

Because this will be referred to the Government Ops Subcommittee, I would like to recognize its chairman, Mr. Mica, for a short opening statement.

Mr. MICA. Well, thank you for yielding, and also thank you, Chairman Issa, for holding this important hearing, hearing that deals with government waste, particularly on the eve of the Congress considering expanding our national indebtedness, where it is nearly at $16.5 trillion, and we have got to look at every avenue and source of wasteful spending.

This is not a small-potatoes item. IT, we spent in the last decade $600 billion. And the information we have today we gain primarily from a 2012 report from the GAO which took the opportunity to review what was going on and highlighted the need to address potentially duplicative IT investments to avoid, again, wasteful spending. In fact, in the fiscal year that GAO looked at, 2011, they found that the Federal government funded 622 separate human resources systems, 580 financial management systems, and 777 supply chain management systems.

So what we have ended up with is various Federal agencies, as well as offices within the different agencies, making separate and very costly investments in back office systems that often perform the same function. And all this duplication comes at some pretty significant cost.

Unfortunately, that has been our approach. And what we should be doing is aggregating demand among the agencies and their different offices to get the best prices for various IT products and services, which we aren't properly doing.

We also waste money investing in systems that fail to become fully functional. And the staff, from the report, this GAO report, indicated that, for example, the National Archives and Records Administration, also under our committee's jurisdiction, poured—now listen to this—$375 million into the development of an electronic records archive system that has now been put to a halt. And we will look further at that.

Then we look at the office of OPM, Office of Personnel Management, cancelled its Retirement Systems Modernization program after spending nearly $0.25 billion on that program. We will look at this.

Despite these failed investments, OMB, unfortunately, recently abandoned the practice of including in the President's budget submission a summary of the extent of the risk represented by major Federal IT investments. According to a report issued by GAO last fall, the President's budget submission from 2007 to 2009 included an overview of the investment performance over several budget years of IT projects in need of management attention. But this practice was abandoned, unfortunately, by the White House in its last four budget submissions.

The unfortunate reality is that 16 years following the signing of the seminal Clinger-Cohen legislation that laid the very foundation for the Federal government's acquisition and management of IT and 10 years after the E–Government Act was passed which established the Federal chief information officers, the program would set program failure rates and cost overruns which currently now plague us and, unfortunately, they account for an estimated 72 to 80 percent of large government IT programs. And that is an industry calculation.

The first step in addressing any problem is determining who is responsible and holding people accountable. The Office of Management and Budget also needs to take responsibility for the lack of coordination and intelligent investment in IT being done at the agency level. OMB has to be willing to step up and take responsibility and say the buck stops here.

Finally, I am also disappointed that the head of OMB's Office of Federal Procurement Policy, the Federal government's chief acquisition individual and person responsible, is not with us today, although he was invited to testify. But I am glad we have with us today OMB's financial chief information officer. Look forward to his testimony and the others and look forward to working with you on this important issue. And yield back.

Chairman ISSA. I thank the gentleman.

We now recognize the ranking member, the gentleman who replaced our first witness, for his opening statement.

Mr. CONNOLLY. I thank the chair. And I thank the ranking member, Mr. Cummings, for his kind words. And I want to thank the chair. If the entire 113th Congress can begin on the note we are beginning on today, we are going to be making music for 2 years. But I want to thank the chair for his leadership in this particular area. We are working together and our staffs are working together on a draft bill that I think can move us into the bright sunshine of this part of the 21st century, giving more flexibility to the Federal government and to Federal managers. Because some of the

problems outlined by my friend, Mr. Mica, the new chairman of the Government Operations Subcommittee, have to do with how the government is organized and the flexibility or lack thereof that we give to managers.

And as indicated, we spend about $81 billion a year, not all of that well. Government is slow to pull the plug when we do make a mistake, much slower than the private sector. Government has a problem in terms of recruiting and retaining the skilled workforce you need for large, complex contracts such as these.

And so addressing those issues, both in process, procurement, and people, I think is very important.

And so I look forward to continuing to work with the chairman of the full committee and with the chairman of the subcommittee in trying to come up with legislation that makes sense, that provides flexibility, that gives maybe more discretion to CIOs, to the chief information officers of Federal agencies, and that will save money and make sure that the deployment of the resources we do have is more efficacious.

Finally, Mr. Chairman, I do want to welcome my predecessor, Tom Davis, former chairman of this committee, whose portrait hangs here, who preceded me on the Board of Supervisors of Fairfax County, proceeded me as the chairman of Fairfax County, and preceded me here in Congress.

Just last week, Tom was gracious enough to participate in a staff retreat I held—I have an annual staff retreat—sort of giving us a different take on some issues and how he did it in terms of managing constituent services and legislative assignments in the 14 years he graced these halls. I want to thank Tom for his graciousness as my predecessor and for making my transition here in Congress as smooth as possible. It is a model for bipartisan cooperation.

Welcome, Mr. Davis.

And thank you again, Mr. Chairman.

Chairman ISSA. I thank you.

Now we recognize the Honorable Mr. Davis, who has returned to the place in which he was hung.

Mr. DAVIS. Many times.

Chairman ISSA. Tom, you are my friend, you are my mentor. And as you have heard from both sides of the aisle, you are somebody whose opinion we respect. And with that, you are recognized.

STATEMENT OF HON. TOM DAVIS, A FORMER REPRESENTATIVE IN CONGRESS FROM THE STATE OF VIRGINIA

Mr. DAVIS. Mr. Chairman, thank you very much. And congratulation to both you and Mr. Cummings on a terrific start. I sat on this committee where the rules, sometimes we would be here all afternoon. So that is a good start. And I think the hearing is a great place to start because this is not a Republican or Democratic issue. We can argue over we have too much government or not enough government. But we want the government we are paying for. And that is really what this is about today. So I think we can join on that.

I just also say to subcommittee chairman Mr. Mica and to Mr. Connolly, Mr. Connolly, you followed me on the Board of Super-

visors, as chairman of the board and to Congress, and if you can like me retire undefeated and unindicted maybe one day you will be a witness as well.

Chairman ISSA. I think he wants to be hung, too.

Mr. DAVIS. Take a couple more terms and a switch. But I am not going to get into that.

Let me just also acknowledge, Jim Turner is here. He was the author of the E–Government Act. I attached a number of pieces of legislation, but Jim was a distinguished member of this committee on the Democratic side when I was the subcommittee chairman in 2002 when we worked that bipartisan legislation together. And I think it is time for an update. And I think this is an apt hearing for that.

Let me put all of my testimony in the record and just make a few salient points. The Federal government spends about $81 billion in IT annually, making it the largest single acquirer, adopter, and user of IT globally, more than any other nation, global corporation, or organization. So the Federal government should be the best at how it plans, sources, implements, and operates IT to achieve missions successfully. Doesn't always do it that way.

Few thoughts. We could get an improved return on investment. In the private sector, IT is an investment, it is a strategic enabler. But in the Federal government all too often IT is viewed and treated as a discretionary expense. Cost savings realized from these investments can be many times greater than what you achieve when you cut IT and require, and we can achieve part of this by executive oversight.

CIO authority. Department-level CIOs currently have responsibility and accountability to manage their IT deployments, but they lack the organizational and budget authority.

Too loud? Okay.

Chairman ISSA. Just if you could, Tom, if you could pull it a little bit closer. We are getting a little echo up here.

Mr. DAVIS. Okay.

Shared services. Federal government is the only large multinational organization globally who has not implemented shared services for its back office functions. OMB should build upon its prior line of business and shared first strategies to require agencies to move away from the bureau-centric administrative systems and to department-wide and government-wide administrative shared solution services.

Also, on cybersecurity, really nothing else matters in Federal IT if the government doesn't get cybersecurity right. We passed FISMA, the Federal Information Security Management Act, as a part of the E–Government Act in 2002. It needs to be updated and operationalized. I know there are jurisdictional problems here in Congress, but if we don't get cybersecurity right, nothing else is going to matter.

Information, devices, and the Federal workforce is becoming increasingly mobile. Therefore, OMB and congressional oversight for government-wide implementation of existing cybersecurity priorities is critical. And as the government moves from securing systems and devices to securing data at rest and data in transit for information-sharing purposes, the government will need to identify

and implement new solutions in areas such as continuous monitoring, identity, authentication, and credential management and cryptology.

Let me also move in my last minute and a half, the procurement workforce. This has been a problem. We have cut back the procurement workforce, we don't give them appropriate training, we don't give sometimes enough leeway. This is critical. So many IT functions that go sideways are because we don't have the appropriate oversight, we haven't empowered our procurement workforce to do the job.

Procurement processes, as you know in government, sometimes the mission is not to make a mistake. So you don't get the kind of innovation that you would get in other cases. And I could talk more on that during the questions and answers, but I want to get through my time.

Continuing resolutions. CRs kill IT procurements, it kills innovation in government, because no agency head is going to be spending their budget on new procurements, follow-on work, if they don't know what their budget is going to be. Their inclination is to protect their people. And we have seen us step backward and backward as Congress doesn't get budgets done on time and goes through CRs.

And finally, some of the rules that we have that I think are passed with good intentions to ensure that lobbyists don't come in and have undue influence also hurt us because many times the people writing these have not had appropriate contacts with the outside world, small companies trying to get in and share their ideas in government and operate in a bubble.

I think it is a good idea for companies to come in and share their ideas and have an open door to policymakers so that they know what the existing technologies are, can be aware of what government's needs are, and therefore can address them in the procurements. And I will stop there on time.

Chairman ISSA. I have never seen a professional get it exactly to the second. Tom, you are good.

[Prepared statement of Mr. Davis follows:]

Statement of the Honorable Thomas M. Davis
"Wasting Information Technology Dollars:
How Can the Federal Government Reform its IT Investment Strategy?"

House Committee on Oversight and Government Reform
January 22, 2013

Good afternoon, Chairman Issa, Ranking Member Cummings, and Members of the Committee. Thank you for the opportunity to be here today to offer my thoughts on the Federal information technology investment strategy. I would note that I am here in my capacity as the former chairman of this Committee, not on behalf of my current employer, Deloitte.

I applaud the Committee for looking at these important IT issues. There is never a good time to waste money on cost overruns, schedule delays or failed projects. In a time of extreme budgetary pressures, however, it is more important than ever to realize the potential efficiencies Federal information technology can offer, as taxpayers will expect the same level of service from government despite reduced funding.

As a Member of Congress, I had the honor of serving on this Committee, to include periods as the chairman and ranking member. During that time, I devoted much of my efforts to realizing the potential of information technology to modernize the operations of the Federal government. As this committee embarks on a renewed effort, there are a few points I would like to raise.

1. Our procurement process and procurement workforce are insufficient.

In general, if we want to get the best value for the government at the best price, our procurement process should be geared towards just that – getting the best value for the best price. But it's not. It is focused on other objectives, such as promoting small businesses, disadvantaged demographic groups or domestic sourcing ("Buy America"). These goals might be laudable, but the taxpayer pays a price in terms of increased complexity and diminished outcomes.

With respect to IT procurement, the IT industry and the Federal procurement process couldn't be more different. Information technology is the most innovative, entrepreneurial and disruptive part of our economy. Federal procurement is just the opposite. The life cycle of a given procurement is simply too long to allow agencies to keep up with evolving technology. This isn't helped by the ever increasing number of bid protests.

There is little room for innovation or creative thinking. We do not reward achievement; rather, we punish mistakes. Thus, it is little surprise that's what the focus has become – not making a mistake.

It would be in everyone's interest is to create more flexibility in the system and to shift the focus to outcomes, rather than just costs. There might be some errors – there already are errors – but the tradeoff would definitely be in the taxpayers' favor. Along these lines, I have long favored the use of share-in-savings contracts. This would allow companies to offer innovative ideas to create savings. The formula is simple – they bear the risk of actually delivering on what they say they can do. If they are successful, they make money; if not, they don't. A criticism of this approach often is that the government ends up giving away too much of the saved revenues, but that misses the point entirely. There would have been no savings at all had the share-in-savings approach not been used.

Another recurring issue is the need for a highly skilled procurement workforce. I think it is a good idea to advocate a core group of technology procurement professionals that agencies can leverage for their more complex needs. Having a select number of such groups, coupled with a reduced number of GWACs, would provide a certain amount of inter-governmental competition while not unnecessarily raising industry's costs to get on an inordinate number of contract vehicles. Everyone would benefit from such an approach – government needs procurement professionals who know more than the people selling to them. For contractors, having a smart client who knows what the government wants is the best situation. They might drive a harder bargain, but it is a much better working situation.

When I was on the committee, I advocated a Digital Tech Corps. This is one approach, and would have involved bringing in private sector talent on a revolving basis. This would give the Federal government access to additional skills and capabilities. For someone in the private sector, it would provide a valuable opportunity to gain the perspective of the public sector.

2. Manageable Chunks

The government's approach to buying IT systems is problematic in that it often tries to do too much at once. Instead of setting out upon the mammoth task of procuring a system worth hundreds of millions of dollars, it might be better to do things in smaller pieces. If something goes wrong with a component of a large implementation, the whole effort can begin to crumble, and instead of ending up with a super system that does everything, we get a pile of worthless technological rubble. It would be better to break things up into smaller chunks and make sure they work before going on to other steps. This is the way private industry works – government should move in this direction as well.

3. Accountability

There must be a balance between centralization and decentralization in Federal information technology. In my opinion, it is difficult to expect departmental chief information officers to perform as intended if they do not have appropriate authority over the IT budget. This is an issue the Committee should review. There may be concerns this would create an unnecessary level of bureaucracy, but again, there needs to be somebody with cognizance, oversight and authority – especially over enterprise-wide systems. Otherwise we cannot expect a departmental CIO to even know what is going on in the functional agencies, and greatly increases the opportunities for problems.

In closing, the issues I have mentioned are perennial problems. They say there is a silver lining in every cloud - I am left to wonder if the current fiscal environment could help us drive past some of these obstacles to a fully functioning Federal government. The work you are undertaking here could well be an important step in that direction.

Again, thank you for the opportunity to testify. I would be more than happy to answer any questions you may have.

Chairman ISSA. Because you are an unusual witness, I have so many questions that I will just follow up endlessly over dinner sometime.

But, Mr. Davis, the one thing that I wanted your comment on that wasn't in your opening statement was, because you were here for the creation of chief information officers, did you ever envision having more than one chief per agency and on the average more than two chiefs per agency and all but one of them not having any budget authority?

Mr. DAVIS. No. I don't think anyone knew what would happen when we set them up this way. There has certainly been a proliferation of CIOs. But I think you can have as many as you want if you give them the right authority. The problem is they are sitting out there and in many cases they are toothless tigers. Some great people, very dedicated. But if you can't enforce this, that is why we get so many stovepipes built up.

Chairman ISSA. So it would be fair to say that the 40 CIOs that are in Department of Justice alone would be a little more than you would have assigned.

Mr. DAVIS. I don't think anybody envisioned that when we did it originally.

Chairman ISSA. Or the 35 in the Department of Transportation.

Mr. DAVIS. Well, I am not picking on anybody. But I just think, at the time—what you need are lines of authority and decision makers. It is okay to have a multiplicity of CIOs if they have authority. But if they don't have authority.

Chairman ISSA. So, in short, if they have their share of the budget and can be held accountable for every penny that goes under their jurisdiction, you are okay with it as long as, in fact, that is what comes with being a chief, is budget authority.

Mr. DAVIS. Well, you know, look, you don't want 40 stovepipes out there. You have got to have your CIO for your agency overseeing those kind of things. And whatever you call the other CIOs, at the end of the day there needs a congruency there that is not always built into the system. CIOs don't know who to report to. If you are a CIO, for example, subsidiary within an organization, do you report to your CIO or do you report to your agency head? So there is just I think a lot of confusion out there over what the authority lines go.

Chairman ISSA. Mr. Cummings?

Mr. CUMMINGS. Tom, when you were chairman of this committee, you authored the Federal Information Security Management Act, and Chairman Issa and I worked together last Congress to introduce legislation to update FISMA, which has now been in place, of course, for over a decade. Our bill would require that the Federal government shift to a system of continuous monitoring of information systems.

One of the things that we hear a lot about, of course, is cyber threats. You have already said that you think that FISMA needs to be updated. But can you talk about the cyber threats, because it seems that that is what we should be worried about, because it is my understanding that these threats and cyber attacks can do quite a bit of damage, and I just wanted you to comment on that.

Mr. DAVIS. They do all kinds of damage. First of all, they could do societal damage like a 9/11, when you get into it, if they get into the wrong systems and were at play. But you have a lot of information being lifted. And I don't want to get into—you have had situations where we are negotiating trade agreements and we are negotiating with other countries and they have been able to lift all of our information off.

So it is basically the fact that a lot of confidential private government information is being lifted off by our competitors and we are providing it to them free. It is a huge cost to taxpayers and a huge cost basically to America.

Mr. CUMMINGS. Now, are there any other changes to the law that you think we need to make?

Mr. DAVIS. Well, I think just on FISMA how you do it there are probably a dozen ways to do it, but it needs to be operationalized. It has turned into a check-the-box routine. It has had some good things, because they weren't even checking boxes before this. But I think your idea of continuous monitoring, testing, prodding of the systems is very, very important. So that is the direction I think it needs to move.

Mr. CUMMINGS. Mr. Chairman, I yield back.

Chairman ISSA. I thank the gentleman.

Per your agreement, I understand you will be able to answer written questions by both sides.

With that, we will take an extremely short recess and go to our next panel.

Thank you again, Mr. Davis.

[Recess.]

Chairman ISSA. While that second panel is getting set up, for the new members I think it is important to note that normally Members of Congress who come before this committee testify but don't answer any questions. So Mr. Davis sort of is in that in between, and I appreciated that he took a couple of follow-ups. But for future reference, and this includes when you may go based on areas of expertise to other committees, that is normally the tradition, is Members are not sworn and Members of the House and Senate normally don't answer questions, although they may. So just a little piece of information from an old guy.

And with that, we recognize our second panel of witnesses. Mr. Steven VanRoekel is the Federal Chief Information Officer of the Office of Management and Budget. Now, that is a chief's chief. We want to make sure we get that out here, because Mr. Davis defined such a thing. And Mr. David Powner is the Director of Government Accountability Office, Information Technology Management, and in fact for those again new members, GAO works for us.

So I want to thank both of you for being here today. Pursuant to the committee rules that were just passed before your very eyes, I would like you to both rise and take the oath. Please raise your right hands. Do you solemnly swear or affirm that the testimony you are about to give will be the truth, the whole truth and nothing but the truth? Let the record indicate that both witnesses answered in the affirmative. Please be seated.

My previous chairman, Mr. Towns, is now retired, but I will one time more introduce the clock the way he did. Everywhere in

America we know that green means go, yellow means go through the intersection real quick, and red means stop. So it is a 5-minute clock. Please come as close as you can to it.

Mr. VanRoekel?

WITNESS STATEMENTS

STATEMENT OF STEVEN VANROEKEL

Mr. VANROEKEL. Good afternoon, Chairman Issa, Ranking Member Cummings and members of the committee. Thank you for the opportunity to testify on the administration's efforts to manage the Federal government's investment in information technology.

The growth of cloud computing, mobile devices, data and social media is creating a demand for government services that is once unforeseen. Americans' expectations of their government have reached a critical point even faster than we anticipated. They expect us through the use of technology to provide the same quality of service they experience in their everyday lives and we must meet these expectations efficiently and securely.

During my nearly 20 years in the private sector, I woke up every day focused on improving and expanding core services and customer value while also cutting costs. We must ensure the Government has the same mentality by driving innovation to meet customer needs, maximizing the return on our investment in Federal IT, and in establishing a trusted foundation for securing and protecting our information resources.

Since the mid-1990s, Federal IT spending grew about 7 percent annually. A culture was built which assumed that to do new things we must spend more. Had we continued on that growth curve, we would be spending over $100 billion on IT today versus the $78 billion to $81 billion we do spend. In 2009, we worked to freeze Federal IT expenditures, and under my watch we have reduced it year over year. Although spending is flat or declining, we refuse to use this as an excuse to do less with less. Instead, we are applying the private sector mentality of continuous improvement to expand and improve core services and customer benefit while reducing costs. In this time of fiscal austerity, we must ensure that we are always innovating with less.

But if we focus solely on cost reduction we will overlook the value that IT brings to the Government and our country. Few, if any new government services will be established without technology as their foundation. Strategically investing and deploying IT can provide a downstream multiplier effect, not only in efficiency and cost savings, but by making us more productive, more customer friendly and more secure.

Today I would like to highlight the three principles in our approach to innovate with less. First, we are working every day to drive innovation into everything we do. The value of government programs rests upon their ability to positively impact the lives of Americans. Simply put, the American people must be at the center of every action we take and no decision should be made that cannot be tied to significant customer benefit or savings.

We must also embrace 21st-century ways of building government solutions. For too long the Federal landscape has not benefited

from productivity gains seen in the private sector. We can't just spend less; we need to change the way we do business. This includes modular solutions, embracing mobile technology in new ways, and creating services that were once unforeseen.

Driving innovation doesn't end at the walls of government. The information maintained by the government is a national asset with tremendous potential value to the public, entrepreneurs, and to our own programs. The administration's innovation agenda includes multiple initiatives that will open data to enhance information exchanges, interoperability, and public release of data while safeguarding information security and privacy. Open government data is creating an incredible platform for innovation in the private sector, continuing to foster an increasingly important role for government in the new data economy. Today, private sector entrepreneurs are leveraging this asset to create jobs and provide better service for the American people.

Second, we are focused on maximizing the overall return on investment in Federal IT and are providing agency leadership with tools to help look across their IT portfolios to make strategic investment decisions. We are driving cost savings in government through many targeted efforts, including investment reviews, our cloud-first policy, strategic sourcing, data center optimization and PortfolioStat. By gaining efficiency we can not only save money, but we can drive innovation in government by culling from inefficient programs and reinvesting in high ROI, mission-focused technology solutions.

Third, we are advancing cybersecurity capabilities on every front. This issue requires creative solutions to address emerging and increasingly sophisticated threats and new vulnerabilities introduced by rapidly changing technology. To overcome this challenge we must continue to implement initiatives such as the cybersecurity agency goals, FISMA and FedRAMP, and to continuously measure agency progress in improving information security performance. Building on the last four years, our focus going forward will be to drive innovation in government and make investments in technology that better serve the American people. We will use technology to improve productivity and lower barriers to citizen and business interaction with government, all while bolstering cybersecurity.

Thank you for the opportunity to appear today, and I look forward to our discussion.

Chairman ISSA. Thank you.

[Prepared statement of Mr. VanRoekel follows:]

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

January 22, 2013

STATEMENT OF STEVEN VANROEKEL
FEDERAL CHIEF INFORMATION OFFICER,
ADMINISTRATOR FOR E-GOVERNMENT AND INFORMATION TECHNOLOGY,
OFFICE OF MANAGEMENT AND BUDGET

BEFORE THE HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

"Innovating with Less: Strategically Investing in Federal IT"

Good morning, Chairman Issa, Ranking Member Cummings, 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).

As I was finishing my undergraduate degree, the era of personal computing was just being set in motion, and within months of graduation, I was working for the Microsoft Corporation. Before joining Federal Government in 2009, I spent my entire post-college private-sector career at Microsoft, including three years as Speech and Strategy Assistant to Bill Gates, the corporation's co-founder, and most recently as Senior Director of the Windows Server division. I saw firsthand the power of technology and saw the incredible impact American innovation has on society.

During that nearly 20 years in the private sector, I woke up every day focused on improving and expanding core services and customer value, while also cutting costs. Although information technology is a small part of the Government's annual spending, it is at the core of almost everything we do. As such, 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.

As the Committee is aware, customer demand, fiscal austerity, and the interconnectedness of our digital world dictate that we must continually improve the way we procure, build, and manage Federal IT. The growth and pervasiveness of cloud computing, mobile devices, information, and social media are creating a demand for Government services that were once unforeseen. Expectations have reached a critical point even faster than anticipated.

Today, Americans pay bills online and buy plane tickets on smartphones. They expect us, through the use of technology, to provide the same quality of service they experience in their everyday lives. The Government must work to meet these expectations, efficiently and securely.

Eliminating duplicative IT, reforming Federal IT management, and streamlining service delivery were at the core of the Administration's first term IT agenda. Building on the progress of the last four years, my objective is to balance cost savings with innovation by continuing to cut costs while we invest in technology that securely serves the American people.

Strategic Priorities

The Administration must approach the strategic investment in IT through three priorities: innovating for the American people; improving our return on investment, or ROI; and advancing cybersecurity.

- **Innovate for the American People** – The value of Government programs rests upon their ability to positively impact the lives of Americans. Simply put, the American people must be at the center of every action we take, and each decision should be tied to a significant benefit for them. We should evaluate the success our IT investment by whether those efforts are meeting the public's needs. Those needs include simplifying the complexity of Government for the public. Additionally, the Government possesses a rich inventory of data. When utilized properly, with attention to privacy and security concerns, this data can create an incredible platform for innovation in the private sector while continuing to foster an increasingly important role for Government in the new data economy.

- **Improve the Return on Investment (ROI) of Federal IT** – To maximize our investment in IT, the Government must better manage the cost of providing IT services. Managing IT in an innovative way means consolidating redundant applications, systems, and services. It also means establishing common testing platforms to foster interoperability and portability so that we can build once and then use many times across the whole of Government. We must streamline the delivery of new infrastructure, and shift from asset ownership to service-orientation, which means that technology is delivered as a service – much like water or electricity – rather than built as a proprietary system. By culling from inefficiency and reinvesting in high ROI areas, we can drive innovation in government that creates efficient, mission-focused technology solutions.

- **Advance Cybersecurity** – The cybersecurity threat is one of the most serious national security, public safety, and economic challenges we face as a Nation. This issue requires creative solutions to address emerging and increasingly sophisticated threats, as well as

new vulnerabilities introduced by rapidly changing technology. To overcome these challenges, Federal agencies must improve cybersecurity capabilities to provide safe, secure, and effective mission execution and services to the American people, with a focus on accountability. Specifically, we must continue to implement initiatives such as the Cybersecurity Cross Agency Priority Goal, or CAP Goal, which is part of the Administration's broader performance management improvement effort, Federal Information Security Management Act, and the Federal Risk Authorization and Management Program (FedRAMP), and to continuously measure agency progress in improving information security performance.

In the near term, the Administration is using three strategic initiatives to measure and drive results in these areas. The first is the Administration's Digital Government Strategy—released last May – that is a comprehensive set of measures to deliver better digital services for the American people. The second is PortfolioStat, which is a tool agencies use to assess and improve the maturity of their IT portfolio management processes. The third is Cyberstat, which is a process that manages the security of our IT assets by identifying gaps and opportunities in agency cyber capabilities.

Digital Government Strategy

The Administration's Digital Government Strategy has three main objectives: (1) ensure the American people and an increasingly mobile workforce have access to high-quality, digital Government information and services anytime, anywhere, on any device; (2) ensure that in adjusting to this new digital world, the Government seizes the opportunity to procure and manage devices, applications, and data in smart, secure and affordable ways; and (3) unlock the power of Government data to spur innovation across our Nation and expand and enhance services available to the American people.

PortfolioStat

Last year, I launched PortfolioStat, which instituted a forum for agency stakeholders to collectively examine targeted outcomes, strategy, and overarching management processes to identify opportunities for improvement. This effort resulted in ambitious, forward-looking strategies that, if implemented, will save the Government from spending $2.5 billion over the next three years by consolidating duplicative systems, buying in bulk, and ending or streamlining off-track projects. In 2013, the Administration will continue to drive comprehensive performance and management evaluations so that agencies may better manage and improve the maturity of their IT portfolios. PortfolioStat demonstrates that there continues to be opportunity for agencies to focus on terminating redundant, outdated or otherwise low value investments to free up resources to fund emerging priorities.

CyberStat

CyberStat is a review process focused on improving agency cybersecurity performance as part of the Cybersecurity CAP Goal. The Cyber CAP Goal measures agency progress in implementing the three priority cybersecurity capabilities of continuous monitoring, trusted Internet connections, and strong authentication with Homeland Security Presidential Directive 12 (HSPD 12) personal identity verification cards. These reviews provide the opportunity for agencies to identify cybersecurity capability areas where they may be facing challenges (such as technology, organizational culture, internal process, or human capital/financial resource challenges), as well as prospects and strategies to improve cybersecurity performance.

Over the long term, the Administration, along with the Federal IT community will focus on opening our data, making use of lightweight emerging technologies, and adopting modular development methodologies, consistent with system security and privacy controls, to allow us to further increase the quality of Federal services while curbing costs.

Additionally, we recognize that agencies are at different levels of progress in terms of how they are using and managing technology. Rather than attempt to force-fit all agencies into the same solutions, we must begin with flexible frameworks that enable all agencies to innovate.

Results through Innovation

Innovation must become the central tool to drive strategic investment in Federal IT. There are many initiatives across Government that illustrate how, over the long term, we can more efficiently and effectively manage IT. Today, I want to highlight three examples of initiatives aligned with the strategic priorities in IT

Open Data. The information maintained by the Government is a national asset with tremendous potential value to the public, entrepreneurs, and to our own Government programs. The Administration's innovation agenda includes multiple initiatives that will open Government data to enhance information exchanges, interoperability, and public release (subject to valid restrictions) while enabling the public, including private sector entrepreneurs, to leverage open government data to create jobs and provide better services for the American people. We are already seeing new companies and new services being built around utilizing newly-available Government data. For example, in the last year, the online real estate services Trulia and Zillow made initial public offerings. The service these companies provide would not be possible without the government data that underlies the two websites.

IT-as-a-Service. Through the advent of cloud computing, the IT community now has a scalable and transparent way to purchase and provide services, enabling agencies to transform how the organization leverages technology by pivoting away from the old model of buying IT as an asset.

The technology "as-a-service" model allows agencies to buy only what they need and to share services more effectively across organizational silos. For example, the Department of Homeland Security (DHS) Office of the Chief Information Officer has stood up multiple "as a service" technology platforms, including email as a service, customer relationship management as a service, and business intelligence as a service, that each component of DHS can leverage without investing or building proprietary solutions of their own. This model allows DHS components to save time and money and instead focus their human capital on the varied and important missions across the Department.

Continuous Monitoring. Continuous monitoring is an integral part of an enterprise-wide risk management process that allows agencies to establish the context of their risk management programs, and subsequently assess, respond to, and monitor risk on an ongoing basis. As the world becomes increasingly interconnected, we must prepare to confront a host of new threats that evolve in real time.

These three examples are a small sample of many across the Federal Government where a strategic investment in innovation is driving better management of Federal IT. These initiatives, and the many other IT gains attained by this Administration, were achieved while lowering overall expenditures on Federal information technology.

Conclusion

In challenging times, we must tap into underutilized human capital, technology, information, and other resources, picking up the pieces to transform them into something completely new. Rather than use the current fiscal situation as an excuse to reduce services, the Administration views it as an opportunity to cut inefficiencies and invest in innovation that will drive better service, efficient spending, and more vigilant security.

As a general matter, the Federal Government has shifted its mindset from building proprietary and highly customized systems to adopting a vision of innovating with less. I appreciate the work this Committee has done in this area—as you know, the magnitude and importance of these efforts requires all of us to continue to work together.

Thank you for the opportunity to appear today and I look forward to our discussion.

Chairman ISSA. Mr. Powner?

STATEMENT OF DAVID A. POWNER

Mr. POWNER. Chairman Issa, Ranking Member Cummings and members of the committee, we appreciate the opportunity to testify on wasteful IT spending. My comments will focus on three areas. One, the Government's poor record when it comes to delivering IT. Two, recent OMB initiatives to address the problems. And three, what needs to be done to fully address the issues at hand.

GAO's work and others over the year have shown that the Government has a poor track record when it comes to managing and delivering IT. My written statement lays out several recent examples where billions of taxpayers' dollars have been wasted on failed projects. In addition, the IT Dashboard currently shows nearly 200 investments totaling $12.5 billion that are at risk, and these numbers are understated.

To address these issues, over the past several years OMB has put in place several initiatives that have resulted in improvements. First, the IT Dashboard provides realtime reporting of over 700 major investments and highlight CIOs' assessment of each. This information has been used to terminate and scale back projects and reduce budgets by nearly $4 billion, according to OMB. In addition, the comprehensive IT reform plan covers areas like IT governance, program management and procurement. An important goal of this plan is for agencies to turn around one-third of their underperforming projects.

One of the more important aspects of the reform plan is the data center consolidation effort, in which OMB claims could result in $3 billion in savings. And more recently the administration rolled out the PortfolioStat initiative that focuses on eliminating duplicative IT systems. OMB estimates about $2.5 billion in savings here. The big takeaway here is that by turning around troubled IT projects, consolidating data centers, and eliminating duplicative commodity IT systems, the Government can save somewhere between $5 billion and $10 billion if indeed these initiatives are successfully carried out.

Based on our work over the past several years, here are key areas that need more attention. First, we need even better transparency and more action on troubled projects. This starts with accurate information on the IT Dashboard. We can't have situations where agencies like DOD report no high risk systems when in fact they have many. On the other hand, some agencies, like DHS, are reporting accurately and moving more of their projects to a green status. However, overall agencies are nowhere near accomplishing the IT reform goal of turning around one-third of the underperforming projects. I would like to stress the importance of tackling these projects in smaller increments. My written statement highlights seven successful IT acquisitions and each took an incremental approach.

Second, we need to tackle duplication more aggressively. For example, our work shows that 27 major departments and agencies have nearly 600 financial management systems and spend almost $3 billion on these systems annually. The administration's

PortfolioStat process is an excellent initiative to address this duplication.

Third, OMB and agencies need to follow through on their data center plans. Server utilization rates are far below desired amounts, consolidation still needs to occur, and ultimately the key performance metric here is dollars saved. DOD alone reports that they can save $2.2 billion and OMB claims that the Government can save $3 billion by 2015.

Finally, the Government needs to perform the required operational analysis on the operational systems totaling $55 billion so that over time we can spend more money on modernizing government operations and less on maintaining old, archaic systems. All these areas—improving transparency, turning around large IT acquisitions, tackling duplication, optimizing data centers, and shifting the percentage of what we specifically are spending the $80 billion on—require strong and accountable chief information officers and attention to the many GAO recommendations we have made in these areas.

Mr. Chairman, GAO's plan is to stay on top of these important issues as we currently have worked, looking at the Dashboard, PortfolioStat, data center consolidation and IT duplication. We look forward to further assisting you in your important oversight role. This concludes my statement. I would be pleased to respond to questions.

Chairman ISSA. Thank you.

[Prepared statement of Mr. Powner follows:]

United States Government Accountability Office

GAO

Testimony

Before the Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 1:00 p.m. EST
Tuesday, January 22, 2013

INFORMATION TECHNOLOGY

OMB and Agencies Need to Fully Implement Major Initiatives to Save Billions of Dollars

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

GAO-13-297T

January 22, 2013

GAO
Accountability * Integrity * Reliability

Highlights

Highlights of GAO-13-297T, a testimony before the Committee on Oversight and Government Reform, House of Representatives

INFORMATION TECHNOLOGY

OMB and Agencies Need to Fully Implement Major Initiatives to Save Billions of Dollars

Why GAO Did This Study

The federal government plans to spend more than $74 billion on IT investments in fiscal year 2013. Given the size of these investments and the criticality of many of them to the health, economy, and security of the nation, it is important that OMB and federal agencies provide appropriate oversight of and adequate transparency into these programs. Nevertheless, IT projects too frequently incur cost overruns and schedule slippages, and result in duplicate systems while contributing little to mission-related outcomes.

GAO was asked to testify on the results and recommendations from its selected reports that focused on key aspects of the federal government's acquisition and management of IT investments. To prepare this statement, GAO drew on previously published work.

What GAO Recommends

GAO has issued numerous recommendations to OMB and agencies on key aspects of IT management, including (1) OMB's public website, known as the IT Dashboard, which provides detailed information on federal agencies' major IT investments, and (2) efforts to oversee IT operations and consolidate data centers.

View GAO-13-297T. For more information, contact David A. Powner at (202) 512-9286 or pownderd@gao.gov.

What GAO Found

GAO has issued a number of key reports on the federal government's efforts to efficiently acquire and operate information technology (IT) investments and found that if major initiatives are fully implemented, billions of dollars in savings could be realized. In particular, GAO has made recommendations regarding the Office of Management and Budget's (OMB) public website, known as the IT Dashboard, which provides detailed information on federal agencies' major IT investments; agencies' efforts to perform analyses on existing IT investments; and agencies' progress toward consolidating data centers.

OMB has taken significant steps to enhance the oversight, transparency, and accountability of federal IT investments by creating its IT Dashboard, and by improving the accuracy of investment ratings. However, there were issues with the accuracy and reliability of cost and schedule data in the Dashboard, and GAO has recommended steps that OMB and agencies should take to improve these data—this is important since the Dashboard reports 190 investments totaling almost $12.5 billion being at risk. GAO recently reported that six federal agencies consistently rated the majority of their IT investments as low risk. Further, the Department of Defense's (DOD) ratings reflected considerations in addition to those OMB recommends, and consequently it did not rate any of its investments as high risk. However, GAO has recently reported that several DOD investments experienced significant performance problems and were indeed high risk, and that DOD business systems modernization is a high-risk area. In the past, OMB reported trends for risky IT investments needing management attention as part of its annual budget submission, but discontinued this reporting in fiscal year 2010. GAO recommended OMB analyze agencies' investment risk over time as reflected in the Dashboard's ratings and present its analysis with the President's annual budget submission.

While agencies plan to spend billions on operational investments—more than $54 billion in fiscal year 2013— they have not always provided adequate oversight of these investments. Specifically, GAO reported in October 2012 that five agencies had operational investments with a fiscal year 2011 budget of over $3 billion that had not undergone operational analyses as required by OMB. The report also noted that until operational investments are fully assessed, there was increased potential for these multibillion dollar investments to result in unnecessary waste and duplication. GAO recommended that the five agencies conduct required analyses.

GAO reported on the federal government's progress toward data center consolidation (which OMB expects will save $3 billion by 2015). In July 2012, GAO found that agencies updated their required inventories and plans, but only 3 of 24 agencies in the review submitted complete inventories and only 1 agency submitted a complete plan, as required by OMB. Until these inventories and plans were complete, agencies would continue to be at risk of not realizing anticipated savings, improved infrastructure utilization, or energy efficiency. Accordingly, GAO reiterated a prior recommendation to update inventories and plans, and also recommended that agencies use best practices when developing estimates.

January 22, 2013

Chairman Issa, Ranking Member Cummings, and Members of the Committee:

I am pleased to be here today to discuss the highlights and recommendations of our selected reports that focused on key aspects of the federal government's acquisition and management of information technology (IT) investments. As reported to the Office of Management and Budget (OMB), federal agencies plan to spend more than $74 billion on IT investments in fiscal year 2013. Given the size of these investments and the criticality of many of these systems to the health, economy, and security of the nation, it is important that OMB and federal agencies provide appropriate oversight of and adequate transparency into these programs.

As we have previously reported, federal IT projects too frequently incur cost overruns and schedule slippages while contributing little to mission-related outcomes.[1] During the past several years, we have issued multiple reports and testimonies on federal initiatives to acquire and improve the management of IT investments.[2] We made numerous recommendations to federal agencies and OMB to further enhance the management and oversight of IT programs.

As part of its response to our prior work, OMB deployed a public website in June 2009, known as the IT Dashboard, which provides detailed

[1]See, for example, GAO, *Information Technology: Better Informed Decision Making Needed on Navy's Next Generation Enterprise Network Acquisition*, GAO-11-150 (Washington, D.C.: Mar. 11, 2011); and *Border Security: Preliminary Observations on the Status of Key Southwest Border Technology Programs*, GAO-11-448T (Washington, D.C.: Mar. 15, 2011).

[2]GAO, *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); *Information Technology: Agencies Need to Strengthen Oversight of Billions of Dollars in Operations and Maintenance Investments*, GAO-13-87 (Washington, D.C.: Oct. 16, 2012); *Data Center Consolidation: Agencies Making Progress on Efforts, but Inventories and Plans Need to Be Completed*, GAO-12-742 (Washington, D.C.: July 19, 2012); *Information Technology: Critical Factors Underlying Successful Major Acquisitions*, GAO-12-7 (Washington, D.C.: Oct. 21, 2011); *Information Technology: Continued Attention Needed to Accurately Report Federal Spending and Improve Management*, GAO-11-831T (Washington, D.C.: July 14, 2011); and *Information Technology: Investment Oversight and Management Have Improved but Continued Attention Is Needed*, GAO-11-454T (Washington, D.C.: Mar. 17, 2011).

information on federal agencies' major IT investments,[3] including assessments of actual performance against cost and schedule targets (referred to as ratings) for approximately 700 major federal IT investments. In addition, OMB has initiated other significant efforts following the creation of the Dashboard. For example, it developed a 25-point plan for reforming federal IT (IT Reform Plan), launched an initiative to reduce the number of federal data centers (the Federal Data Center Consolidation Initiative (FDCCI)), implemented a cloud computing[4] policy, and recently initiated its PortfolioStat effort.[5]

You asked us to testify on the results and recommendations from our selected reports that focused on key aspects of the federal government's acquisition and management of IT investments. Accordingly, my testimony specifically discusses our recent reports on OMB's IT Dashboard, IT acquisition best practices, management of IT operations and maintenance (O&M) investments, cloud computing, the IT Reform Plan, and data center consolidation.[6] All work on which this testimony is based was performed in accordance with generally accepted government auditing standards or all sections of GAO's Quality Assurance Framework that were relevant to our objectives. Those standards and the framework require that we plan and perform our audits and engagements to obtain sufficient, appropriate evidence to provide a reasonable basis for our

[3]A major IT Investment is a system or an acquisition requiring special management attention because it: has significant 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.

[4]Cloud computing is an emerging form of delivering computing services via networks with the potential to provide IT services more quickly and at a lower cost. Cloud computing provides users with on-demand access to a shared and scalable pool of computing resources with minimal management effort or service provider interaction. It reportedly has several potential benefits, including faster deployment of computing resources, a decreased need to buy hardware or to build data centers, and more robust collaboration capabilities.

[5]PortfolioStat is intended to be a tool for agencies to use to assess the current maturity of their IT portfolio management process and make decisions on eliminating duplication across their organizations. Agencies are to use data from PortfolioStats to establish targets for commodity IT spending reductions and deadlines for meeting those targets.

[6]GAO-13-98; GAO-13-87; GAO-12-742; GAO-12-7; and GAO, *Information Technology Reform: Progress Made; More Needs to Be Done to Complete Actions and Measure Results*, GAO-12-461 (Washington, D.C.: Apr. 26, 2012).

findings and conclusions based on our audit objectives; the framework also requires that we discuss any limitations in our work. We believe that the information, data, and evidence obtained and the analysis conducted provide a reasonable basis for our findings and conclusions based on our objectives.

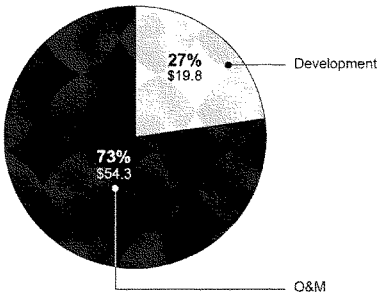
Background

OMB assists the President in overseeing the preparation of the federal budget submission and supervising budget administration in executive branch agencies. In helping to formulate the President's spending plans, OMB is responsible for evaluating the effectiveness of agency programs, policies, and procedures; assessing competing funding demands among agencies; and setting funding priorities. Further, the agency ensures that the budget submission is consistent with relevant statutes and presidential objectives.

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 $74 billion on IT investments in fiscal year 2013, which is the total expended for not only acquiring such investments, but also the funding to operate and maintain them. Of the reported amount, agencies plan to spend about $20 billion on development and acquisition, and $54 billion on O&M. Figure 1 shows the percentages of total planned spending for 2013.

Figure 1: Percentages of Planned IT Spending for Fiscal Year 2013

Dollars in billions



Source: OMB's IT Dashboard.

However, this $74 billion does not reflect the spending of the entire federal government. We have previously reported that OMB's figure understates the total amount spent in IT investments.[7] Specifically, it does not include IT investments by 58 independent executive branch agencies, including the Central Intelligence Agency, or by the legislative or judicial branches. Further, agencies differed on what they considered an IT investment; for example, some have considered research and development systems as IT investments, while others have not. As a result, not all IT investments are included in the federal government's estimate of annual IT spending. OMB provided guidance to agencies on how to report on their IT investments, but this guidance did not ensure complete reporting or facilitate the identification of duplicative investments. Consequently, we recommended, among other things, that OMB improve its guidance to agencies on identifying and categorizing IT investments.

To assist agencies in managing their IT investments, Congress enacted the Clinger-Cohen Act of 1996, which requires OMB to establish processes to analyze, track, and evaluate the risks and results of major capital investments in information systems made by federal agencies and

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

report to Congress on the net program performance benefits achieved as a result of these investments.[8] Further, the act places responsibility for managing investments with the heads of agencies and establishes chief information officers (CIO) to advise and assist agency heads in carrying out this responsibility.

Many of these investments are critical to our nation. For example, they include systems to process tax returns, secure our nation, and control aircraft.

However, the federal government has spent billions of dollars on poorly performing IT investments, as the following examples illustrate:

- In July 2010, OMB directed the National Archives and Records Administration (NARA) to halt development of its Electronic Records Archive system at the end of fiscal year 2011 (1 year earlier than planned). OMB cited concerns about the system's cost, schedule, and performance and directed NARA to better define system functionality and improve strategic planning. Through fiscal year 2010, NARA had spent about $375 million on the system. We issued several reports and made recommendations to improve this system.[9] These findings and recommendations contributed to the decision to halt the system.

- In January 2011, the Secretary of Homeland Security ended the Secure Border Initiative Network program after obligating more than $1 billion to the program because it did not meet cost-effectiveness and viability standards. Since 2007, we have identified a range of issues and made several recommendations to improve this

[8]40 U.S.C. § 11302(c).

[9]See, for example, GAO, *Electronic Records Archive: Status Update on the National Archives and Records Administration's Fiscal Year 2010 Expenditure Plan*, GAO-10-657 (Washington, D.C.: June 11, 2010); *Electronic Records Archive: The National Archives and Records Administration's Fiscal Year 2009 Expenditure Plan*, GAO-09-733 (Washington, D.C.: July 24, 2009); and *National Archives: Progress and Risks in Implementing its Electronic Records Archive Initiative*, GAO-10-222T (Washington, D.C.: Nov. 5, 2009).

program.[10] For example, in May 2010 we reported that the final acceptance of the first two deployments had slipped from November 2009 and March 2010 to September 2010 and November 2010, respectively, and that the cost-effectiveness of the system had not been justified.[11] We concluded that the Department of Homeland Security (DHS) had not demonstrated that the considerable time and money being invested to acquire and deploy the program was a wise and prudent use of limited resources. As a result, we recommended that the department (1) limit near-term investment in the first incremental block of the program, (2) economically justify any longer-term investment in it, and (3) improve key program management disciplines. This work contributed to the department's decision to cancel the program.

- In February 2011, the Office of Personnel Management canceled its Retirement Systems Modernization program after several years of trying to improve the implementation of this investment.[12] According to the Office of Personnel Management, it spent approximately $231 million on this investment. We issued a series of reports on the agency's efforts to modernize its retirement system and found that the Office of Personnel Management was hindered by weaknesses in several important management disciplines that are essential to

[10]See, for example, GAO, *Secure Border Initiative: DHS Needs to Strengthen Management and Oversight of Its Prime Contractor*, GAO-11-6 (Washington, D.C.: Oct. 18, 2010); *Secure Border Initiative: DHS Needs to Reconsider Its Proposed Investment in Key Technology Program*, GAO-10-340 (Washington, D.C.: May 5, 2010); *Secure Border Initiative: DHS Needs to Address Testing and Performance Limitations That Place Key Technology Program at Risk*, GAO-10-158 (Washington, D.C.: Jan. 29, 2010); *Secure Border Initiative: DHS Needs to Address Significant Risks in Delivering Key Technology Investment*, GAO-08-1086 (Washington, D.C.: Sept. 22, 2008); and *Secure Border Initiative: SBInet Expenditure Plan Needs to Better Support Oversight and Accountability*, GAO-07-309 (Washington, D.C.: Feb. 15, 2007).

[11]GAO, *Secure Border Initiative: DHS Needs to Reconsider Its Proposed Investment in Key Technology Program*, GAO-10-340 (Washington, D.C.: May 5, 2010).

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

successful IT modernization efforts.[13] Accordingly, we made recommendations in areas such as project management, organizational change management, testing, cost estimating, and earned value management. In May 2008, an Office of Personnel Management official cited the issues that we identified as justification for issuing a stop work order to the system contractor, and the agency subsequently terminated the contract.

- In March 2011, we reported that while the Department of Defense's (DOD) Navy Next Generation Enterprise Network investment's first increment was estimated to cost $50 billion, the program was not well-positioned to meet its cost and schedule estimates.[14] Accordingly, we recommended DOD limit further investment until it conducts an interim review to reconsider the selected acquisition approach and addresses its investment management issues. DOD stated that it did not concur with the recommendation to reconsider its acquisition approach, but we maintained that without doing so, DOD could not be sure it was pursuing the most cost-effective approach.

- In December 2012, DOD canceled the Air Force's Expeditionary Combat Support System after having spent more than a billion dollars and missing multiple milestones. We issued several reports on this system and found that, among other things, the program was not fully following best practices for developing reliable schedules and cost estimates.[15]

In addition to these poorly performing investments, the IT Dashboard identifies other at-risk investments. Specifically, as of August 2012,

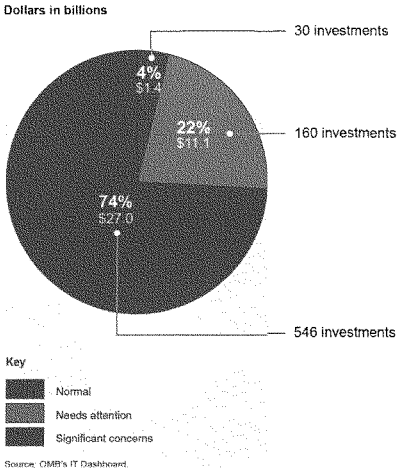
[13]GAO, *Office of Personnel Management: Retirement Modernization Planning and Management Shortcomings Need to Be Addressed,* GAO-09-529 (Washington, D.C.: Apr 21, 2009); *Office of Personnel Management: Improvements Needed to Ensure Successful Retirement Systems Modernization,* GAO-08-345 (Washington, D.C.: Jan 31, 2008); *Comments on the Office of Personnel Management's February 20, 2008 Report to Congress Regarding the Retirement Systems Modernization,* GAO-08-576R (Washington, D.C.: Mar 28, 2008); and *Office of Personnel Management: Retirement Systems Modernization Program Faces Numerous Challenges,* GAO-05-237 (Washington, D.C.: Feb 28, 2005).

[14]GAO-11-150.

[15]GAO, *DOD Business Transformation: Improved Management Oversight of Business System Modernization Efforts Needed,* GAO-11-53 (Washington, D.C.: Oct. 7, 2010) and *DOD Financial Management: Implementation Weaknesses in Army and Air Force Business Systems Could Jeopardize DOD's Auditability Goals,* GAO-12-134 (Washington, D.C.: Feb. 28, 2012).

according to the IT Dashboard, 190 of the federal government's approximately 700 major IT investments—totaling almost $12.5 billion—were in need of management attention (rated "yellow" to indicate the need for attention or "red" to indicate significant concerns). (See fig. 2.)

Figure 2: Overall Performance Ratings of Major Investments on the IT Dashboard, as of August 2012



Source: OMB's IT Dashboard.

OMB's Recent Major Initiatives for Overseeing IT Investments

As previously mentioned, in June 2009, to further improve the transparency into and oversight of agencies' IT investments, OMB publicly deployed the IT Dashboard. As part of this effort, OMB issued guidance directing federal agencies to report, via the Dashboard, the performance of their IT investments. Currently, the Dashboard publicly displays information on the cost, schedule, and performance of over 700 major federal IT investments at 26 federal agencies. Further, the public display of these data is intended to allow OMB, other oversight bodies,

and the general public to hold the government agencies accountable for results and progress.

In December 2010 OMB released its 25-point plan to reform federal IT. Among other things, the plan noted the goal of turning around or terminating at least one-third of underperforming projects by June 2012.

To its credit, OMB's IT Reform Plan provided specific actions to agencies so they could (1) more effectively manage IT acquisitions and (2) achieve operational efficiencies. To effectively manage IT acquisitions, the plan identified key actions such as improving accountability and governance and aligning acquisition processes with the technology cycle. To achieve operational efficiencies, the plan outlined actions required to adopt cloud solutions and leverage shared services. One of these actions was the consolidation of data centers as described in OMB's FDCCI, which was announced in February 2010 and included a high-level goal to reduce the cost of data center hardware, software, and operations. Another action that was identified was related to cloud computing. OMB developed a "Cloud First" policy that required each agency CIO to fully migrate three services to a cloud solution by June 2012, and implement cloud-based solutions whenever a secure, reliable, and cost-effective cloud option exists.

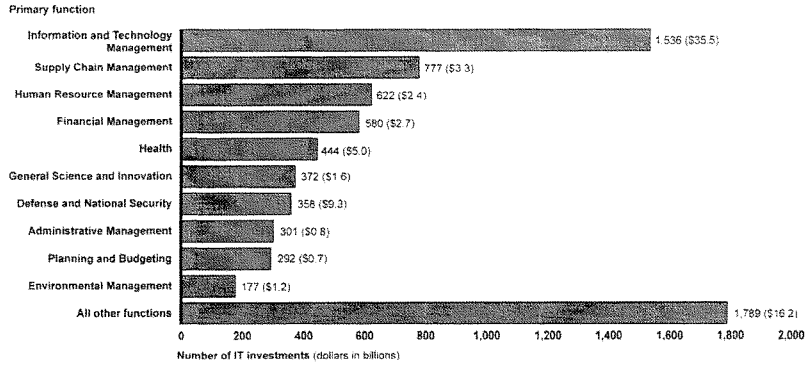
As part of the IT Reform Plan, in 2011 the Federal CIO Council launched an initial Best Practices platform on http://www.CIO.gov to provide agency case studies that demonstrate best practices in managing federal IT systems.[16] According to OMB, agencies have been encouraged to develop practices that focus on early, frequent, and constructive communication during the acquisition process so that the government clearly understands the marketplace and can obtain an effective solution at a reasonable price.

Further, since June 2010, OMB has required agencies to develop and carry out an operational analysis (OA) policy for examining the ongoing performance of existing operational IT investments to measure, among other things, whether the investment is continuing to meet business and customer needs and is contributing to meeting the agency's strategic goals. OMB's guidance calls for the policy to provide for an annual OA of each investment that addresses the following: cost, schedule, customer satisfaction, strategic and business results, financial goals, and innovation.

[16]Federal CIO Council, http://cio.gov/category/best-practices/.

More recently, the Federal CIO initiated the PortfolioStat effort for commodity IT in March 2012. OMB requires agency Deputy Secretaries or Chief Operating Officers to lead PortfolioStats—IT portfolio reviews—working in coordination with CIOs, Chief Financial Officers, and Chief Acquisition Officers. Such an effort, as planned, is appropriate given the numerous investments performing the same function, as we reported in February 2012.[17] For example, 27 major federal agencies planned to spend $2.7 billion on 580 financial management systems in 2011. See figure 3 for the total number of investments within the 27 federal agencies, by function.

Figure 3: Number of Government IT Investments by Primary Function, as of July 2011



Source: GAO analysis of exhibit 53 data.

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.

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

We previously reported and testified on the issue of duplicative IT investments at DOD and the Department of Energy.[18] Specifically, we found 37 potentially duplicative investments, accounting for about $1.2 billion in total IT spending for fiscal years 2007 through 2012. We made recommendations to those agencies to report on the progress of efforts to identify and eliminate duplication, where appropriate.

Opportunities Exist to Improve Acquisitions and Operations of IT Investments

Over the past several years, we have highlighted OMB efforts to enhance oversight of IT acquisition. Most notably, we issued a series of reports on the IT Dashboard. In addition, we identified common factors critical to successful IT investments.

IT Dashboard

OMB has taken significant steps to enhance the oversight, transparency, and accountability of federal IT investments by creating its IT Dashboard, and by improving the accuracy of investment ratings. However, there were issues with the accuracy and reliability of cost and schedule data, and we recommended steps that OMB should take to improve these data.

- Our July 2010 report[19] found that the cost and schedule ratings on OMB's Dashboard were not always accurate for the investments we reviewed, because these ratings did not take into consideration current performance. As a result, the ratings were based on outdated information. We recommended that OMB report on its planned changes to the Dashboard to improve the accuracy of performance information and provide guidance to agencies to standardize milestone reporting. OMB agreed with our recommendations and, as a result, updated the Dashboard's cost and schedule calculations to include both ongoing and completed activities. Similarly, in March 2011, OMB had initiated several efforts to increase the Dashboard's value as an oversight tool, and had used its data to improve federal IT

[18]GAO-12-241 and GAO, *Information Technology: Potentially Duplicative Investments Exist at the Departments of Defense and Energy*, GAO-12-462T (Washington, D.C.: Feb. 17, 2012).

[19]GAO, *Information Technology: OMB's Dashboard Has Increased Transparency and Oversight, but Improvements Needed*, GAO-10-701 (Washington, D.C.: July 16, 2010).

management.[20] However, agency practices and the Dashboard's calculations contributed to inaccuracies in the reported investment performance data. These included, for instance, missing data submissions or erroneous data at each of the five agencies we reviewed, along with instances of inconsistent program baselines and unreliable source data. As a result, we recommended that the agencies take steps to improve the accuracy and reliability of their Dashboard information, and that OMB improve how it rates investments relative to current performance and schedule variance. Most agencies generally concurred with our recommendations; OMB agreed with our recommendation for improving ratings for schedule variance. It disagreed with our recommendation to improve how it reflects current performance in cost and schedule ratings, but more recently made changes to Dashboard calculations to address this while also noting challenges in comprehensively evaluating cost and schedule data for these investments.

- Our subsequent report[21] noted that that the accuracy of investment cost and schedule ratings had improved since our July 2010 report because OMB had refined the Dashboard's cost and schedule calculations. Most of the ratings for the eight investments we reviewed were accurate, although more could be done to inform oversight and decision making by emphasizing recent performance in the ratings. We recommended that the General Services Administration comply with OMB's guidance for updating its ratings when new information becomes available (including when investments are rebaselined) and the agency concurred. Since we previously recommended that OMB improve how it rates investments, we did not make any further recommendations.

- More recently, in October 2012 we found that opportunities existed to improve transparency and oversight of investment risk at our selected agencies.[22] Specifically, CIOs at six federal agencies consistently rated the majority of their IT investments as low risk. These agencies rated no more than 12 percent of their investments as high or

[20]GAO, *Information Technology: OMB Has Made Improvements to Its Dashboard, but Further Work Is Needed by Agencies and OMB to Ensure Data Accuracy,* GAO-11-262 (Washington, D.C.: Mar. 15, 2011).

[21]GAO, *IT Dashboard: Accuracy Has Improved, and Additional Efforts Are Under Way to Better Inform Decision Making,* GAO-12-210 (Washington, D.C.: Nov. 7, 2011).

[22]GAO-13-98.

moderately high risk, and two agencies (DOD and the National Science Foundation) rated no investments at these risk levels. Over time, about 47 percent of the agencies' Dashboard investments received the same rating in every rating period. For ratings that changed, DHS and Office of Personnel Management reported more investments with reduced risk when initial ratings were compared with those in March 2012; the other four agencies reported more investments with increased risk. In the past, OMB reported trends for risky IT investments needing management attention as part of its annual budget submission, but discontinued this reporting in fiscal year 2010. Accordingly, we recommended OMB analyze agencies' investment risk over time as reflected in the Dashboard's CIO ratings and present its analysis with the President's annual budget submission, with which OMB concurred.

Further, agencies generally followed OMB's instructions for assigning CIO ratings, which included considering stakeholder input, updating ratings when new data become available, and applying OMB's six evaluation factors. DOD's ratings were unique in reflecting additional considerations, such as the likelihood of OMB review, and consequently DOD did not rate any of its investments as high risk. However, in selected cases, these ratings did not appropriately reflect significant cost, schedule, and performance issues reported by GAO and others. Although three DOD investments experienced significant performance problems and were part of a GAO high-risk area (business systems modernization), they were all rated low risk or moderately low risk by the DOD CIO. For example, in early 2012, we reported that Air Force's Defense Enterprise Accounting and Management System (DEAMS) faced a 2-year deployment delay and an estimated cost increase of about $500 million from an original life-cycle cost estimate of $1.1 billion (an increase of approximately 45 percent), and that assessments by DOD users had identified operational problems with the system, such as data accuracy issues, an inability to generate auditable financial reports, and the need for manual workarounds.[23] In July 2012, the DOD Inspector General reported that the DEAMS's schedule delays were likely to diminish the cost savings it was to provide, and would jeopardize the department's goals for attaining an auditable financial statement. DOD's CIO rated

[23]GAO, *DOD Financial Management: Reported Status of Department of Defense's Enterprise Resource Planning Systems,* GAO-12-565R (Washington, D.C.: Mar. 30, 2012) and GAO-12-134.

DEAMS low risk or moderately low risk from July 2009 through March 2012.

Moreover, DOD did not apply its own risk management guidance to the ratings, which reduces their value for investment management and oversight. Therefore, we recommended that DOD ensure that its CIO ratings reflect available investment performance assessments and its risk management guidance. DOD concurred with our recommendation.

Critical Factors Underlying Successful Major Acquisitions

To help the federal agencies address the well-documented acquisition challenges they face, we identified seven successful investment acquisitions and nine common factors critical to their success in 2011.[24] Specifically, we reported that department officials identified seven successful investment acquisitions, in that they best achieved their respective cost, schedule, scope, and performance goals.[25] The nine common factors critical to the success of three or more of the seven investments were: (1) program officials were actively engaged with stakeholders; (2) program staff had the necessary knowledge and skills; (3) senior department and agency executives supported the programs; (4) end users and stakeholders were involved in the development of requirements; (5) end users participated in testing of system functionality prior to formal end user acceptance testing; (6) government and contractor staff were stable and consistent; (7) program staff prioritized requirements; (8) program officials maintained regular communication with the prime contractor; and (9) programs received sufficient funding. Further, officials from all seven investments cited active engagement with program stakeholders as a critical factor to the success of those investments. These critical factors support OMB's objective of improving the management of large-scale IT acquisitions across the federal government, and wide dissemination of these factors could complement OMB's efforts.

[24]GAO-12-7.

[25]The seven investments were (1) Commerce's Decennial Response Integration System, (2) DOD's Defense Global Combat Support System-Joint (Increment 7), (3) Department of Energy's Manufacturing Operations Management Project, (4) DHS's Western Hemisphere Travel Initiative, (5) Department of Transportation's Integrated Terminal Weather System, (6) Internal Revenue Service's Customer Account Data Engine 2, and (7) Veterans Affairs Occupational Health Record-keeping System.

In addition to efficiently acquiring IT investments, it is also important for the federal government to efficiently manage operational investments, especially since agencies are planning to spend about $54 billion in fiscal year 2013 on operational systems. Accordingly, we issued key reports on the federal government's oversight of IT investments in O&M, progress toward meeting OMB data center consolidation goals, and progress toward cloud computing as specified in the "Cloud First" policy.

Oversight of Investments in O&M

While agencies spend billions on operational investments, they have not always provided adequate oversight of these investments. Specifically, assessments of the performance of such investments—commonly referred to as OAs—varied significantly, as we reported in October 2012.[26] OMB guidance calls for agencies to develop an OA policy and perform such analyses annually to ensure O&M investments continue to meet agency needs. The guidance also includes 17 key factors (addressing areas such as cost, schedule, customer satisfaction, and innovation) that are to be assessed.

We reviewed five agencies[27] and found that they varied in the extent to which they followed OMB guidance. For example, DHS and HHS developed a policy which included all OMB assessment factors and performed OAs. However, they did not include all investments and key factors. In particular, DHS analyzed 16 of its 44 steady state investments, meaning 28 investments with annual budgets totaling $1 billion were not analyzed; HHS analyzed 7 of its 8 steady state investments. For OAs performed by DHS and HHS, both fully addressed approximately half of the key factors. In contrast, DOD, Treasury, and VA did not develop a policy and did not perform analyses on their 23 major steady state investments with annual budgets totaling $2.1 billion. Overall, these five agencies have steady state investments with a fiscal year 2011 budget of over $3 billion that had not undergone needed analyses, and while OMB called for agencies to perform OAs, its existing guidance did not provide mechanisms that ensure the OAs are completed and allow public transparency into the results of the assessments. As a result, we recommended that DOD, Treasury, and VA develop an OA policy and conduct annual OAs; DHS and HHS ensure OAs are being performed for

[26]GAO-13-87.

[27]The agencies in our review were DHS, DOD, the Departments of Health and Human Services (HHS), the Treasury, and Veterans Affairs (VA).

all investments and that all factors are fully assessed; and OMB revise its guidance to include directing agencies to report on the IT Dashboard the results from the OAs. The five agencies and OMB agreed with our recommendations.

Data Center Consolidation

Agencies have developed plans to consolidate data centers; however, these plans were incomplete and did not include best practices. We issued two reports on the federal government's effort to consolidate data centers and made several recommendations for improvements.

- Our July 2011 report found that agency consolidation plans indicated that agencies anticipated closing about 650 data centers by fiscal year 2015 and saving about $700 million in doing so.[28] However, only one of the 24 agencies submitted a complete inventory and no agency submitted complete plans. Further, OMB did not require agencies to document the steps they took, if any, to verify the inventory data. We noted the importance of having assurance as to the accuracy of collected data and, specifically, the need for agencies to provide OMB with complete and accurate data and the possible negative impact of that data being missing or incomplete. We concluded that until these inventories and plans were completed, agencies would not be able to implement their consolidation activities and realize expected cost savings. Moreover, without an understanding of the validity of agencies' consolidation data, OMB could not be assured that agencies were providing a sound baseline for estimating consolidation savings and measuring progress against those goals. Accordingly, we made several recommendations to OMB, including that the Federal CIO require that agencies, when updating their data center inventories, state what actions have been taken to verify the inventories and to identify any associated limitations on the data.

- In a subsequent report[29] we noted that agencies updated their inventories and plans, but key elements were still missing. Specifically, as of September 2011, 24 agencies identified almost 2,900 total centers, established plans to close 1,186 of them by 2015, and estimated they would realize over $2.4 billion in cost savings in doing so. OMB noted that the savings would be even greater and

[28]GAO, *Data Center Consolidation: Agencies Need to Complete Inventories and Plans to Achieve Expected Savings*, GAO-11-565 (Washington, D.C.: July 19, 2011).

[29]GAO-12-742.

estimated that FDCCI would realize $3 billion in savings by 2015.[30] However, while OMB required agencies to complete missing elements in their data center inventories and plans by the end of September 2011, only 3 agencies submitted complete inventories, and only 1 agency submitted a complete plan. Further, in their consolidation plans, 13 agencies did not provide a full master program schedule, and 21 agencies did not fully report their expected cost savings. Our report noted that until these inventories and plans were complete, agencies would continue to be at risk of not realizing anticipated savings, improved infrastructure utilization, or energy efficiency. We also reiterated our recommendation that the agencies complete the missing elements of their inventories and plans.

In addition, while OMB required a master program schedule and a cost-benefit analysis (a type of cost estimate) as key requirements of agencies' consolidation plans, none of the five agencies we reviewed had a schedule or cost estimate that was fully consistent with the four selected attributes of a properly sequenced schedule (such as having identified dependencies) or the four characteristics that form the basis of a reliable cost estimate (such as being comprehensive and well-documented). OMB had established a standardized cost model to aid agencies in their consolidation planning efforts, but use of the model was voluntary. As a result, we recommended that the five selected agencies should implement recognized best practices when establishing schedules and cost estimates for their consolidation efforts and that OMB ensure agencies utilize its standardized cost model across the consolidation initiative. OMB and three agencies agreed with our recommendation, and two did not agree or disagree with it.

Finally, we highlighted consolidation successes, such as the benefits of focusing on key technologies and the benefits of working with other agencies and components to identify consolidation opportunities. However, agencies continued to report a number of the same challenges that we first described in 2011, while other challenges were evolving. For example, 15 agencies reported continued issues with obtaining power usage information, and 9 agencies reported that their organization continued to struggle with acquiring the funding required for consolidation. In light of these successes and challenges, we noted that it was important for OMB to continue to provide

[30]OMB, *Analytical Perspectives, Budget of the U.S. Government, Fiscal Year 2013.*

leadership and guidance, such as—as we previously recommended—using the consolidation task force to monitor agencies' consolidation efforts. Therefore, we recommended that OMB ensure that all future revisions to the guidance on data center consolidation inventories and plans are defined in an OMB memorandum and posted to the FDCCI public website in a manner consistent with the guidance published in 2010. OMB agreed with our recommendation.

Cloud Computing

Implementing cloud computing has security implications, which federal agencies began addressing. Further, agencies made progress implementing OMB's "Cloud First" policy. We reported on these two issues and made recommendations.

- In May 2010, we reported that cloud computing can both increase and decrease the security of information systems in federal agencies.[31] Risks included dependence on the security practices and assurances of a vendor, dependency on the vendor, and concerns related to sharing of computing resources. Federal agencies had begun efforts to address information security issues for cloud computing, but key guidance was lacking and efforts remained incomplete. Although individual agencies had identified security measures needed when using cloud computing, they had not always developed corresponding guidance. For example, only nine agencies reported having approved and documented policies and procedures for writing comprehensive agreements with vendors when using cloud computing. Agencies had also identified challenges in implementing existing federal information security guidance and the need to streamline and automate the process of implementing this guidance. These concerns included having a process to assess vendor compliance with government information security requirements and the division of information security responsibilities between the customer and vendor. Among other things, we recommended that OMB establish milestones for completing a strategy for implementing the federal cloud computing initiative.

- Federal agencies made progress in implementing OMB's "Cloud First" policy, as we reported in July 2012.[32] Consistent with this policy, each

[31]GAO, *Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing*, GAO-10-513 (Washington, D.C.: May 27, 2010).

[32]GAO, *Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned*, GAO-12-756 (Washington, D.C.: July 11, 2012).

of the seven agencies in our review incorporated cloud computing requirements into their policies and processes. Further, each of the seven agencies met the OMB deadlines to identify three cloud implementations by February 2011 and to implement at least one service by December 2011. However, two agencies did not plan to meet OMB's deadline to implement three services by June 2012, but planned to do so by calendar year's end. Each of the seven agencies also identified opportunities for future cloud implementations, such as moving storage and help desk services to a cloud environment. While each of the seven agencies submitted plans to OMB for implementing the cloud solutions, all but one plan were missing key required elements. As a result, we recommended that the seven agencies develop key planning information, such as estimated costs and legacy IT systems' retirement plans, for existing and planned services. The agencies generally agreed with these recommendations.

IT Reform Plan

OMB's IT Reform Plan acknowledged many of these acquisition and operation issues by requiring 25 actions to be completed by 2012. For example, it required agencies to launch a best practices collaboration platform and shift to a "Cloud First" policy. We reported on the federal government's progress toward implementing these actions in April 2012.[33] OMB and key federal agencies had made progress on action items in the IT Reform Plan, but there were several areas where more remained to be done. Specifically, we reviewed 10 actions and found that 3 were complete:

- stand-up contract vehicle for infrastructure,
- reform and strengthen investment review boards, and
- design a cadre of specialized IT acquisition professionals.

Additionally, 7 items were partially completed:

- complete plans for data center consolidation,
- issue guidance on modular development,
- shift to a "Cloud First" policy,
- work with Congress to create budget models for modular development,
- work with Congress to consolidate routine IT purchases under agency CIO,
- launch a best practices platform, and

[33]GAO-12-461.

- redefine the role of agency CIO and CIO Council.

OMB reported greater progress than we determined. While OMB officials acknowledged that there is more to do in each of the topic areas, they considered the key action items to be completed because the IT Reform Plan has served its purpose as a catalyst for a set of broader initiatives. They explained that work will continue on all of the initiatives even after OMB declares that the related action items are completed under the IT Reform Plan. We disagreed with this approach and noted that in prematurely declaring the action items to be completed, OMB risked losing momentum on the progress it has made to date. We recommended that three agencies complete key IT Reform action items. We also recommended that OMB accurately characterize the status of the IT Reform Plan action items in the upcoming progress report in order to keep momentum going on action items that are not yet completed.

Further, OMB and key agencies planned to continue efforts to address the seven items that we identified as behind schedule, but lacked time frames for completing most of them. For example, OMB had planned to work with congressional committees during the fiscal year 2013 budget process to assist in exploring legislative proposals to establish flexible budget models and to consolidate certain routine IT purchases under agency CIOs. However, OMB had not established time frames for completing five of the seven IT Reform Plan action items that were behind schedule. Accordingly, we recommended that OMB ensure that the action items called for in the IT Reform Plan be completed by the responsible parties prior to the completion of the IT Reform Plan's 18-month deadline of June 2012, or if the June 2012 deadline could not be met, by another clearly defined deadline; and provide clear time frames for addressing the shortfalls associated with the action items.

Last, OMB had not established performance measures for evaluating the results of most of the IT reform initiatives we reviewed. Specifically, OMB established performance measures for 4 of the 10 action items, including data center consolidation and cloud computing. However, no performance measures existed for 6 other action items, including establishing the best practices collaboration platform and developing a cadre of IT acquisition professionals. Thus, we recommended that OMB establish outcome-oriented measures for each applicable action item.

In summary, OMB's and agencies' recent efforts have resulted in greater transparency and oversight of federal spending, but continued leadership and attention is necessary to build on the progress that has been made.

For example, federal agencies need to continue to improve the accuracy of information on the Dashboard to provide greater transparency and even more attention to the billions of dollars invested in troubled projects. Further, the expanded use of the common factors critical to the successful management of large-scale IT acquisitions should result in the more effective delivery of mission-critical systems. In addition, the federal government can more efficiently manage operational systems by ensuring the $54 billion in O&M is continuing to improve mission performance, in particular the $3 billion which had not undergone required analyses. The federal government can also build on the momentum of the $2.4 billion in estimated savings as a result of data center consolidation efforts. Overall, implementation of outstanding GAO recommendations can help further reduce wasteful spending on poorly managed, unnecessary, and duplicative investments.

Chairman Issa, Ranking Member Cummings, and Members of the Committee, this concludes my statement. I would be pleased to answer any questions at this time.

GAO Contact and Staff Acknowledgments

If you should have any questions about this testimony, please contact me at (202) 512-9286 or by e-mail at pownerd@gao.gov. Individuals who made key contributions to this testimony are Dave Hinchman, Assistant Director; Gary Mountjoy, Assistant Director; Rebecca Eyler; Kevin Walsh; and Shawn Ward.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
Connect with GAO	Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Website: http://www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Please Print on Recycled Paper.

Chairman ISSA. For all the members, be aware that somewhere in the 2 o'clock time range we will have our first and only series of votes for the day. It will be no more than three votes, and we will return immediately following that. I will go down the order normally, but if somebody is here ahead of you, then I will go to that person first and then return to the normal order.

Mr. Powner, I guess the first problem we seem to have is that the software for the IT Dashboard is not performing properly, if I heard you say, that in fact what we are getting there in reporting, granted it is not automated reporting, but that reporting is not factual. In a nutshell, how do we fix that? How do we get that reporting to fairly reflect the real green, red, yellow that we should?

Mr. POWNER. Well, Mr. Chairman, there is reporting on cost and schedule performance, but there is a key report on CIO assessment and that doesn't require the software to function. That requires the CIO to be on top of their projects and to accurately report. So we issued a report late last year that highlighted some of the problems.

We have some departments and agencies reporting accurately. DOD reported zero red investments, and that was soon after they cancelled the one investment that you highlighted in the opening to the hearing here. So we need to make sure that we get accurate reporting, that CIOs are on top of the status of these 700 major IT investments.

Chairman ISSA. Let me follow up briefly. There is 243 CIOs. Only one has full budget authority, and that is Veterans Affairs. Do you see a difference between the one and the 242 in the sense of accountability? I know that is a very small offsetting number. We don't have a second example. But can you give us a contrast that you think budget responsibility and authority can bring?

Mr. POWNER. Clearly budget authority helps with your authorities, but there is also some CIOs in the Federal government, I can point to several examples, where even without budget authority they are still quite successful. And some areas, if you look at IRS as an example, over the years they have greatly improved. Their chief information, chief technology officer there gets a lot done, gets it done well. DHS is another good example where even without budget authority they still can be quite successful.

Chairman ISSA. Before I move on, this committee has a long history of bringing people in when they screw up. How do I do what you just did? How do I find the areas of excellence, identify them and recognize them? And not just I, I mean our Government. Because certainly we do have, and I have met many of them, these information officers that are doing an excellent job that are on top of it, but out of 243 clearly some are not.

Mr. POWNER. Well, you know, I mentioned a few agencies that are performing better than others, but clearly Steve VanRoekel has the best picture into who those stronger CIOs are across the Federal government. He meets with them frequently in many of his initiatives, he has seen them firsthand, in addition to our work at GAO. But he has much more hands-on working experience and I would rely heavily on him.

Chairman ISSA. Then I will go to the gentleman. Can you give me your best and brightest and tell me how I leverage the acco-

lades to them so that the others will realize that excellence is rewarded?

Mr. VANROEKEL. I am happy to provide names and lots of examples of best practices that we have done.

Chairman ISSA. We will take them.

Mr. VANROEKEL. We are taking this direction and actually institutionalizing a lot of this work in the CIO Council. We have stood up an effort this year to immortalize best practice sharing in a way that really has never been done before, putting examples of best case around procurement, around implementation of different technologies and things like that, as well as starting a CIO university that we bring new CIOs that are entering the Government to bear to consume our handbook, hear from the better CIOs on how to get best results and things like that.

Chairman ISSA. By the way, who is the IRS CIO that you mentioned?

Mr. POWNER. Terry Milholland. He goes by CTO, but in fact he is their chief information officer.

Chairman ISSA. Excellent. I am going to just touch on a couple of areas. Ms. Duckworth actually brought this to me, so sometimes the most important questions are from freshmen.

I have been in Congress for 12 years. Before I was in Congress I worked on a voluntary basis for my county. So as far back as about 16 years ago I was acutely aware that we put a lot of money into interoperable systems so that our counties, our cities, our fire departments and so on could communicate, particularly in times of emergencies, which San Diego tends to have a fire, a major fire every year or two. It is now more than a decade later and these systems are generally no better. Additionally, we reported in fiscal year 2011 we funded 622 separate human resource systems at a cost of $2.4 billion.

The frustration that I have, the frustration the gentlelady has from Illinois is how do we stop looking at things 6 years, 10 years, 20 years later and find out that what we said the job was to consolidate, the job was to go to a single interoperable system and so on, just as we are doing here today, how do we stop it from expanding? Because I am sure that we are not 622 separate human resource systems, and I know for a fact that the systems used by fire and emergency operations around my State at least are not 14 years old. They are systems that don't talk to each other that were bought after we recognized the problem.

Mr. VanRoekel?

Mr. VANROEKEL. I think a primary way to think about this is if you look at the history of technology and the way it grew up, even in the private sector, and I was, as I mentioned in my opening statement, in high-tech in the private sector for 20 years, most of that at Microsoft Corporation, so I saw a lot of evolution in this space.

The industry grew up in a way that was very single purpose, where it was unthinkable on a server to install multiple kinds of software. You would just put an e-mail on one, a database on another and things like that. There is now technology available that allows us to do things massively different.

I think the private sector has realized that. As Mr. Davis said in his opening statement, there is this inflection point we all go through where technology is seen as this very discretionary thing to a very strategic thing, as you mentioned, the way to connect to customers or sales people or data, things like that. We are in the midst of that inflection point in government and it hasn't been fully realized. And I think that, coupled with the cost pressure, the cybersecurity pressure, and probably most importantly the expectations of citizens, are going to drive a different behavior.

What I have probably noticed the most coming into government is that we spend a lot of time focusing on a single role, saying a CIO kind of owns this function, procurement professional owns this function, CFO, human resources, et cetera. And one of the things I am working very hard to instill is across C-level conversation on these things.

When I ran the PortfolioStat process last summer, my agenda with that process was not just to look at the IT portfolio and sort of have an assessment there, but it was to get people around the table and teach from the deputy secretary and all the C-level executives how to run a private sector investment review board meeting, how to actually take a look at all the levers they can pull and how to make this strategic. So our initial goal was really consolidation at that level, saying it is unthinkable to run more than one email system if you are in an agency, and many are running more than one. It is unthinkable to run more than one other system. And so encouraging them to drive that level of consolidation.

And then Joseph Jordan and I, the head of the Office of Federal Procurement Policy, worked last year and launched the Strategic Sourcing Leadership Council that is a group of C-level executives from some of the largest agencies in government representing the majority of our IT spend who are right now working on a plan to do a minimum of those 15 systems of consolidations. They are going to be reporting back to us in the next month or two.

Chairman ISSA. Thank you.

Mr. Cummings.

Mr. CUMMINGS. Thank you very much. Mr. Chairman, I am glad you asked Mr. Powner about the person at IRS that apparently is doing it right. That is a good thing. I think it is important that we highlight those people who come in and do the right thing and do it well.

And that leads me to you, Mr. VanRoekel. When you were talking about best practices and trying to put them into policy, are we getting—you know, a lot of times people try to guard their little turf. They feel like they are doing everything right. And maybe they have been there for a while and they see somebody like Terry McMillan, is it? What was the name? Terry?

Mr. VANROEKEL. Milholland.

Mr. CUMMINGS. Milholland come along and they are resistant. Do you find that to be a problem at all?

Mr. VANROEKEL. Definitely we have many challenges in government around moving the ball forward, embracing innovation. I often will call it blinking light syndrome, where people just love to own their own servers and have their own thing, where they like the blinking lights of those servers. Culture is an inhibitor. Past

behavior and people saying, well, that is the way we have always done it, I assume that is the way we should always do it in the future, is definitely a challenge we see.

Mr. CUMMINGS. Are we getting the skills? Several people have mentioned skill levels of people coming in. Are we getting the kind of skilled people that we need to do the job? Because certainly if you don't have the skills, you can be the blind leading the blind and losing money and effectiveness at the same time. I am just wondering. And if we are not getting those kind of people, how do we go about getting them?

Mr. VANROEKEL. In my many years in the private sector, including a stint as Bill Gates' assistant and being by his side and seeing some of the most fascinating, amazing people in the technology field, probably the biggest surprise I have had coming to government is the quality of some of the people in government. And you find many of them around government who are either yearning or doing things in amazingly innovative ways.

A lot of times it is about giving those people permission, and I think that is the essence of good policy, is giving them a permission slip to go innovate, to break the culture of the way things have done in the past and move forward. I often hear from people after I have issued some policy around doing something massively differently than we have done before, they run around their agency holding that in the air saying, see, I can now do what I have been wanting to do, and that is creating a nice dynamic.

We have also got, you know, there are people that have been in government a long time, haven't maybe been trained to the level of 21st-century ways of doing things, and we have worked really hard to build new training mechanisms for them. And probably the most impactful thing we have done in the last year is we have launched what is called the Presidential Innovation Fellows Program that actually does rotations of private sector professionals in a non-conflicted way into government to work side-by-side with public sector employees to work on innovation challenges that the country is facing, but more importantly teach them how to do things in a 21st-century way. And that has beared incredible fruit.

Mr. CUMMINGS. One of my concerns is cybersecurity. Do you believe that the updates to FISMA might help OMB and DHS in your efforts to ensure that the government information is protected from cyber attacks?

Mr. VANROEKEL. I think the essence of what we need to do is really about flexibility. Cybersecurity threats are evolving every day. New technology, new devices present new threats. And having a mechanism like FISMA where you only do assessments on a not very regular basis is a good check and balance, but it is not the ultimate solution. And so I am probably most encouraged about our work in the continuous monitoring areas that we funded last year and are now starting to roll out this year. And this is a great highlight of across-government shared service where a procurement went out that is going to allow not only the Federal government to take advantage, but State, local and tribal are also eligible for this procurement to get volume and scale in our buying power, to actually look at a consistent view of cybersecurity threat monitoring across the government.

Mr. CUMMINGS. My last question is you recently said that you are encouraging agencies to evaluate the mission of their agencies when evaluating how they will cut their budgets if Congress does not pass legislation in time to avoid sequestration, and this is what you said, and I quote. "Cybersecurity is a top priority. When people are making the right priorities to meet the mission of the agencies in the most safe, secure and protecting citizens' privacy way, we will make the right trade-offs I think to assure that this is happening." And that is the end of the quote.

How could budget cuts impact cybersecurity initiatives and how much do you worry about that?

Mr. VANROEKEL. Well, I definitely worry about cybersecurity all the time, and it is something we have to be ever vigilant on, no matter what the budget situation is. And certainly budget cuts may have some impact, unforeseen impact on that. But the cybersecurity is a unique category of spend because it is in everything we do. It is not just one line item on the balance sheet. It is something that we look at and think about. Across, you know, from your mobile device to your desktop to your server room to your data center and everywhere in between, cybersecurity is a factor. So as agencies are looking at possible budget cuts, they have to look across that landscape and say, if I cut this program, this element of cyber that is associated with it may go away and does that change the dynamic on what our cyber stance is. It certainly could be that case, and we hope that is to be avoided.

Mr. CUMMINGS. Thank you very much.

Mr. MICA. [presiding.] Thank the gentleman.

What we are going to do is they have called a vote, and I guess we have about 12, 13 minutes. So I would like to ask a few questions. We probably have time for one more on this side to be fair. We go in order of seniority. And then we will come back and pick up where we left off and the witnesses will return.

Does staff know how many votes there are? Three votes. So it will probably be almost a half-hour.

So with that, let me just ask a couple of questions, recognize myself. Usually the components you need to be successful are policy or a law in place, and then you have to have the personnel to execute it, and then you have to buy the right IT equipment to make this stuff work.

My first question would be, are there changes in law that you would recommend that do not give you the ability to be successful?

Mr. VANROEKEL. I think there is definitely room within the existing law on the policy side, implementation of people side, that definitely allow us the flexibility to be successful. I think the fact that we have——

Mr. MICA. So within existing law you have the authority by law and ability to do what you need to do to be successful?

Mr. VANROEKEL. I do believe so. The challenge I think we face is probably around budgeting and thinking about how do we—and I know this is not an appropriations hearing—but how from a budget standpoint are IT dollars spent. One of our inhibitors I think on implementation of IT is that oftentimes for most agencies it is single-year spend, and without being able to extend that——

Mr. MICA. Well, then there is something missing, too, because you said you have people who have great ideas, very great capabilities, but they don't proceed. So somewhere they are not getting the policy which would either be set from your level, which you just said when you give them the authority they run around with the paper. So somewhere we are missing the ability to move forward.

The second thing, Mr. Powner, on the IRS, you mentioned IRS, and we get into personnel. And Mr. Cummings I think mentioned this too. You have got to have the best personnel. You said we have many of them, but sometimes we have turnover, we don't keep them or we don't attract them.

When this committee worked on some reform of IRS, years ago I worked on that, one of the problems we had, we had these very expensive IT systems and computer, massive operations, but we weren't retaining, able to recruit or maintaining and keeping folks that could do this work. We came back and changed the parameters of being able to hire people. Sometimes in the private sector you can make three and four times what we were paying them. So do we have the ability to hire people and pay them and retain them, from your experience?

Mr. POWNER. Yeah, IRS is a good example. And you are right, they were the poster child for years, and then there was a fair amount of congressional interaction and there was critical positions pay granted at IRS, and a number of those positions were granted towards the IT professionals. So their pay was bumped up. And then also when you mention about continuity of leadership, over the last nine years they have had two CIOs. One was there for 4 years, he is the current CIO at DHS, and the current one has been there for more than 4. So the turnover is a big deal.

Mr. MICA. I know we did that for IRS, and I know I worked on something for a CFO actually in Transportation because we couldn't get one or retain one. Government-wide, though, do we still have a problem as far as this personnel issue and the flexibility to retain and pay people?

Mr. POWNER. Turnover is a big deal, because currently I think the average CIO, it is around 2 years and they are in and out, and that varies a little bit depending on how you break it down by political appointees and career, but not much. But on average it is about a 2-year turnover.

Mr. MICA. What do you think, Mr. VanRoekel?

Mr. VANROEKEL. Yeah, I think there is quite a bit of turnover. But the essence of a lot of what we try to do is institutionalize best behavior and best practices in a way that will kind of mitigate some of the turnover.

Mr. MICA. We can look at that. And then if you said DOD has $2.2 billion worth of potential savings, is that what you said, identified?

Mr. POWNER. Yes. That was when you look at their data center consolidation efforts, their current plan projects $2.2 billion in savings.

Mr. MICA. And why isn't that moving forward, or is it?

Mr. VANROEKEL. It is moving forward. In their last public budget submission, they represented I think around or slightly over $300 million in saving.

Mr. MICA. But the balance of the Federal government is $3 billion identified in savings. That billion just beyond defense doesn't seem realistic. I think there is probably a lot more room, wouldn't you agree?

Mr. VANROEKEL. I think we are at the tip of the iceberg on some of this, yes.

Mr. MICA. Okay. And finally, maybe for the committee you could submit—now, I am fascinated by Obamacare. I just came from Transportation, government buildings. They came to us. I guess we passed the law that allowed them to acquire a building to house 5,000 bureaucrats, just the folks that are going to be administrating Obamacare. I am interested to know, they are going to have to set up IT systems and everything, maybe you could provide the committee with information that you have on where they are going with that.

This is going to be a huge agency, a huge operation and requiring a lot of IT investment. Maybe you could share that with the committee. I will ask you. You don't have to respond.

Mr. MICA. Mrs. Maloney?

Mrs. MALONEY. First of all, thank you very much. I want to ask a question about the Office of Financial Research, which was created under Dodd-Frank, and the purpose of it was to have the authority to collect data across the industry to look for systemic risk. So when you are talking about these data systems, they are put in place in many ways to save money. So taking out elements of them and whatever may hinder their ability, obviously if we had had such a system that could have foreseen the systemic risk and taken steps to prevent the subprime crisis and other credit default swaps and other instruments that were rocking our economy. I want to note that the chairman and I during this committee did a series of amendments trying to really legislate parts of the Office of Financial Research, so this is a bipartisan effort.

But my question is, what factors go into determining which data centers will be closed? Certainly someone thought they were important to begin in the first place. And if you do close one, is there an appeal process where the agency or others can say you are telling us to close three data systems, but these are three or four elements that we think are going to save money in the long run, save lives or prevent financial crises.

So how is that happening? Obviously you could go in and say, well, close down all the data systems, we are going to save money. But actually they are put in place for many reasons, one of which is to save money and to manage government better.

Mr. VANROEKEL. Right. This is the essence of why I like to focus on data center optimization versus just closures. One of the reasons data centers that exist today in the Federal portfolio are inefficient is because of the way we use the data center itself versus what is actually running in the data center. The way IT has grown up, it is very inefficient to use single servers in data centers for single functions. New technology allows you to run multiple functions on single machines at a much lower cost than you have seen in the past. So in essence we are going to optimize and close data centers by shifting the resources of one to other ones, to more efficient data centers, not taking away services, not deprecating any service that

we provide. And if anything, while we make that shift, we actually modernize those systems to provide even better service. So it is a really nice opportunity to build efficiency and effectiveness at a much lower cost.

Mrs. MALONEY. Well, your statement and Mr. Davis' and others, I agree completely that cybersecurity is a national security concern and it should and is a bipartisan concern. And if there was one area that we should be moving swiftly on, it is cybersecurity. It is not only hitting the Pentagon, but financial institutions, trade institutions, commercial institutions. It is everywhere and every day, and countries have complete government agencies out there just going after our information.

The fight before us reminds me very much of the intelligence fight we had after 9/11. It was basically a turf fight. No one wanted to give up turf. We were told our basic problem was a lack of up-to-date intelligence. We had to create better interagency talking and preventive methods to make our country safer.

And we have a turf battle now on cybersecurity. No one wants to give up their turf. Obviously OMB is the enforcer, but you need an agency that comes in and pulls all of this together and forces these agencies to work together, talk together, move together, to do that.

What agency do you think would be the best lead agency if we were going to pull everyone together? I think we have a huge, huge turf battle that is preventing us from going forward.

Mr. VANROEKEL. We have done a lot to move the ball forward on thinking about coordination in the cyber realm. And we take it sort of in two views. One is the classified network side, and then one is the public network side, the unclassified side. I am a chair member on a safeguarding committee that looks at the classified side and we should have another venue in which we talk about some of that.

On the unclassified side, we have made the decision and worked very closely with Department of Homeland Security to provide the cyber capabilities, operationalize the cyber capabilities of the Government along with OMB and the White House to focus on what our capabilities are on cyber. So they run incident response through a group called US–CERT, the Cyber Emergency Response Team. They are leading the charge on the implementation of the government-wide continuous monitoring system, and then they work with us on CyberStat reviews which are going out and implementing FISMA, but a more regular touch base on cyber capabilities at the agency level. And I think we have done a lot there, along with the CIO Council, to coordinate our cyber activities in a way that I feel very confident that we are making not only good progress, but great progress on.

Mr. MICA. There is one minute left in the vote. We will recess at this time. I would ask both of the witnesses if you would stay in recess and then be available, we will see if there are future questions.

The committee stands in recess.

[Recess.]

Chairman ISSA. [Presiding] Earlier, when I talked to Mr. Davis, as a friend and mentor, I did sort of badger him on the question of, for example, 40 CIOs at DOJ. I would like to revisit that again.

The term CIO, one that you have, what is it supposed to mean? And do we, in fact, find another title for people who are less than the CIO and, in fact, those who either don't have budget authority or who receive their budget authority as a subset of somebody else who has budget authority? If you would like to comment on that.

Mr. VANROEKEL. Yes. As Mr. Davis said, I think it is not necessarily just a titling problem or opportunity that we maybe have in front of us. The title of CIO, it varies in many agencies. I think the thing that we need to examine as a tech community in looking at Federal IT is really the role and responsibility of the CIO and the CIO's organization across the enterprise. You know, there are many agencies where the person at the top of the org chart has less budget and less authority than they maybe had when they were a subcomponent agency CIO. And so we see challenges there, challenges in governance, challenges in the ability to have influence and visibility across the entire IT portfolio.

The very first memo I issued in my job when I took over for Mr. Kundra——

Chairman ISSA. Is this the 25-point plan?

Mr. VANROEKEL. No. I did inherit that, which is great. But the first memo I issued was a memo that actually addressed CIO authorities and brought to bear new OMB guidance that CIOs need to be more empowered in agencies to make decisions around commodity IT and things like that across the agency. And so many agencies are operational I think now.

Chairman ISSA. And I think, rightfully so, you know, the question of portfolio is a big part of the answer to the question.

But let me ask a different question. To a certain extent, don't we have a proliferation of CIO as a title because it also comes with pay; that is, an expectation that, you know, that you can't get somebody above a given level unless you give them that title, and by creating that title, you create, quite frankly, a more expensive employee?

Mr. VANROEKEL. I think pay could be a factor there.

Chairman ISSA. By the way, just so you know, my limited experience outside of Congress was trying to get a clerk-typist to be, first, a secretary and then a stenographer. It was the same person, worked for the same colonel, but he wanted to pay her more, while I was in the military. I am very aware that titles, in fact, change pay. And so when you say "could be," I am presuming you say almost inevitably must be in some cases.

Mr. VANROEKEL. I just think there are other factors that play out in the Federal landscape. Having come from the private sector as I did and the position I was in before I came here, I certainly didn't take this job for pay, even though I am the highest ranking CIO, conceivably, in the Federal government. It was more about the scope of responsibility.

I think oftentimes that that title comes with a lot of responsibility. And thinking to the concept of I want to get the best person either inside government or outside government to take the job, the title actually matters because it equates to the scope of the respon-

sibility related there. Look at the Department of Transportation as an example. I would certainly want someone looking over the FAA to be a CIO, to be a person that has actually got that title and that authority.

Chairman ISSA. But do you think the DOT has 35 such needs?

Mr. VANROEKEL. I think the essence there is good governance, good policy inside the agency. You mentioned the Department of Justice. After we——

Chairman ISSA. Yeah, they top the list with 40.

Mr. VANROEKEL. Yeah, they do. And after we issued the guidance on the Department of Justice, every dollar spent within the agency on IT, even at the level of purchase cards, goes across the desk of the main CIO in the Department of Justice. So they now have spending transparently and have built mechanisms to do that spend based on the guidance I issued, which is about the ability to manage and govern spending at that agency. So I think it is not a titling problem, it is a governance and management problem.

Chairman ISSA. I hope you are right. And I am going to go to the gentleman from Texas. But I might mention that since they don't seem to be able to read wiretap warrants to find out that, in fact, they would expose wrongdoing at ATF under their watch, I would suggest that they probably aren't looking at every credit card receipt all that well.

Mr. Farenthold?

Mr. FARENTHOLD. And I want to expand a little bit on that, and on the Dashboard system, in particular. I am concerned we have a system here of garbage in, garbage out. And what kind of checks and balances do we have to make sure that we are getting good data in there? Is it just coming from the agencies? Do we have some sort of, you know, other checks and balances?

Mr. POWNER. So a couple things. That is a legitimate concern, and we see it varies by agency. So we have issued numerous reports looking at the accuracy and reliability of what is going into those Dashboard ratings. The good news is over time we see that accuracy improving. But we still have some agencies that aren't as accurate as we need them to be.

Obviously, it is on the CIOs at those agencies to ensure that we have accurate reporting. OMB plays a key role. If they see something that raises red flags, you know, they can pick up the phone and make sure that we have better accuracy there. And we will continue to that do in our work for the Congress, looking at the accuracy.

Mr. FARENTHOLD. Is there something we can do to help improve that?

Mr. POWNER. Sure, there are some things you could do, I think, with your oversight. You can look at the Dashboard right now and you could look at some rather large departments and agencies and you see zero high-risk investments, similar to DOD. And some of these are large departments and agencies. And I think congressional hearings such as this where you have panels of those agencies that have zero reds would be a good thing.

Mr. FARENTHOLD. All right. Let's talk a little bit, Mr. VanRoekel, you worked for Microsoft for a while. And I think part of the problem that we have here is when we are buying things, how we are

specifying them and how we are deciding what we need and how it is all happening. You know, in the consumer market, and small, medium, and even to some degree large business market, Microsoft dictated what the standard was. Industry said: This is our product, do with it as you may.

In the government, you tend to have the government come up with all of these detailed specifications for stuff that has to be custom coded or whatever. And then you look at probably the biggest success story coming out of the government, which was the Internet, which came out of DARPA, and it was a collaborative, almost open-systems sort of thing.

Is there a way we can adopt the Internet model for developing the overall computing scheme of the government rather than having all these different agencies come up with all of these different technical standards, or relying on manufacturers saying, this is what our product is, take it or leave it?

Mr. VANROEKEL. Yeah, I think the normal motion in the government in the past has been one where you say, well, I am faced with some challenge, some opportunity to build some system. You do one of two things, and you highlighted one of them. I think one is you go out and buy packaged software that exists and then you hire an integrator to try to glue it all together to come up with some solution. Or what you do is your requirements are so unique, exactly to your point, you describe this very monolithic, big solution and you have someone try to build it from scratch.

And the problem with both of those approaches is that the risk surface is so incredibly high, and the outcome of that effort is not realized until much farther down the road. If you think about a quarterback throwing the long ball, you know, that you have a much higher likelihood that that thing is going to not be caught or intercepted, or it is just very, very risky, versus a 4-yard pass down the road. We have a lot more product managers in government that can throw the 4-yard pass that can actually architect a long-ball pass.

And so what we need to do and what we have proposed in policy and what we are doing working with the industry is to really scope a modular approach, to say, you know, we don't need to build these big monolithic things, we don't need to absorb that much risk on the side of government. What we need to do is build smaller solutions that interoperate and work with each other. The private sector has been doing this for years, the government has not. And we are working with the private sector on developing that.

Mr. FARENTHOLD. And I think one of the struggles we have in the government is getting—I mean, we have got some good people here. But we don't offer what—you go in the private sector, you have got a great idea for doing something or solving a problem, you work out of your garage for a while, and then you have an IPO and then you are Steve Jobs. Pardon me for me going right after your one of your former employer's biggest competitors.

But is there a solution, maybe, again, going back to the Internet model, of having some of our standards and solutions developed in the academic field, rather than, you know, trying to get it done with employees, many of whom are really looking for the long term, you know, to be the next Mark Zuckerberg?

Mr. VANROEKEL. Yeah. I think the approach we are seeing emerge in government is something that is encapsulated in a strategy I published last summer called the digital strategy for the 21st century government. And what it basically prescribes is exactly that, using open standards, open-source software and other approaches to say there is a new way of building these solutions where you can have data interoperability across agencies, you can have system interoperability, that when we build solutions within government, we should built it once and use it many times, versus using these siloed approaches.

So if you look at the use of technologies like GitHub, where we are now sharing code across government, some of our best practices work and some of the solutions we are building, this is the approach that I think is going to be the new default within government.

Almost every project that I have text added in government where I can have a face-to-face meeting with a project that is going awry, I have recommended they go to this modular approach, and then in every single case it has turned out well.

Mr. FARENTHOLD. I am out of time. We could go on for a long time. Maybe I will——

Chairman ISSA. Call your own hearing on this. I thank the gentleman.

We now go to the gentlelady from the District of Columbia, Ms. Holmes Norton.

Ms. NORTON. Thank you, Mr. Chairman. I wanted to get back to get some clarification on savings. You know, this Congress is very interested in savings, for good reason. And we know that there should be an incentive to use cloud first, we know it is the government's policy, because you pay for the service you use. And yet we have contrarian responses. There are some agencies, apparently, where it would be cheaper to stay with a data center. I don't understand why. But that is apparently the case. But I was, frankly, shocked to read a column yesterday about—here's a figure that was in the column. It's called "My Cup of IT," Steve O'Keefe. "GAO tells us Feds spend 69 percent of the $81 billion IT budget on hospice care for geriatric systems," you know.

Let's leave aside his characterization for the moment. But it would seem to imply that these systems are long past their usable lives. And yet it looks like the lion's share of money is spent on propping them up.

Why aren't agencies rushing toward cloud, saving themselves money, and doing what the government's policy says they should be doing in the first place? Either one of you can answer that question. I would appreciate it.

Mr. VANROEKEL. I will take the first take on it. I think the challenge that we often face is the capital expenditure it takes to make the transformation. You often can't just pick up a system you have——

Ms. NORTON. Well, of course.

Mr. VANROEKEL. —and just move it to the cloud, you actually have to spend money to do that.

Ms. NORTON. So is the administration budgeting for capital expenditure?

Mr. VANROEKEL. In many cases we are. But in this fiscal environment, my approach has been, let's go find savings where we can, where we find low-hanging fruit, and then reinvest those savings. So my budget guidance I put out to agencies, for example, was to cut 10 percent of their IT budget in targeted areas. And I gave them the target areas, things around we've just been discussing today, commodity IT and other places where it doesn't take that capital lever to move. And then I, to net to a 5 percent down, I gave them 5 percent of that 10 back to say, okay, now this is capital you should be investing in these new areas. And the new areas should be focused on systems modernization, cybersecurity, employee productivity or citizen-facing services, making those run in a better way.

And then I ran the portfolio set process to help them find that 10 percent within their agency in a very data-driven way. We went and analyzed all the commodity IT systems they were running and things. And so this is a spirit that I am trying to inject into government.

Ms. NORTON. Because it looks like for sometime now there is not going to be the capital. I mean, the cloud is an ideal. A cloud is what we would like to see. But let's face it, like so much of IT, if it takes heavy capital investment, it just can't happen for some time. It is going to happen very gradually. Isn't that so?

Mr. VANROEKEL. That is right. Unless you inspire this let's examine what's working, what's not working, take what's not working, cut it, and then move it in.

Ms. NORTON. Have you all ever done a cost benefit? I mean, would it be worth it to speed it up because of the savings? Or is this just not something we could bring money to bear on at this time, no matter what?

Mr. VANROEKEL. In certain cases, definitely, it would be. It would be advantageous. But what you have to be careful about is looking at the—you don't want to just take bad behavior that is local and move it, that bad behavior, to the cloud. You should think about, how am I re-architecting these systems? And that's part of the underlying work we are doing, thinking about these open architectures and modular design and things that are going to be evolutionary as well as revolutionary in there.

Ms. NORTON. What kinds of agencies are there where it would be cheaper to stay with a data center than to go to the cloud?

Mr. VANROEKEL. In an aggregate world, I don't think it is cheaper in many cases that they would not be running to the cloud provider. Where it is more around, do I have the money today to invest to move that capital expenditure? And I think the cheapness equation comes in a single-year view, because that is the way we budget in many agencies, versus the long year. We often see this with Federal real estate, where it would be cheaper to buy a new building than rent an expensive building or things like that, where the capital expenditure to move is challenging.

Ms. NORTON. Thank you, Mr. Chairman. My only concern is, if these systems are really as old and presumably unreliable as is implied by this columnist, I really do wonder about cybersecurity and about investing in cybersecurity in such old systems only to have to reinvest it when the cloud comes.

Chairman ISSA. If the gentlelady would yield?

Ms. NORTON. I would be glad to yield to the chairman.

Chairman ISSA. Perhaps there is one salient point that you would appreciate, but 75 percent or so of the budget is spent on legacy systems, some of them are so internal and can only be run locally and they are operating on obsolete computers and obsolete operating systems and they are written in COBOL, they are written in Fortran, they are not able to process through the cloud at all. They are pretty much hack-proof. That is the one good part, is they don't go into cyberspace. Therefore, they actually——

Ms. NORTON. You mean all that hacking is done on only cloud systems that we read about every other day?

Chairman ISSA. Well, I think the gentleman would probably tell you that some of the systems he looks at do not, in fact, have a portal for remote access through an Internet-based process.

Mr. VANROEKEL. That is right.

Chairman ISSA. That is not the good part. I am just saying, it is so bad that hackers can't even bother to go back. There are aren't old enough hackers for it, perhaps.

Ms. NORTON. Be grateful for small favors.

Chairman ISSA. If the gentleman from Virginia would give me a dispensation, the gentlelady from Illinois and the gentleman from—where the heck are you from?

Mr. POCAN. Wisconsin.

Chairman ISSA. Wisconsin, Madison, Wisconsin, returned so promptly, would you mind if I took one of them first?

Mr. CONNOLLY. Go right ahead, Mr. Chairman. I was just going to say, thank you for making that point, though. Who knew that actually obsolete and antiquated systems were helping in the fight against cyberattacks? Thank you.

Chairman ISSA. You two figure out which one of you go. The gentlelady is recognized. Smart move.

Ms. DUCKWORTH. Thank you, Mr. Chairman. So I hope to build on the bipartisan nature that you have started these hearings today with.

My question, which is really one coming from a freshman Democrat who is concerned about a Governor's rights and States' right. Specifically, 95 percent of our military support to civilians within the homeland is conducted at the State level through State active-duty status, which is funded out of State coffers or Title 32-funded State missions which are Federally funded. I am concerned about a Governor's ability to command and control his forces, such as during a natural disaster, if we defund his State IT network and attempt to replace it with a Federal solution that may prioritize Federal military missions over National Guard homeland domestic operations. I am concerned that building a new Federal solution, such as an IT backbone, purchase of routers, the like, could be more costly than continuing to fund existing IT solutions that the States have already built to meet their specific mission requirements.

Louisiana and New Jersey have very different needs than my home State of Illinois, although some remain the same. And they have different commercial IT networks that can be leveraged. I would like to see Federal and State Governments leverage existing

commercial networks for cost savings wherever possible rather than pay to build new solutions.

I am also weary of infringing on a Governor's ability to command his or her National Guard forces. As I see it, consolidating of IT is a great thing, but it does set up a tension between the DOD Federal priorities and the State priorities. You know, it works well to consolidate for Federal Title 10 mission support, but tends to prioritize the Governor's National Guard forces below active component for funds. This low priority threatens the ability of Guard forces to respond to and coordinate efforts and really for the Governor to remain in control of his or her State active duty and Title 32 forces.

So I have two questions and either gentleman can choose to answer. The first question is this: How does the centralized Federal IT acquisition process support military operations at the State level?

And my follow-on question is, are there any safeguards that would ensure that State IT requirements, missions, such as under State active duty or Title 32 missions, can be given the same priority as the Federal forces under Title 10? Thank you.

Chairman ISSA. Clearly, the gentlelady is not new to asking questions.

Mr. VANROEKEL. I am not a subject matter expert on the tactical aspects of technology deployment at the State level. So especially the second question, I think I would love to take back for the record and get you a response that is much better than one I would postulate myself.

But on the first, the military at the State level and thinking about integrated acquisition at that level, one of the things I think we do pretty well and are getting much better at is setting up more centralized requirement gathering. You know, one of the main challenges we see, both on the Federal side and the private sector side working with the Federal government to supply services, is the unpredictability. You know, when we are unpredictable in our procurement of cloud computing, for example, prices tend to go up, variability in cyber protection goes up, and other challenges are presented.

So I will definitely work with the Office of Federal Procurement Policy and DOD to get you an answer to this. But I think the essence of this is going to be around not necessarily just setting up a one-size-fits-all for the entire country, but more around, you know, how are we coming together as a community to solve a common mission purpose around a set of predictable requirements but flexible requirements that allow variability at the State level, I think is essential.

Ms. DUCKWORTH. And I think it is a very specific case, a very narrow situation. You rarely have this type of situation where it is the same unit, entity that has both a Federal and a State mission. I just want to make sure that we are not infringing on a Governor's right to control his or her forces when they are under that State active duty or Title 32 and to make sure that that is given the same priority by DOD. Because if DOD gets access or control over the funds, the acquisition funds for the entire military, including Guard, they will naturally, I would assume, prioritize Title 10

or active-duty missions over the equally important State missions. And I just want to make sure that there is some way to ensure that those State requirements, as set forth by the Governor, are well respected.

Mr. VANROEKEL. Great.

Chairman ISSA. Would the gentlelady yield for just a second?

Ms. DUCKWORTH. Gladly, sir.

Chairman ISSA. When you are answering her question, would you sort of try to the best extent you can include how we best leverage, either through this act or other things that you are currently doing, the dollars being spent federally being made available, if you will, for cheap or free to the States? In other words, our procurement falling to their benefit, and particularly if you look at source code, where a State may choose to modify the software but they have to be able to get the software and source code basically at no cost for the Federal use and then be able to add on their hooks for the State. And I think that is a big part of what the gentlelady is speaking about. If you could answer how you envision that, I think the committee would appreciate it.

Thank you. We now go to the gentleman from Virginia for five minutes.

Mr. CONNOLLY. Thank you, Mr. Chairman.

I am going to ask three categories of questions. And I am going to do it as fast as I can. And I ask you to be as fast as you can.

Process. It seems to me that when you compare it to the private sector, the Federal process is hopelessly out of date and not at all suited for this kind of IT procurement. You know, you have got long lead times. By the time we have figured out the RFP, we have figured out the contract award process, we have awarded the contract, we have set the terms, we have dealt with the protests, the technology has already passed us by. Or the mission, technologically, has been redefined necessarily. And we don't seem to be very flexible in addressing that. And that is to say nothing of the fact that, you know, we have this stovepipe process all over the place.

The Chairman has pointed out that we have 243 CEOs. That sounds likes way too many. What could go wrong with that in terms of accountability, a point of decision making? It seems almost a system to make sure there is no accountability.

Your comments, both of you, on process?

Mr. POWNER. That is a very valid point on the long lead times. And if you look at many of these large acquisitions, the time between major milestones sometimes is years. And that is still the case. I think Steve's comments earlier about modular development, we need to have the procurement side of the house align with the technology side of the house. So modular contracting along with development is clearly where we need to go so that we can get a bit more modern here in the Federal government.

When you look at the CIO issue, yeah, there are a lot of CIOs across the Federal government. The thing we like, and we have been looking at large-scale IT acquisition problems for years now at the Government Accountability Office, is having the Dashboard where you have a single CIO accountable at these major departments and agencies that allows you to go someplace and get ques-

tions answered. And that actually caused a lot of problems when the Dashboard was rolled out because there wasn't a single person to go to and there was a lot of scrambling that needs to go on to get status. And we are still probably feeling the effects of that. We like that model where there is a single CIO, where you have other CIOs, where you figure out the reporting. That is what is really needed.

Mr. CONNOLLY. Okay. Mr. VanRoekel?

Mr. VANROEKEL. I think on your two points, first, the process on long lead, I couldn't agree more on that is a big challenge. I think part of solution to this is in existing law and exists in the realm of myth-busting, where we are explaining to agencies there are new ways and new approaches of doing this. The two that are most encouraging to me are, one, are just flexible contracts, having an open contract where, when you need a resource and you need a developer to develop some solution, you need something done, you can call upon them and bill as you go. We have seen that as a great model.

The second is modular contracting, as Mr. Powner said. Getting agencies to embrace modularity, smaller deliverables that can be done in a much faster pace really ups the level of both quality and agility on their ability to deliver. Joe Jordan and I delivered just in 2012 modular contracting guidance for agencies that is new policy around teaching both the acquisition community and the IT community how to deliver on modular.

On the number of CIOs, I think from a titling perspective, we have a lot of CIOs. And I think there are many cases where there is span-of-control and some government challenges that we need to get our arms around, thus, the first memo I issued out of my office that went right to the heart of this.

I think part of the solution to that is, first, getting all those CIOs out of the job of things that should be centralized across their agency. You know, having multiple email systems in an agency doesn't make sense; you should run one. Having multiple——

Mr. CONNOLLY. When you were at our field forum, I thought you said that one agency had, like, 36 emails systems?

Mr. VANROEKEL. Yeah. Over 20 I think is what I said. And that same agency, over 1,000 mobile contracts. They now have one. It is one email system. It is a third of the cost. And the 1,000 mobile contracts went to a few blanket purchase ones, which is massive. So if you get CIOs at the fringe out of the business of managing that commodities stuff and more focused on the mission of their division or their agency or their bureau, you can really up the quality of the citizen services and the effectiveness of that agency. And that is part of the magic of the mix.

Mr. CONNOLLY. I am going to run out of time, so I am not going to get to all three of the things that I think the chairman and I are both trying to look at in the legislation, unless the Chairman wants to be a little generous here. I am trying to lay some intellectual——

Chairman ISSA. Start asking before you run out of time.

I ask unanimous consent the gentleman have an additional minute. Without objection, so ordered.

Mr. CONNOLLY. I thank the chair.

Tom Davis testified about procurement personnel, that that is one of our problems, the lack of skill set. Often the person selling has a higher skill set than the person purchasing. Your views about that problem in the Federal government?

Mr. VANROEKEL. I agree that that is a challenge. You often have the person doing innovation in an agency, not the person that also purchases. And there is a divide there.

What we are encouraging—and this is coming straight out of the Office of Federal Procurement Policy—is, first, is integrated program teams. Getting those communities' human capital, acquisitions, IT, finance, and others sitting around the table, as I mentioned earlier, and getting involved with integrated acquisition teams on specific projects that are of high priority is just so essential, to have everyone sitting around the table.

And the second is IT acquisition cadres, getting areas of expertise and specialization within agencies that can focus on certain solutions or certain challenges. You know, negotiating a very effective mobile contract with a mobile carrier is not easy and there is some complexity in that. If you have a team in government that focuses on it and thinks about it, that is a recipe for success.

Chairman ISSA. I think the gentleman.

Mr. CONNOLLY. I thank the chair.

Chairman ISSA. We now recognize the gentlelady from Wyoming for her questions.

Mrs. LUMMIS. Thank you, Mr. Chairman.

And, Mr. Powner, I apologize if this question has already been brought up in my absence. But my question is, we know that agencies are supposed to analyze legacy systems and try to keep ahead of the technology curve, but we also understand from GAO's work that many are not doing that.

Can you describe the extent of that problem and perhaps include in your answer roughly how many billions are being spent on IT programs for which we have no analysis of where the agency is on its technology curve?

Mr. POWNER. Well, let's just talk about framing how much we spend on legacy systems. So of the $80 billion, roughly, you have $55 billion, or 70 percent is being spent on legacy systems.

There is a very good requirement that OMB has that on an annual basis each of the legacy systems need to be evaluated. And, basically, what it asks for is this: Is it continuing to meet the mission needs? And can it be done in a much more efficient way? So with the discussion we had prior about going to the cloud, perhaps we can go to the cloud and do it much cheaper.

There are also things we can do with back-end systems. If you really went in and analyzed some of these old archaic legacy systems, there are tweaks we could do to make that pot of $55 billion, we could spend that much more efficiently going forward. Cloud is clearly one way to get there.

What we did is we looked at a small sample. We looked at five agencies in the review that you are talking about. And what we saw was, the Department of Homeland Security and Health and Human Services, they actually had a policy and they were doing these operational analyses. Now, they weren't doing them well in all cases, but they had a policy and they were doing them. We had

agencies like DOD, VA, and Treasury, no policy. In the year that we looked at, they didn't do a single operational analysis.

So what we found in our little samples, we had about $3 billion in systems that were not evaluated. So that $3 billion investment, technically, that could have been invested much more efficiently if we looked at that in the appropriate manner.

Mrs. LUMMIS. Thank you.

And a follow-up for Mr. VanRoekel. So knowing that—and I assume this is not new information to you—knowing that, what is your plan for all agencies to complete operational analysis? And when should we expect full compliance? And I say that with the caveat that we have been waiting for a clean audit from DOD forever. They have never had one. And so now to hear that DOD is one of the agencies that has not completed this analysis is not surprising either. But do you have a plan to get these people onboard?

Mr. VANROEKEL. So it is our expectation that both through our policy and accountability mechanisms that agencies will step up. And we have made a lot of improvements, as I think has been highlighted a little bit here today on IT Dashboard, to expose some of the areas where we think the quality of the information that is being submitted isn't there or it is just lacking altogether.

One of the features that we have added is data quality reports that actually look at, if a date is unrealistic, if numbers don't line up, if due dates are too far out, that is actually now highlighted on the IT Dashboard to build a level of accountability for these agencies. That, coupled with our budget guidance, which is putting a lot of pressure on agencies to really examine these legacy systems, I think are elements of how we are going to get there.

You know, something I used every day because I was part of a team that ran a pretty large P&L within the private sector company I was a part of, was depreciation. You know, we thought every day about, how do we wind down the things we have done in the past in order to fund the things going forward?

You know, we used our balance sheet as a strategic tool. In the public sector, we tend to use the balance sheet just as an auditing tool, just to check back on how we have done. And a clean audit is success, versus are we properly managing this turnover of old and giving to new, stealing from the OPEX column to give to the CAPEX column. So the budget guidance gets right to the heart of this, and I think will inspire more action than actually doing oversight assessments through the IT Dashboard. By telling agencies you need to cut 10 percent and you need to take 5 percent of that and put it back into the top of your priority list, I think we will start to see more turnover. And definitely from a trending analysis, looking at where the old system support is going, we are now starting to see it, which is very encouraging.

Mrs. LUMMIS. And, Mr. Chairman, one more question.

For either of you, have you seen a State that represents the best practice among States in getting a handle on these same issues? I know in my State, I was in all three branches of State government during different times in my life. And in every branch of State government, we struggled with these very issues, especially in the executive branch.

So is there a State that is the leader in this that even the Federal government could look to for some streamlining?

Chairman ISSA. If you say Wyoming, you will get a lot of points here. Illinois will work, too. Southern California.

Mr. POWNER. I don't know if I can point to one State, but I will say this, because we do a lot of work with the National Association of State CIOs. And I think when you look at the budget situation in a number of States across the country, they were forced to consolidate data centers. They had no choice. Things were getting cut and they needed to find ways to lower their overall budgets.

So there are a number of states that I am aware of through the National Association of State CIOs, but they face very similar problems. They are trying to put in place Dashboards so they get better performance on their large acquisitions. But I do think you will see many success stories at the State level on data center consolidation.

Mr. VANROEKEL. And the other thing we are seeing at the State level is groups of States now getting together and saying let's create a regional authority to look at sharing procurement, sharing technology, and sharing other things. And that has been very successful as well.

Chairman ISSA. Excellent.

Mr. Pocan?

Mrs. LUMMIS. Thank you, Mr. Chairman. I yield back.

Chairman ISSA. I would say so.

Mr. POCAN. Thank you, Mr. Chairman. And thank you, gentlemen.

I am going just going to ask one question and then I am going to try to yield my time back to Mr. Connolly so he can get his third question in.

Mr. Powner, I know there has been some progress made in consolidating data centers, but your GAO report highlighted that many agencies have failed to produce complete data center inventories and plans and the vast majority even the basic requirements, such as schedules and cost estimates. And that without these plans and inventory there is a lack of consistency among agencies, it is difficult to summarize projections. I was just wondering, based on your research, why are so many agencies failing to complete these requirements?

Mr. POWNER. So a couple comments here. We looked two periods of time looking at data center consolidation inventories and plans. And you are right, the last time we looked, the last we reported, there were three agencies that had complete inventories, that was SSA, HUD, and National Science Foundation. And then only one agency had a complete plan when you look at the requirements that were laid out by OMB, and that was the Department of Commerce.

Some agencies, like DOD, really struggle to get their arms around their inventories. It is somewhat expected. But our point is that you need to keep on, on the task, make sure that you identify all those centers that are out there so that you can look to optimize, consolidate, and ultimately save money.

There has been a lot of good work. I mean, we now know there are almost 3,000 data centers across the Federal government.

There has been this goal to close about 1,200 of them. Ultimately, you want to get to a point where you get away from the inventories and plans and you get down to the action on actual optimization and consolidation. And that is really what we are looking with our recommendations going forward. With sound baselines, that is clear. But ultimately, it is about the actions. And that is why I say when you look at the ultimate performance metric on data center consolidation, whether you are talking consolidation, optimization, it is dollar savings. And if DOD says there is $2.2 billion, there is probably more than that. And I think the estimate of $3 billion that OMB has, it is likely more than that also.

Mr. POCAN. Thank you. And then I would just like to yield my time to Mr. Connolly.

Mr. CONNOLLY. I thank my colleague.

And the third set of questions I wanted to ask, again referring to the testimony of our former colleague, the chairman former chairman of this committee, Tom Davis, he talked about how budgets matter, especially when we put ourselves on a continuing resolution. He actually said it stifles innovation, it sets us back in terms of thoughtful Federal IT procurement.

I want to give you both an opportunity to comment on that, your views about that.

Mr. VANROEKEL. When I was in the private sector implementing solutions in technology or even building products, about 2 days after the beginning of the fiscal year we would get our full year budget. And of course we had to make adjustments based on quarterly returns and things, since we were a large enough division to affect the stock price and other parts of the balance sheet.

But in large part, we were able to predict, you know, not only what our operating budget was that year, but based on certain other parameters we could make investments that were around solutions that were going out into out years. I could say I am going to incubate a product, I am going build it, and it is going to take 4 years to do it, but it is going to have this much ROI at the end of that.

In the Federal government, we often face a situation where we get to back-to-back CRs or other elements where the money that is budgeted is allocated so late in the fiscal year that you have 2 to 3 months, if that, often to not only procure what you are hoping to procure once you know the money you have, but then try to implement and get things done in time. And that is a real limiter on the ability to drive innovation and a long-term view of where you could go with some of this. We have seen capital budgeting and some other things in government be helpful in that area.

Mr. CONNOLLY. Mr. Powner?

Mr. POWNER. Well, in addition to innovation, I know I do work specifically on weather satellites. And there has been situations where with the weather satellites, they are very important, you look at polar-orbiting satellites in this country, they were essential to predicting the Sandy superstorm. That was a real success story in terms of the accuracy of when that storm hit. It was spot-on, due to these weather satellites. And I know the current acquisition on those satellites has been affected in a negative way due to some CRs.

Mr. CONNOLLY. Well, I thank you both very much. I do think it is other constraint we have to look at in terms of our own process in Congress and how, perhaps unwittingly, we contribute to some of the problems in the whole process of Federal IT procurement. Thank you both so much.

Thank you, Mr. Chairman, and I thank my colleague.

Chairman ISSA. Thank you. Would the gentleman further yield? Thank you. I just want to have something answered for the record.

This committee took a keen interest under both Mr. Waxman and Mr. Davis in the failures of FTS 2000, the telecommunications modernization. At least at the last time that we had a hearing, what we found was that agencies had simply refused—they didn't say refused—but never implemented the cost savings that came with modernization.

We now have, it has now been renamed in that 2009 networks. And many agencies are still struggling to, if you will, take advantage of cost savings of buying better telecommunications for less. And as we talk about the cloud, obviously, if you don't have a low-cost, high-speed Internet connection, you are going to also resist the cloud.

So could you, there is no time left right now, but either at the end or in writing, if you would answer on your vision of where we go there, because, tangentially, it is part of the problem.

Chairman ISSA. With that we recognize the gentleman from Tennessee, Mr. Duncan.

Mr. DUNCAN. Thank you very much, Mr. Chairman. And it seems to me that this is a pretty important subject, and I appreciate your calling this hearing. And I think almost every member should be upset or should be at least concerned if they would read what was in our committee memorandum. And it says, "Despite spending more than $600 billion over the past decade, too often Federal IT budgets ran over budget, behind schedule, or never deliver on the promised solution." And it says, "Some industry experts have estimated that as much as 70 percent of new Federal IT acquisitions fail or require re-baselining"—70 percent. I mean, that is almost a shocking figure that I don't think we would accept in almost any other field.

Just a week and a half ago, I read in the New York Times a story that said that conversion to electronic health records has failed so far to produce the hoped-for savings in the healthcare costs and has had mixed results, at best, and said optimistic predictions by RAND in 2005 helped drive explosive growth in the electronics records industry. And yet today it says this 2005 report that helped lead to all this explosion in the technical equipment for the Federal government was paid for by a group of companies, including General Electric and Cerner Corporation, that have profited by developing all this equipment.

And so often in other committees I have heard, whenever a government agency messes up they always say one of two things or both. They say they are underfunded or their technology is outmoded or out of date. And yet the technology in the Federal government is usually much newer than anything that most of the private sector has.

And I was thinking about this a few minutes ago, and I thought back to something that former Governor Rendell, when he was mayor of Philadelphia many years ago, he was having trouble with city employee unions. And he testified in front of the House Ways and Means Committee and he said that government does not work because it was not designed to. He said, there is no incentive for people to work hard, so many do not, there is no incentive for people to save money, so much of it is squandered.

And what I keep seeing in this, the only people who really understand this subject are techies who want us to buy all the newest and latest equipment and all the bells and whistles even though we really can't afford it and it is not cost effective it is not producing the results that we are paying for.

And so I guess the only real question I have is, can either of you think of any way that we could put more good Federal employees, since the money to buy all this new equipment and spend all these mega-billions each year is not coming out their pockets. So they don't really have any incentive or any pressure to hold these down costs or not buy new equipment every year or every other year.

Is there some way that we can get some incentives or pressures to do better? I mean, surely we sure need to do better in this area.

Mr. VANROEKEL. I very much agree. And I am in my job now largely because of that fact. And I think we are able to have much of the conversation. You were able to cite some of the statistics you were in your comments because we are making progress in these areas.

The accountability mechanism of the IT Dashboard, the ability for us to put a public-facing Web site up that says, here is what we are doing in government and IT, here is where people are implementing certain technologies, here is what is happening, down to a very granular level with new features being added to that all the time is creating a really interesting dynamic of accountability relative to the delivery against those Federal projects and priorities.

I think that is part of the equation. I also think we need to change the way we do business inside government. The way we build solutions is a very mid-20th-century, mid- to late 20th-century kind of view, where in the 21st century we have a much different model of building solutions.

When I was building products at Microsoft, I wouldn't have thought to take a government-like approach to anything. It was all about speed and modularity and the ability to build in a very fast way high-quality outcomes. And in the government, that hasn't been the norm, to your comments. And I think we have the ability to change that through good policy, which we are implementing now.

Mr. DUNCAN. All right. Mr. Powner? You see my point? I mean, I own two cars; one is a 2003 and one is a 2006. But if somebody else was paying for it, I might be out there trying to get one that has got better, newer equipment. And I think that is the problem.

Mr. POWNER. I do agree with Steve's comments about the Dashboard. I think the accountability through the Dashboard, where you have someone who is responsible for those investments and if they are not being delivered appropriately, there needs to be ac-

countability. Someone needs to be able for answer to that. Because there is a lot of dollars. We are talking about $80 billion we spend here.

To give you an example, in the report, my written statement, we did a report looking at successful IT acquisitions. So we went to the top 10 spenders and we said, give us one example of a success story where something was delivered, it is in operations, users are using it, and it was somewhere in the ballpark of cost and schedule. And there are seven examples, seven agencies gave us one. And that includes DOD. And you can read about those projects in there.

But there were three agencies couldn't give us

one. Three agencies could not give us one success story of a mission-critical system that was delivered recently. That is sad and someone should be held accountable for that, if we are spending $4 billion, $5 billion, $6 billion at these agencies and they can't give you one success story.

Mr. DUNCAN. Maybe we should come up with some bonus programs for Federal employees who save us money in this area in some way.

Thank you very much.

Chairman ISSA. I thank the gentleman.

For the record, would you mind doing some quick research on the three agencies that couldn't give you any examples and find out whether they had contracts that paid bonuses and whether or not employees received bonuses for overseeing those contracts that they couldn't give you, to the extent that you can?

As we close, this committee has taken note in the past of FedRAMP, something your predecessor began. We thought and still believe that it shows great promise. My understanding is, to date, we don't have, out of the five tests, if you will, up-and-running sites that can be sold, that are FISMA compliant, that can be sold across the government. If you would answer for the record your vision of how you get from zero to five or more and any other information you'd like to give us, that will probably be a follow-up hearing.

Mr. VANROEKEL. Yes, sir. We are actually at one right now, as of the last couple of——

Chairman ISSA. Conditional or provisional.

Mr. VANROEKEL. Authority to operate, yes.

Chairman ISSA. I understood they were provisional in some way. Is that just a term?

Mr. VANROEKEL. No, we have one vendor that does have an official authority to operate.

Chairman ISSA. Okay. So there is one to sell.

Mr. VANROEKEL. That is right. And we have 78 in the pipeline behind them. And we are processing through the pipeline right now those 78. So you will start to see more and more coming online in short order.

Chairman ISSA. Excellent.

Mr. VANROEKEL. And we expect 2013 will be a big year for getting vendors online with FedRAMP.

Chairman ISSA. Okay. Well I appreciate that. That is a why where we'd like to have a good news story.

I would like thank our panel. You have been very patient through the votes.

And with that, we will set up for the next panel.

We now welcome our third panel, beginning with Mr. Douglas Bourgeois. He is vice president and chief cloud executive at VMware, spoken about earlier as an entity that allows us to leverage multiple operating activities on a single piece of hardware.

Mr. Michael Klayko is the former CEO and current advisor to Brocade Communication Systems, Inc.

And Mr. Chris Niehaus is the director of Microsoft U.S. Office of Civic Innovations, meaning, you are bringing us what is good and modern, something we were talking about wanting in the last panel.

Again, you saw this earlier. Pursuant to the committee rules, would you please rise to take the oath and raise your right hands.

Do you solemnly swear or affirm the testimony you are about to give will be the truth, the whole truth, and nothing but the truth?

Let the record indicate that all three witnesses answered in the affirmative.

Again, as the previous panel, we would ask you to please do your best to limit to 5 minutes, and we will do the same.

Mr. Bourgeois?

STATEMENT OF DOUGLAS BOURGEOIS

Mr. BOURGEOIS. Thank you. Chairman Issa, Ranking Member Cummings, and members of the committee, thank you for this opportunity to discuss how the Federal government can reform its information technology investment strategy. Technology has always evolved rapidly, and that rate has accelerated to a pace that we have never seen before. Unfortunately, the government's methods for the acquisition and utilization of IT have not evolved in a manner that keeps pace with this innovation.

We believe that there are three fundamental challenges that should be addressed for the government to effectively leverage advancements in technology. These are complexity, expertise, and culture.

The IT acquisition environment is too complex. Advances in technology, such as virtualization and cloud computing, have rapidly accelerated the delivery of IT resources and made organizations more agile. Technology resources that once would have taken weeks, if not months to deploy can be carried out in a matter of minutes. By leveraging such dynamic capabilities, organizations are able to respond very rapidly to changing market conditions without making substantial capital investments in technology. But the IT acquisition process in the Federal government still moves at glacial speed.

In addition, these innovative technologies have turned a significant amount of IT products and services into commodities. The government should acquire these commodity technologies using performance-based contracting methods that address the longstanding tendency of the government to over- specify their requirements. Furthermore, the use of performance-based contracting methods, such as share and savings contracts, would also lower the risk of underperforming IT acquisitions and increase accountability for vendors.

Another way to simplify IT acquisitions is to simplify the overall IT environment within which IT products and services operate. Thus, the Federal government should continue with the efforts to consolidate and reduce the number of data centers government-wide. But the consolidation effort should not stop there. Other simplification tactics, such as virtualization of the networks and desktops, as well as the elimination of duplication of applications would drive further savings across the government.

The high degree of complexity in both the acquisition environment and the data centers throughout the government puts a tremendous strain on the workforce. In addition, studies have shown how the shear volume of Federal acquisitions has grown in recent years. At the same time, the staffing level of acquisition professionals has not kept pace with the growth.

Let me be clear in saying that while the growth itself is an issue, it is not the only issue. Existing efforts to increase the expertise of the IT acquisition workforce, such as the use of cadres and certification programs, should be expanded. The increased use of intern programs, perhaps in partnership with universities, and IT specializations should be established.

However, the IT acquisition workforce isn't the only area where additional expertise is required. Certain technical resources within IT organizations should also be trained and certified to develop the necessary level of expertise in critical technologies. As we have heard in the testimony previous hearing, that if the government staff that don't have the level of expertise as the contractors do, then there are going to be problems that occur as a result.

The third and final area in need of change is the culture. The decentralized approach to IT acquisition across the government has created a culture that is detrimental to performance and efficiency. The highly distributed approach also makes it difficult to gather data for analysis and transparency. This overall culture needs to become more centralized with areas of IT specialization to improve efficiency. Acquisition centers need to become more services-based with built-in incentives for performance and accountability. For example, IT acquisition centers should publish commitments to customers that clearly specify the timeliness and other performance criteria in advance.

Contracting tools are also duplicated and inefficient. A collaborative tool should be developed to foster more efficient handling of complex acquisition material, to track the responsiveness of program and acquisition professionals, and to increase transparency.

But the acquisition culture isn't the only one that needs to change. As the transition to cloud computing continues, IT organizations also need to transform to an IT-as-a-service model as well. Government CIOs must be in position to effectively carry out the responsibilities as the role of the IT organization changes to be more of a broker of service options.

For this reason, I strongly support strengthening the role and authority of agency-level CIOs to reflect the intent and requirements of the Clinger-Cohen Act. I also suggest that the structure of the IT budget needs to evolve to be more compatible with the industry trend away from capital investments and towards operating expenses.

In closing, we commend the leadership of the current and previous Federal CIOs to set the right course for Federal government. The journey to IT as a service has already begun through the consolidation of data centers and cloud first policy. In order to continue making progress, the methods for the acquisition and management of IT resources needs to evolve. Specifically, changes need to be made to address the changes of complexity, expertise, and culture.

We thank you for the opportunity to participate in this hearing today on this very important matter.

Chairman ISSA. Thank you.

[The statement of Mr. Bourgeois follows:]

Testimony of Doug Bourgeois, Vice President and Chief Cloud Executive, US Public Sector Division, VMware

Before the U.S. House of Representatives Committee on Oversight and Government Reform

on the subject of

Wasting Information Technology Dollars: How Can the Federal Government Reform its IT Investment Strategy?

Tuesday, January 22, 2013

Chairman Issa, Ranking Member Cummings, and Members of the Committee: Thank you for this opportunity to share VMware's perspective on how the federal government can reform its information technology (IT) investment strategy.

My name is Doug Bourgeois, and I serve as Vice President and Chief Cloud Executive for VMware's U.S. Public Sector Division. With headquarters in Palo Alto, California, VMware is a leading provider of software that makes data centers across the globe operate more efficiently, frees employees to access applications securely from anywhere at anytime, and allows both government and commercial organizations to respond to dynamic business needs. Through continued investments, VMware has established itself as a global leader in innovation that benefits all sectors including government, healthcare, finance, education, and small business, among others. Over the past 15 years, VMware has grown to be a $4 billion global leader with a proven history of helping both government and commercial organizations save money and operate more effectively. VMware currently supports roughly 300,000 total customers globally.

In the United States, VMware helps thousands of organizations increase the utilization of existing IT investments, lower the costs of IT operations, lower energy consumption, and become more agile and competitive. Through our U.S. Public Sector Division, VMware serves all sectors of the U.S. Federal Government – Civilian agencies, the Department of Defense, and the Intelligence Community – state and local governments; and all levels of education including K-12 and higher education. In fact, VMware's Public Sector Division

comprises about 10 to 12 % of our total business, which amounts to about $500 million on an annual basis. Some examples of our more notable public sector customers are:

- All of the U.S. military services (i.e., U.S. Army, U.S. Navy, U.S. Air Force, the U.S. Marine Corps), and all joint commands (i.e., NORTHCOM, SOUTHCOM, EUCOM, PACOM, and SOCOM) and DISA;
- Numerous civilian agencies, including the IRS, DOE/National Nuclear Security Administration, Department of State, VA, DHS, DOT/FAA, HHS/Center for Disease Control, among others;
- Many state and local governments from the states of California to Michigan and New York to the cities of San Francisco and New York; and
- Various higher education institutions including the California State University System and the state of Texas University System, and research programs such as the Johns Hopkins University Applied Physics Laboratory.

Based on VMware's public and private sector experience – and our global technology leadership position – we are honored and pleased to share our perspective on how the government can reform its IT investment strategies and acquire IT products and services more efficiently and effectively.

Innovation Through Technology

Technology has always evolved at a rapid pace – and that rate has accelerated to a pace that we have never seen before. At the same time, evolution of technologies such virtualization and cloud computing has ignited a phenomenon that crosses all industries and government sectors. Technology now enables enterprises, large and small, to deliver IT resources and applications in a highly responsive, services based model. Whereas in the recent past, it would have taken weeks if not months to procure and deploy technology resources such as servers, those upgrades can now be accessed and utilized – even on a very large scale – in a matter of minutes. By leveraging such dynamic capabilities, organizations are able to respond very rapidly to changing market conditions without making substantial capital investments in technology. So, in a manner of speaking, there are two fundamental transformation engines at work. One is the transformation to IT as a service that enables IT resources to be utilized by end users in a consumption model and released when no longer necessary. The other is the transformation of the cost of doing business through technology from a capital investment to an operational expense. In a nutshell, the government's methods for the acquisition and utilization of IT resources severely limits the potential value that these innovations might bring to the true benefactors of IT in the

government – the taxpayers. A digital government is possible but only if the methods for the acquisition and management of IT resources in the federal government evolve in a manner that keeps pace with innovation.

The federal government has already embarked upon a journey that involves the gradual adoption of these advanced technologies, which include virtualization and cloud computing, to improve the efficiency and agility of many of its data centers. VMware applauds the leadership efforts of the Obama Administration specifically designed to facilitate the migration of federal information technology to a more efficient operating model. Specifically, the Federal Data Center Consolidation Initiative (FDCCI), the Cloud First Policy, and the 25 Point IT Reform Plan together comprise a significant first step. OMB has reported that the FDCCI is expected to save about $3 billion by 2015 and that an estimated 100 services were migrated to the cloud prior to the end of 2012. When the IT Reform Plan was originally released in late 2010, it projected that approximately $5 billion could be saved across the federal government annually. My point is to neither confirm nor question these savings. Rather, my objective is to shed some light on the fact that these savings are only the beginning. These savings represent a small fraction of the potential savings that could be achieved. VMware commends the leadership of both the current Federal CIO and his predecessor, who have played a major role in setting the direction and laying the groundwork for progress to be made. Yet, we also firmly believe that taking the additional and necessary next steps on this journey – and taking cost savings to an entirely new level – requires that much more be done.

Before I describe the challenges and opportunities for the improvement of the IT acquisition and investment strategy in the federal government, I should share a bit of my background because these experiences have shaped my views on the subject. About 12 years ago, I left an executive position with FedEx to serve as the Chief Information Officer (CIO) at the U.S. Patent & Trademark Office. As CIO from 2001 to 2004, we successfully transitioned from completely paper-based to a completely electronic organization. Subsequently, I served for more than 5 years as the Executive Director of one of the federal government's shared services centers. This organization provided a variety of "back-office" services to other federal agencies such as IT, payroll, HR and financial management on a reimbursable "fee-for-service" basis. Of particular relevance to this hearing, this organization also operated one of the assisted acquisition centers that competed, awarded, and administered about $2.5 billion of contracts each year on behalf of other federal agency customers. From my vantage point provided during these rewarding experiences, there are three fundamental challenges that I believe should be addressed in order for the government to effectively leverage advancements in technology and successfully transition to a digital government: complexity, expertise, and culture.

1. **Complexity** – Advances in technology such as virtualization and cloud computing have turned a significant amount of IT products and services into commodities. In addition, these technologies enable major operations to be initiated within minutes, utilized on a consumption model similar to your utility company, and scale to enormous magnitude – or completely released – on a moment's notice. Yet, even as technology has advanced to enable businesses and government to operate in a very dynamic manner, federal IT acquisition rules and procedures have not kept pace. To further exacerbate the situation, the Federal government has a tendency to over-specify requirements in a way that often crosses over into design, based on dated practices and technologies. This increases inefficiency and ensures that what is being acquired will soon be antiquated if not already. Finally, the complexity and sheer magnitude of federal procurement regulations leads to a considerable amount of individual interpretation when carrying out complex acquisition procedures. Thus, acquisitions across the government tend to lack a degree of uniformity and consistency to the point that acquisitions for the same or very similar IT products or services may appear to be quite different depending upon the agency or individuals involved in carrying out the acquisition itself.

2. **Expertise** – The Federal Acquisition Regulation includes more than 50 parts and roughly 1,100 pages. It should not come as a surprise that the sheer volume of information presents challenges for even the most proactive and studious of contracting professionals. It has been widely reported that there is a shortage of qualified IT acquisition personnel across the Federal government. In fact, the Acquisition Workforce Development Strategic Plan for Civilian Agencies – FY 2010-2014[1] demonstrates how the sheer volume of federal acquisitions has grown in recent years. Specifically, spending on acquisitions across the government had grown by 56% or about $50 billion from 2000 to 2008. While keeping pace with this high growth rate presents a significant challenge, the growth in itself is not the underlying issue. Clearly, an innovative approach is necessary to restructure fundamental acquisition operations to improve efficiency and productivity. In addition, the "generalist" approach to acquisition personnel has created an environment where the same acquisition personnel that purchase pencils and janitorial services also purchase technology products and services. This approach is simply not realistic in today's complicated and rapidly changing world of technology.

[1] http://www.whitehouse.gov/sites/default/files/omb/assets/procurement_workforce/AWF_Plan_10272009.pdf

3. **Culture** – The decentralized nature of IT acquisition across the government has created a culture that is detrimental to performance and efficiency. A decentralized organization that has separate and distinct contracting offices embedded within the various operating units across even a single agency is highly inefficient. Supporting infrastructure like facilities and electronic tools is typically duplicated throughout multiple agencies as each contracting office reinvents the necessary supporting infrastructure. This highly distributed model makes it difficult to gather data for analysis and transparency, as well as obtain funding levels sufficient to maintain the required level of expertise.

   In addition, the culture of the contracting operations across government is that of an internal functional operating unit. Perhaps most significant of all these cultural issues, is that the existing forces stifle innovation and "lock-in" an approach to IT acquisitions that is based on legacy technology and methods. The existing culture hinders new and innovative approaches to IT acquisitions such as crowdsourcing, which has the promise of providing the government with access to highly skilled expertise, at a much lower cost, and in a competitive model that substantially lowers risk for some projects such as application development. This overall culture needs to become more services based with built-in incentives for performance and accountability.

Proposed Solutions

The challenges I have presented are deeply rooted in a legacy that has been solidified through legislation, supporting policy and longstanding business practices. As such, the solutions to these challenges must be equally pervasive and comprehensive. I would be remiss if I did not commend many of the efforts already underway to improve IT acquisition and management within the federal government. These are solid improvements and should be fully implemented. Yet, I also caution against the assumption that current efforts are enough to solve all the problems associated with federal IT contracting and management. We need to build on current solutions in order to fully modernize IT acquisitions and management. Addressing these fundamental challenges – complexity, expertise and culture – will require comprehensive and substantial changes to upgrade IT acquisitions and create a cross-government service that embraces innovation to improve quality, timeliness and transparency across the board.

Based on my experience, I believe the objective for this transformation should be to create an IT acquisition environment that is:

1) services based but expands upon existing improvement efforts,

2) utilizes built-in incentives for performance and expertise development, and

3) balances transparency and accountability with customer needs and compliance.

Pursuant towards these objectives, I offer the following suggestions to improve IT acquisitions and management across the federal government.

Solutions to the Challenge of Complexity

By definition, a problem that is complex cannot be resolved easily or with simple solutions. Without a doubt, the entire acquisition environment in the federal government would benefit from simplification. I cannot think of a better area upon which to focus this simplification effort than the acquisition of information technology (IT) in the federal government. I suggest the following three actions toward simplification: simplified acquisition procedures, utilizing cloud services and enhanced consolidation.

Increasing the use of simplified acquisition procedures within performance-based acquisitions would streamline and accelerate the acquisition of IT products and services. The 25 Point Plan for IT Reform identified that about 25%, or $20 billion, of government IT acquisitions could be met by some form of cloud computing approach. The use of cloud computing has been proven to increase efficiency and save money. In 2010, when OMB first proposed that federal agencies adopt a "cloud first" approach to IT procurement, the federal chief information officer projected $5 billion annually in savings. According to an April 2012 survey[2] of federal civilian and defense personnel conducted by the Citizens Against Government Waste, $5.5 billion had been saved through cloud computing, although survey respondents stated that wider cloud adoption could have saved up to $12 billion. The remarkable thing is that these savings are just scratching at the surface of what's possible. The federal government's journey to cloud computing has only just begun. By continuing on this journey, virtualizing and modernizing mission critical applications, expanding the use of cloud automation and management

[2] http://www.cagw.org/sites/default/files/pdf/issue-brief-2012-12-cloud-report-web.pdf

technologies, and building upon the somewhat isolated cloud pilot projects to transition to fully software defined data centers[3]; the federal government could multiply these cost savings by a staggering amount.

Cloud computing products and services, based on the NIST standard definition, must be ubiquitous by their very nature and consumed in a utility like "pay for consumption" model. Hence, IT products or resources in a cloud computing model should be categorized as a commercially available items. The acquisition of these commercial items would lend itself nicely to the increased adoption of performance-based contracting methods such as Statement of Objectives that are linked to performance based results. Through the use of outcome based objectives, the federal government could begin to simplify its longstanding tendency to over-specify requirements in IT acquisitions. Furthermore, the use of performance based contracting methods with well defined service level agreements (SLAs) would also lower the risk of underperforming IT acquisitions and increase accountability for vendors.

Without a doubt, one way to simplify IT acquisitions is to simplify the overall IT environment within which IT products and services operate. Thus, the federal government should continue with the efforts to consolidate and reduce the number of data centers government-wide. But the consolidation effort should not stop there. The same technology that underpins server consolidation, virtualization, can also enable the simplification of the traditional desktop environment and networks as well. Virtual desktops are more secure, easier to administer, and enable end users to access their desktops via multiple devices. This virtual desktop technology also forms the foundation for mobile applications to be accessed in a secure manner via various platforms such as tablets and smart phones. There is no better time to deploy this virtual desktop as a service environment than coincident with a data center consolidation initiative. Also, as data centers and IT solutions are consolidated, opportunities will emerge to also consolidate the model that is utilized to acquire them. In fact, continuing to utilize a decentralized acquisition model to acquire IT is more likely to lead to the continued acquisition of decentralized IT assets, thus working directly against the overall objectives of increasing efficiency across the government's IT environment.

In 2011, VMware conducted a survey of CIOs within the enterprise segment of our customers. This survey indicated that roughly 42% of the IT budgets for these enterprise customers were allocated to maintaining the infrastructure. This is the portion of the budget that the Federal Data Center Consolidation Initiative (FDCCI) is attempting to right-size. This survey also found that another 30% of the IT budgets were allocated to maintaining applications. In other words, VMware's largest customers reported that they spend an average of

[3] http://cto.vmware.com/interop-and-the-software-defined-datacenter/

72% on operations and maintenance activities and 28% on development, which is an indicator of investment in business capability. This data point is consistent with the data gathered by GAO, which indicates that about 71% of the federal IT budget is spent on operations and maintenance and 29% on development. Compare this to leading-edge corporations that have fully embraced cloud computing and application rationalization to lower their IT operations and maintenance costs to less than 60% of their IT budgets. This corresponds to a rate of investment in applications of about 40%, which is almost double the rate of the federal government. My point is that the federal government could increase the cost savings opportunity within the overall IT investment portfolio by focusing upon the rationalization of applications as well as consolidating data centers through the use of cloud computing and other advanced technologies and models.

Solutions to the Challenge of Expertise

The problems that place considerable strain on the acquisition workforce across the federal government have been widely documented. In 2009, OMB released the Acquisition Workforce Development Strategic Plan for Civilian Agencies[4]. This document described how spending on acquisitions across the government had grown by 56% from 2000 to 2008 but the number of qualified IT acquisition professionals had only grown by 24% during that same period. While I do not believe simply increasing the size of the acquisition workforce will solve the problem, we should ensure that the IT acquisition workforce is qualified and productive. Some additional measures would increase the productivity of the federal acquisition workforce – at least those working in centralized IT acquisition centers. I make the following recommendations based on my knowledge and experience: establish an IT acquisition intern program, develop a training curriculum, and leverage a working capital fund.

First, many of the recommendations in the acquisition workforce strategic plan are sound and should be built upon. For example, from my own personal experience as an executive in the federal government, I can assure you that acquisition intern programs are a highly effective means of creating qualified acquisition professionals. Consistent with the establishment of IT acquisition centers, the federal government should also consider the establishment of an acquisition intern program or track that addresses the unique and complex aspects of IT acquisitions. In addition, the government should expand the usage of acquisition intern programs and consider partnerships with universities to develop graduates capable of being productive at graduation. Asking federal

[4] http://www.whitehouse.gov/sites/default/files/omb/assets/procurement_workforce/AWF_Plan_10272009.pdf

agencies that participate in these programs to wait patiently for up to two years while new interns are being minted is simply too much to ask in the existing environment. By partnering with universities for intern programs, the federal government would have access to college graduates that are proficient in their new chosen career in federal acquisitions on day one.

In addition to the expansion of the acquisition intern programs, the federal government should develop a training curriculum specifically to foster expertise among IT program personnel as well. While certification programs already exist for Program Managers and Contracting Officer Technical Representatives (COTRs), these programs should be enhanced to address the complexities and characteristics of IT acquisitions. This approach would also provide the opportunity to clarify and strengthen the role and responsibilities of IT programs in working collaboratively with IT acquisition personnel throughout the entire life cycle of IT contracts. This would also reduce the risk of IT acquisitions through an approach that is focused on managing the entire contract from inception to completion. In addition, training and certification programs should be geared towards the ongoing development of technical expertise to keep pace with advancements in technology such as virtualization and cloud computing. In this manner, IT acquisition and IT program personnel would gain expertise sufficient to complete market research, define the government's requirements, evaluate technical proposals, and administer contract delivery for these advanced technologies. For the purpose of efficiency, such training should be aligned with the specific commodity technologies that any IT acquisition center offers thus ensuring a highly trained workforce for each IT acquisition center.

From a tactical execution standpoint, one of the most significant barriers to a well-trained workforce in a constrained resource environment is lack of sufficient funds. Without a doubt, the highly inefficient and decentralized acquisition model contributes to this phenomenon. In concert with the establishment of a small number of IT acquisition centers, these centers should be authorized to operate using a revolving type of funding mechanism called a working capital fund. Furthermore, these assisted IT acquisition centers should be authorized to charge fees that are in excess of costs by a marginal and capped amount specifically to ensure adequate training and workforce development. Since these revolving funds must meet certain auditability requirements, the use of this approach would be subject to transparency and the rigor of audit oversight. In fact, this approach might just increase the transparency and level of oversight associated with the operations of these IT acquisition centers and operations.

Solutions to the Challenge of Culture

One of the many lessons in leadership that I have learned is that it is not easy to change a culture. Thus, it takes much more than leaders and policy makers urging the workforce to embrace change. Any executive that has had success with culture change knows that a variety of aspects must be addressed, including: organizational matters, processes, and technologies. These three major elements must be transformed in concert and consistently for the change to have a chance of success. Fundamentally, the federal acquisition community on the whole, which obviously includes the IT acquisition community, needs to be transformed from an internal functional culture to a services based culture. Based on my experience, four items would improve culture: a transparent customer-supplier model, a collaborative work environment, crowdsourcing, and effective CIO authority.

It is not possible to have a services approach without a customer and supplier model. Thus, the assisted IT acquisition centers should enter into explicit agreements with customers to clearly define the expectations and desired outcomes. In addition, these centers should publish commitments to customers that clearly specify the timeliness and other performance criteria. In addition, a performance-based approach with built-in incentives should be utilized to ensure quality and results based outcomes. This could be as simple as including well-defined performance objectives within the annual performance plans of the IT acquisition workforce or as aggressive as the establishment of a pay-for-performance system based on measures of success.

I have also learned through experience that the "back and forth" nature of IT acquisitions can make an incentive or performance based approach very difficult to administer. Thus, a collaborative work environment, such as a collaborative tool, should be developed to foster more efficient handling of complex acquisition materials, to track the responsiveness of customers and acquisition professionals alike, and to avoid the "falling through the cracks" that seems to plague the current IT acquisition process when ongoing work changes hands on a repeated basis. To further enhance efficiency and streamlining, this collaborative environment could be augmented to also include best-case-example templates and other materials to avoid every IT acquisition having to "start from scratch." Best-case examples of requirements documentation, statements of objectives, evaluation critera and many other artifacts could be made available via an on-line library. Each assisted IT acquisition center could administer its own library to balance the need to tailor such artifacts to the specifics of the IT acquisition type but to gain the benefit of widespread availability and reuse. Finally, such a tool would provide an unprecedented degree of transparency into the overall timeliness and performance of the IT

acquisition process. With such data, informed continuous improvement efforts can be executed to further streamline and improve performance.

To further take advantage of modern techniques and improve transparency, collaboration, and accountability; the federal government should adopt a technique called crowdsourcing that has entered the mainstream within the software development community on a global basis. Many federal agencies, including NASA and the U.S. Patent & Trademark Office are already using this technique to tap into the best available expertise, in the most efficient manner possible, and within a competitive framework. Using this technique, one or more assisted IT acquisition centers could "bid" on an IT acquisition project and the customer would be able to select the center that best meets their needs in the most efficient manner possible. Much like the site "Angie's List" the IT acquisition crowdsourcing platform could store customer satisfaction information about the centers, acquisition teams, or even the individual IT acquisition personnel, if desired. In this manner, customers proposing to use the services of an assisted IT acquisition center would have transparency into historical performance information that would be used along with cost and other information to decide which center should "win" the job. Through this combination of factors that span organization, processes, and technology; the IT acquisition culture would be transformed to one that is highly responsive and services based.

Finally, I would be remiss if I did not address the role of the CIO within the government as a potentially significant factor in improving the performance of IT programs and acquisitions. As I described previously, when I was the CIO of the U.S. Patent & Trademark Office, we successfully executed a significant transformation from a completely paper-based approach to one that was completely electronic. In less than 3 years, we transformed the operations of the US PTO to include electronic filing, electronic based examination, and electronic dissemination of public patent and trademark information. Through this transformation, we reduced operational paper based handling administrative costs by more than $30 million annually.

Although there were many factors that contributed to this success, I feel very strongly that one very important one was that the US PTO had fully embraced the intent of the Clinger-Cohen Act. As the senior IT executive and top advisor for the Office, I reported directly to the Under-Secretary and I was an equal member of the Executive Committee that ran the operations of the Office. As the top IT executive, I had the lead role in the development of the IT priorities, strategies, and architecture – including the entire infrastructure, networks, applications, test environments, databases, etc. Once the IT budget was approved and allocated, I had the full authority to execute the budget for the purposes it was authorized. With two minor exceptions, all personnel within IT job categories worked within my organization and were accountable to my management team. Without a doubt,

such widespread change that relied so heavily upon technology would not have been possible unless I was a true peer to the program executives such as the Commissioner of Patents, Commissioner of Trademarks and the CFO. In the true spirit of the Clinger-Cohen Act, we worked together as a team of partners to accomplish common organizational objectives. For these reasons, I strongly support strengthening the role and authority of Agency level CIOs to reflect the intent and specifications of the Clinger-Cohen Act. I also suggest that these CIOs be granted multi-year budget authority and working capital funds as necessary tools to facilitate the transition away from capital expenditures to an increased use of operations expenses to fund IT initiatives and programs.

In addition to the factors described above, any CIO must rely upon a tremendous amount of leadership to be successful. The CIO in any organization, small or large, is often at the center of any problem that arises and is associated with the technology program. The sheer breadth of such challenges includes technology issues, contractual matters, budget management, human resources, security incidents, and compliance – just to name a few. On the one hand, the CIO must be a true peer to the other top executives in the agency to facilitate open communications and collaboration as any such issue is triaged and resolved. On the other hand, the CIO must also be accountable to the agency head in such a manner that the CIO is offered the support to overcome the cultural and control challenges that invariably arise as program officials tend to react to losing control over IT decisions and resources. Without a doubt, CIOs must balance innovative technologies and evolving methodologies within the overall context of mission effectiveness and efficiency and in a collaborative manner with their program executive peers.

As the innovation associated with cloud computing continues and the transition to an IT as a Service model evolves, there will invariably be a considerable impact on the role of the IT organization. As consolidation continues, clouds will become more and more connected across organizational lines. As standards for interfaces and portability progress, clouds will become even more interoperable. As cloud computing matures and programs across government embrace them, the IT organization will need to become a broker of services for the agencies they serve. Government CIOs must be in position to effectively carry out their responsibilities in a services brokering model. This means CIOs must be able to develop and enforce policies that encompass the entire scope of the agency's IT programs and they must have access to a cadre of IT acquisition resources and well trained IT experts. Moreover, the overall transparency of internal and external IT service options must be made extremely clear for IT decisions to be made effectively and for the associated risks to be appropriately identified and managed. This is simply not possible without a common framework for the development of accurate cost estimates for all commodity IT services, whether internal or external. In addition, the corresponding service commitments and performance against those commitments must also be completely

transparent and comparable across cloud service providers. Thus, for the CIO to be successful in a brokering role, the technologies must be in place and supported by a business model that includes a standardized way of comparing costs and performance. This business management framework does not exist today and needs to be operationalized across the federal landscape to avoid unnecessary duplication, high variations, and the potential for waste based on invalid decisions.

Closing

In closing, I emphasize that each of the suggestions I have made are geared to work in concert with the other efforts to improve the rate and effectiveness of innovation through technology in the federal government. Technologies such as virtualization and cloud computing have improved mission results and enhanced competitiveness across industries. The federal government has also begun a similar journey. By leveraging such dynamic capabilities, the federal government can also respond very rapidly to changing market conditions without making substantial up-front capital investments in technology. Through the efforts and leadership of many within the government, the transformation to IT as a service has already begun. Yet, the government's methods for the acquisition and management of IT resources constrains and limits the potential results that these efforts could achieve. The transformation to a digital government is possible, but not without evolving the methods for the acquisition and operation of IT resources in the federal government. In summary, my recommendations are as follows:

1. Continue with efforts to consolidate data centers and migrate to the cloud, but build upon them to leverage additional innovative technologies and take the next steps on the journey to IT as a service;
2. Simplify and consolidate the IT acquisition model to one that is services-based but expands upon existing improvement efforts, with built-in incentives for performance and expertise development; and
3. Strengthen and reinforce the role of the CIOs across government to be elevated to more of a peer role with other top executives with full authority to lead and execute their IT programs for the overall benefit of agency wide users and taxpayers.

VMware sincerely appreciates the opportunity share our thoughts and suggestions on this very important matter. We applaud the leadership and vision of the Chairman and Ranking Member to bring this matter to a hearing. VMware looks forward to continuing to participate in efforts to improve the operations and efficiency of the federal government. And we thank you for the opportunity to participate in the panel today.

Chairman ISSA. Mr. Klayko, I understand that you have a flight to catch?

Mr. KLAYKO. There will be another one.

Chairman ISSA. There will be another one.

Mr. KLAYKO. There will be another flight. This is too important.

Chairman ISSA. Thank you. I certainly appreciate it. You are recognized.

STATEMENT OF MICHAEL KLAYKO

Mr. KLAYKO. Good afternoon. I, too, would like to thank you, Chairman Issa and Ranking Member Cummings, for this opportunity to present testimony in today's hearing, for your great work you are doing to reduce waste in Federal information technology spending. I say this as a business leader and an American taxpayer. It is a privilege to be here, so I want to thank you for that.

I served as the CEO of Brocade Communications from 2005 until last week, where the company announced a new CEO. I announced my intention to resign as CEO in August of 2012. And I have been an employee and advisor to the company during this transition period.

I have also had the opportunity to visit Washington, D.C., many times a year as the CEO of Brocade, a well as the former chairman of Silicon Valley Leadership Group, which is an organization of 395 member companies representing Silicon Valley's largest companies. As the chairman of that group, collectively we employ 1.6 million Americans and have a market cap of about $2 trillion. So I am honored to speak with you today not just representing my company but the people also in the valley. I hope with my experience that I have had in the past since being in technology since 1975, I can share some of the things that have been of interest to us that should be of interest to you.

I would also like to share Brocade's experience with the way Federal government acquires IT equipment and services. My perspective is that of the CEO chartered with managing the growth of a company. Brocade is a true Silicon Valley startup: Four guys, a keg of beer, and an idea, and a dog in 1995. And now 2-plus billion dollars, we compete on a world stage. I truly believe we are an American treasure as we face fierce competition everywhere we go and we win. We sell about $250 million a year annually of network technology to the Federal government, and they are the backbone of the Nation's critical infrastructure.

Some of the challenges we see today are outlined, obviously. But when Federal agencies rely on a single OEM, or original equipment manufacturer for IT solutions like networking, server, storage technology, and the like, it creates situations where the majority of the spending goes to supporting legacy environments. Those legacy environments in equipment, operations and maintenance. This is wasteful, denies Federal agencies the benefits that come from more competitive and innovative environments.

One common practice that we have observed in Federal IT procurement is the use of brand name or equivalent requirements. I want to be clear. There are many situations where you need to specify a particular product or brand. In those case, sole-source jus-

tification can be made when no other technology is available to meet the requirements.

But I am not talking about those cases. Instead, I will focus on the cases where Federal procurement purchasing organizations use brand name requirements in requests for proposals, request for quote, technical reference models. An example, device is listed by name and part number, example, ABC Router 2000, to signal the type of technology being sought in the bid and it is followed by the phrase "or equivalent."

Brand name or equivalent requirements incorporates all the features and function of a particular brand product, however, all these specific features and functions may not actually be needed by the agency to meet the mission, therefore putting the agency in a position for paying for features and functionality that are not necessary.

Systems integrators see brand name or equivalent requirements and they don't want to use non-ABC products in their bids. First, they are concerned that the technical committee will reject the proposal if the package does not include the specific ABC product, therefore eliminating them from the opportunity to secure a bid. They are also concerned with the extra time and effort needed on their part of the technical committee evaluation.

And second, many Federal contracts have specific delivery dates and they fear that testing an alternative solution may cause a delay in the project, thus eliminating them as a possible provider of an alternative solution.

In the purchase of information technology, this creates a perception of bias and limits the technology that integrators and value-added resellers can provide and will provide. The combination of these proprietary features of the brand, the bias created, and the fear of losing dramatically limits the available alternatives and hampers the ability of government contracting officials to fairly evaluate solutions.

Ultimately, depending on a single OEM for a majority of any IT solution increases the cost in two important ways: Limiting competition, missing out on innovation.

So there are options that can be considered, such as open industry standards. When acquiring IT equipment and services, Federal agencies should seek out features, functions, and capabilities relying on open industry standards to maximize competition and innovation. We hope that you will continue to support that.

I have many examples that I would like to share in a question-and-answer session. But I would like to thank you for this testimony today. Look forward to questions and continued discussion.

Chairman ISSA. Thank you.

[The statement of Mr. Klayko follows:]

Testimony by Michael Klayko, Advisor and Former CEO

Good afternoon. I'd like to thank Chairman Issa and Ranking Member Cummings, as well as the members of the Committee, for inviting us to present testimony in today's hearing and for your work to reduce waste in federal Information Technology (IT) spending. I say this both as a business leader and as a taxpayer!

I served as CEO of Brocade Communications Systems Inc., from 2005 until just last week when the Company announced a new CEO, Lloyd Carney. I remain an employee and advisor to the company during this transition period. I have visited Washington DC several times a year and am honored to speak with you today. Prior to Brocade, I held executive roles at other high-tech companies and I have a deep understanding of, and direct experience with, the kinds of issues I believe you're interested in discussing.

Today I would like to share Brocade's experience with the way the federal government acquires IT equipment and services. My perspective is that of a CEO chartered with managing the growth of a company. Brocade is a true Silicon Valley start-up: what started as an innovative idea from four guys with a dog and a keg of beer became a $2 plus billion company that leads in its market through innovation and fierce competition. Brocade sells more than $250 million dollars annually of network technology to the federal government. These technologies are the backbone of our Nation's critical infrastructure.

What challenges do we see today?
When federal agencies rely on a single original equipment manufacturer (OEM) for IT solutions – like networking – it creates a situation where the majority of spending goes to supporting legacy environments in equipment, operations, and maintenance. This is wasteful and denies Federal agencies the benefits that come from more competitive and innovative environments.

One common practice that we have observed in Federal IT procurement is the use of "brand name or equivalent" requirements. I want to be clear: we agree that there are situations where you need to specify a particular brand or product, and in those cases a sole source justification can be made when no other technology is available to meet the requirement. But I am not talking about these cases today.

Instead, I'd like to focus on cases where federal purchasing organizations use brand name requirements in Requests for Proposal (RFPs), Requests for Quote (RFQs) or Technical Reference Models (TRMs). An example device is listed by name and part number (for example, the "ABC Router 2000") to signal the type of device or technology being sought in the bid, and that is followed by the phrase "or equivalent".

Brand name or equivalent requirements incorporate all the features and functions of a particular brand name product. However, all of these specific features and functions may not actually be needed by the agency to meet its mission.

I'll give you a simple example that involves something I love: fly fishing. The fishing rod manufacturer I like adds a lighted reel and rod tip to the rod. Granted, it's a more expensive rod, and it would likely have a higher maintenance cost. It certainly doesn't make me a better fisherman, but I kind of like it anyway. Now, when my friends are looking to buy fishing rods, they ask me which one I use and I tell them. They don't need a lighted tip or reel on the rod either, but they end up with one anyway. They probably spent more than they needed to, and maybe they missed out on an even more recent development – like the solar-powered lights versus a battery powered or fluorescent, who knows?

System integrators see brand name or equivalent requirements and they don't want to use non-"ABC" products in their bids. They're concerned that the technical committee will reject the proposal if the package does not include the specific "ABC Router 2000." They are also concerned with the extra time and effort needed on the part of the technical evaluation committee to evaluate a different offering.

In the purchase of information technology, this creates the perception of bias and limits the technology that integrators and value added resellers can provide. The combination of the proprietary features of the brand and the bias created dramatically limits the available alternatives and hampers the ability of government contracting officials to fairly evaluate solutions.

Ultimately, depending on a single OEM for the majority of any IT solution increases costs in two important ways: (1) by limiting competition, and (2) by missing out on innovation.

(1) Competition – let me give you an example:
Within the DOD, the Army's Installation Information Infrastructure Modernization Program (I3MP) and the Air Force's Combat Information Transport System (CITS) program both require in their TRM that a vendor must be Joint Interoperability Testing Center (JITC) Certified. They do not use brand name device examples, but instead rely on the JITC to ensure a product meets security and other mission critical requirements. If a vendor's products are on the JITC list they can be included on a bid for these programs. This has opened competition and now the Army sees bids with improved pricing on hardware compared to civilian agencies.

(2) Innovation: Another example:
Some federal agencies frequently reference a specific product in a TRM that is now 12 years old. I'm from Silicon Valley, where we live by Moore's Law. The pace of innovation in IT is such that performance, reliability, and energy efficiency improvements introduced in the last 18 months or less can provide superior advantages. Even when purchasing agents or end users request access to newer technology, they can often be denied the ability to acquire products not specifically named in a TRM.

There is a solution to all of this – open industry standards
When acquiring IT equipment and services, federal agencies should seek out features, functions and capabilities – relying on open industry standards - to maximize competition and innovation. We see an effort to promote and support greater technical expertise and resources for procurement officers

in the Chairman's draft bill and we think this will go a long way to helping the situation. Federal agencies should establish whenever possible a set of publicly available specifications against which manufacturers can test and certify their products.

We see another great example in the Department of Veterans Affairs (VA) memo of August 17 2012 entitled: "Open Standard Protocols for VA Networks". This memo describes the decision to migrate from proprietary protocols to open standard protocols on the VA's data networks, in order to enable participation from any vendor. All of this will support cost containment strategies and increase the VA's flexibility and ability to interoperate with multiple vendors.

We're not the only ones saying this either. A Gartner report from 2010 called "Debunking the Myth of the Single-Vendor Network" showed that there is no financial, operational, or functional basis for the argument that a single-vendor network will lower the total cost of ownership for a network infrastructure. They go on to say, in fact, that introducing competition into your network decision process will lower your capital and maintenance costs by a minimum of 30%.

In closing, the use and adoption of open industry standards and multi-vendor networks by federal agencies will reduce costs, increase competition, promote innovation, facilitate interoperability, and provide greater return on investment. The Federal government can send a powerful signal to the IT industry that it values innovation and competition. This will benefit the U.S. economy by encouraging continued investment in R&D, placing value on intellectual property, and creating IT sector jobs in the United States. These practices also drive innovation that sparks new ideas that lead to new companies. These practices reduce waste and promote efficiencies.

Thank you for the opportunity to testify before you today. I look forward to your questions and our continued discussion.

White Paper:

"The challenges and benefits of greater competition in federal IT procurement"

Federal agencies face a range of requirements for information technology infrastructure and must work diligently to design and implement strategic roadmaps that will serve the technology needs of their constituencies for years to come. Limits on budget consistency and visibility introduce additional burdens to planning and implementation. The requirement to provide more and better services for citizens while decreasing the cost of providing those services is a challenge and top priority facing all Federal agencies today.

Federal purchasing organizations frequently are provided and forced to use name-brand requirements when publishing Requests for Proposals (RFPs), Requests for Quote (RFQs) and/or Technical Reference Models (TRMs). In these cases, an example device is listed by name and part number (e.g., the ABC Router 2000) to signal the type of device or technology being sought in the bid. In other cases, the RFP may be brand-name agnostic while referring to a TRM that contains brand name devices as examples.

Brand name or equivalent requirements incorporate all the features and functions of a particular Brand name product. All of the features and functions provided by the brand name product may or may not be an actual requirement needed by the Federal agency to meet its mission. This limits competition and restricts solution innovation. Federal agencies should whenever possible state and evaluate in terms of generic features, functions and capabilities including open industry standards to maximize competition and innovation for information technology solutions.

System integrators and others in the prime contractor role see Brand name or equivalent requirements and are unlikely to include ABC competitors' products in their bids for fear of being rejected. They are concerned that the technical committee reviewing the bid will reject the proposal for not meeting the TRM specifications if the package does not include the specific ABC Router 2000, in this example. They are also concerned with the extra time and effort needed on the part of the technical evaluation committee to evaluate a non-brand name offering and the increased complexity in evaluation process lessens their chance of winning. In many cases the RFP and RFQ is being issued on the premise of commercially available information technology products or services and being evaluated on a lowest price technically acceptable basis where no evaluation teams or committees are set up to evaluate the offers.

Relying on brand-name requirements instead of functional requirements denies federal agencies two important benefits: cost savings and access to innovation.

<u>Cost savings</u>

Within the DOD, the Army's Installation Information Infrastructure Modernization Program (I3MP) and the Air Force's Combat Information Transport System (CITS) program both require in their TRM that a vendor must be Joint Interoperability Testing Center (JITC) Certified. They do not use brand name

device examples, but instead rely on the JITC to ensure a product meets security and other mission critical requirements. If a vendor's products are on the JITC list they can be included on a bid for these programs. This has opened competition and now the Army sees bids with improved pricing on hardware compared to civilian agencies.

Innovation

Purchasing agencies also miss out on recent innovations when they refer to a specific brand names and products in TRMs. For example, some agencies frequently reference a specific product in a TRM that is now 12 years old. While familiarity with a specific product can be beneficial, the pace of innovation in IT is such that performance, reliability, and energy efficiency improvements over 12 years can provide superior advantages. Even when purchasing agents or end users request access to newer technology, they can often be denied the ability to acquire products not specifically named in a TRM.

Federal IT purchasing practices should be adapted to take advantage of functional requirements in TRMs and Requests for Proposals. This practice, already proven effective within some DOD agencies and recognized as a valuable policy direction in the VA, would result in cost savings and the benefit of greater technological innovation inside the federal government. Relying on name brand requirements limits the ability of primary contractors to seek out the most competitive solutions for the purchasing agency.

Support for multi-vendor networks, open standards, and competition in IT procurement

Memo from Roger Baker, CIO, VA: "Open Standard Protocols for VA Networks"
Release date: August 17, 2012
Key statements:

- This memo codifies the decision to migrate from proprietary protocols to open standard protocols on VA's data networks, in order to enable participation from any vendor.
- Migrating to open standard protocols supports cost containment strategies, and will increase VA's flexibility and ability to interoperate with multiple vendors.
- Leaders in new technologies are constantly changing - improved interoperability, innovation and open competition will enable rapid advances in network infrastructure capabilities at the lowest possible costs.

Gartner report: "Debunking the Myth of the Single-Vendor Network"
Publication Date: November 17, 2010
Key findings:

- The idea of a single-vendor network has been promoted by Cisco as a way to simplify operations, ensure reliability and lower the total cost of ownership (TCO) for a network infrastructure. However, it is clear that in most cases today there is no financial, operational or functional basis for this argument.
- Introducing competition into your network decision process will lower your capital and maintenance costs a minimum of 30%.

Case studies highlighting non-competitive trends in Federal IT procurement

Federal Bureau of Investigation - Solicitation Number FBI-12-17-Cisco
Posted July 9, 2012
Amount: $830M over five years

Description: Solicitation for multiple purchases of brand name specific Cisco networking equipment, hardware maintenance, software support and engineering support for the entire FBI
Non-competitive attributes:

- The FBI is operating under several flawed assumptions: 1) maintenance and support for old Cisco equipment will cost less than the purchase of new equipment from other vendors, 2) acquiring vendors other than Cisco will result in security vulnerabilities, and 3) pursuing competitive equipment alternatives would lead to schedule delays.

U.S. Air Force - Base Area Network (BAN) Functional Specification
Published January 2012
Amount: impacts the several hundred Air Force installations in the U.S.

Description: Provides standard network design, configuration and best practice information to facilitate the transition to a single vendor for network infrastructure equipment at every Air Force base.
Non-competitive attributes:

- The Air Force erroneously contends that a single-vendor network is needed to facilitate the operation and management of its base networks; it also fails to consider the risks added by relying on a single vendor, including limited supply chain availability and diversity, security issues, functional limitations, and base-to-base inconsistencies.

U.S. Army - Solicitation Number HC1028-12-R-0045
Posted May 10, 2012
Amount: $578M over five years

Description: Solicitation for Cisco SMARTnet maintenance coverage for the Army's Cisco assets. Also establishes an enterprise license agreement to consolidate existing Cisco SMARTnet contracts.
Non-competitive attributes:

- The Army fails to recognize that older proprietary Cisco technology can be replaced with newer, more efficient and capable standards-based technology at a cost less than the current support cost for older Cisco technology. The RFP specifically limits consideration of alternative routing and switching solutions that are available from a number of network suppliers.

Chairman ISSA. Mr. Niehaus?

STATEMENT OF CHRIS NIEHAUS

Mr. NIEHAUS. Chairman Issa, Ranking Member Cummings, and distinguished members of the committee, good afternoon. My name is Chris Niehaus, and I appreciate the opportunity to discuss the government's IT investment strategy.

I am the director of Microsoft's U.S. Office of Civic Innovation, and my team focuses on delivering innovative solutions to government customers. I hope Microsoft's extensive experience helping public and private sector customers around the world will help this committee.

Microsoft supports the committee's goals of reducing the cost of legacy systems, decreasing duplication, utilizing cost-effective commercial technologies, and maximizing best value. Our experience has taught us three lessons that support these goals. Number one, agencies can reduce IT costs by not only reforming how they buy IT, but also by more effectively assessing and management existing assets. Number two, successful IT solutions result when the private sector collaborates with government to provide commercial devices and services to meet agency missions. And number three, the government gets the best value when it uses full and open competition and clear, mission-focused requirements.

As to the first lesson, to reduce IT costs, GAO reports confirm that better management of existing assets is just as important as reforming the acquisition process. A great way to improve IT asset management is making the OMB-recommended operational assessments and inventories mandatory for CIOs and requiring them to analyze existing assets, needs, and new technologies when starting major IT acquisitions.

An instructive lesson from the private sector is that problems are best solved closest to the mission, which is the case would mean keeping reform efforts at the agency CIO level.

We in industry can help with IT asset management. Gartner studies show that agencies can lower total costs of ownership, up to $2,500 per year, per desktop, simply by better managing technologies they already own. They can further lower costs up to an additional 30 percent by using virtualization technologies to move certain applications and desktop functions, like Microsoft Office, to the cloud. Agency CIOs tell us that they favor the flexibility of cloud-based delivery because it helps them move their IT investments from rigid capital budgets to operating expenses. And industry can also agencies consolidate resources where appropriate. For example, the Microsoft Joint Enterprise Licensing Agreement, or JELA, recently signed with the Army, Air Force, and DISA addresses common needs of each licensee while still addressing unique DOD security requirements.

As to the second lesson, agencies can buy more cost effectively by making smarter use of commercial IT, which costs less and often performs better than custom IT. The key is close and early collaboration among agency CIOs, procurement officers, and industry beginning when the government first starts developing requirements so that it can better understand commercial market capabilities

and avoid the familiar problem of drafting requirements behind closed doors and hoping that the market will deliver.

As an example of strong collaboration, we are working with the Air Force to determine how Microsoft's Xbox Kinect, a motion-sensing game controller that costs about $110, can be used to serve as a rehabilitation tool for wounded warriors. Such creative and agile collaboration would be less possible if the government went back to centralized government-wide IT acquisition models.

Similarly, it would make it harder for the government to get the best that the commercial marketplace has to offer by adopting new acquisition structures focused on so-called commodity IT. In my experience, the term commodity IT is not used in the commercial market. Not even something as ubiquitous as email is treated as a commodity. The recent GSA email-as-a-service blanket purchase agreements, or BPAs, distinguish seven different types of cloud email, depending on security and other requirements. Moreover, unlike pencils, paper, and other true commodities, agency missions and information technologies never stop evolving.

And as to the third lesson, best value means more than simply lowest initial cost. Rather, agency CIOs should be required to make best-value determinations in a technology-neutral fashion, avoiding preferences for any particular license model and using a set of core factors, including total cost of ownership, security, privacy, accessibility, record integrity, data portability, and openness of standards.

Agency CIOs should also be empowered to prioritize among these factors based upon the mission being supported. When agencies are clear about which factors will be prioritized and what requirements must be met, industry can and must be equally transparent about how our devices and services satisfy the government's requirements.

In conclusion, Microsoft looks forward to working with Congress in this critically important area. Together, I am confident we can provide IT solutions that will maximize best value and decrease total cost of IT ownership across agencies.

I thank you and look forward to answering your questions.

Chairman ISSA. Thank you.

[The statement of Mr. Niehaus follows:]

Statement of Chris Niehaus

Director of Microsoft's U.S. Office of Civic Innovation,
Microsoft Corporation

Improving Management and Acquisition of IT Investments

Testimony Before the
Committee on Oversight and Government Reform
U.S. House of Representatives

Hearing on "Wasting Information Technology Dollars: How Can the Federal Government Reform its IT Investment Strategy"

January 22, 2013

Chairman Issa, Ranking Member Cummings, and distinguished Members of the Committee: Good afternoon. My name is Chris Niehaus, and since 2009 I have been the Director of Microsoft's U.S. Office of Civic Innovation. My team focuses on developing and delivering new and unique solutions in the Government, Education and Healthcare communities. We have developed, for example, a cloud-based 3-1-1 system for citizen access to municipal services, and we are adapting a gesture-tracking gaming device to help with injury rehabilitation for wounded warriors and to help detect improvised explosive devices. Additionally, I work extensively with Public Sector customers on technology efficiency and optimization initiatives, from the evaluation and adoption of Cloud Services to the modernization of end user experiences through Mobility and Virtualization technologies. Before becoming Director of Civic Innovation, I was a Director of Technical Sales in our Federal Government business where I launched Microsoft's first Cloud email and collaboration service (the precursor of our current Office 365) and focused on working with government customers to drive efficiency in Systems Management and Desktop Optimization. I appreciate the opportunity to be here today to discuss the Government's management and acquisition of IT investments.

While my experience at Microsoft has focused on public sector customers, that work is informed by Microsoft's broader experience supporting public and private sector customers, large and small, around the world with diverse requirements, sensitivities and constraints. I hope that my practical experience working with both private and public customers will aid the Committee in its consideration of the Government's IT investment strategy.

Before I address areas for improvement, I'd like to commend the steps the Government has taken to optimize costly data centers, cancel troubled custom-designed IT programs, and coordinate a standardized approach for determining the security of cloud-based services. We also support the Committee's goals of reducing the Federal Government's cost of operating and maintaining legacy systems, decreasing duplicative technology, utilizing more cost-effective commercially available technologies, and maximizing the value federal customers receive from their IT assets. At a time when Government agencies must justify and extract maximum value from every dollar they spend, Microsoft's experience repeatedly validates three lessons that support these goals: 1) agencies can decrease the cost of expensive existing IT assets, as well as avoid unnecessary acquisitions, by more effectively assessing and managing existing technology, 2) the most successful and cost-effective IT solutions result when the private sector collaborates with agency CIOs and procurement officials to provide commercially available technologies in a way that meets agencies' unique needs, and 3) the Government is able to obtain the best value when IT is acquired based on principles of full and open competition, and the evaluation factors are clearly defined. These three points help us assess the promise and cost-effectiveness of both existing and pending Federal IT procurements, and inform our views on IT acquisition reform efforts. I hope they will provide you with ideas on how to craft effective legislation in the IT procurement area.

I. Government decreases the cost of expensive existing IT assets, as well as avoids unnecessary acquisitions, by more effectively assessing and managing existing technology.

The Committee is right to focus on "IT investment strategy" today, and not simply acquisition. Though there is room for reform when it comes to acquiring IT assets, as I will discuss, recent

GAO reports show that an equally important area of focus for cost savings is the better utilization of existing IT assets. Such improved utilization practices can, in turn, facilitate more effective acquisitions in the future. In one report dealing with IT operations and maintenance expenditures, GAO focused on the need for agencies to make better use of oversight mechanisms under the Clinger-Cohen Act (e.g., operational assessments) to manage existing IT assets more efficiently. This is particularly important given that GAO found that the "significant majority" of federal IT spending goes towards the operation and maintenance of existing technology, rather than new technology acquisitions.[1] In my experience, spending money on existing technology is not necessarily a problem, so long as that spending is being done on technology that is well managed and continually integrating the latest technological innovations.

In another report, GAO noted that cost savings can result when agencies review and analyze more rigorously the performance of existing IT investments.[2] GAO suggests that review and analysis of existing IT investment is weak, largely because agency risk assessments leave important data out of their analysis. On the other hand, the GAO has noted occasions where agencies have decreased duplicative technology by reviewing portfolios of existing IT investments.[3] These reports validate Microsoft's experience that better management and evaluation of existing IT assets can greatly enhance efficiency.

There are a number of opportunities for the Federal Government to strengthen its process of assessing and managing existing federal IT assets. First, it could make mandatory the OMB recommendations that agencies should assess the operation and performance of existing IT assets based on seventeen key factors. This would address the GAO's concern that such evaluation is not being performed consistently. In line with this, we applaud efforts to require agencies to engage in government-wide inventory of existing assets, including those in the National Defense Authorization Act of 2012. Agency CIOs, working with the CIO Council and OMB, are well situated to perform the type of analysis, inventory, and management of existing IT resources that GAO recommends should be more rigorously implemented. The effectiveness of this process is heightened by establishing one CIO within each agency.

Second, we believe it makes sense that agency CIOs should perform a business case analysis evaluating current assets, existing needs, and new technologies to increase efficiency, before making IT acquisitions of a certain magnitude. This would decrease the likelihood of duplication and more closely mirror the private sector's continual focus on identifying and evaluating alternatives for reducing the total cost of ownership. In addition, this process would be superior to requiring that such analysis be performed on a government-wide basis by a single outside agency that would lack a CIO's intimate awareness of the needs and resources of a particular agency. Giving heightened budgetary authority to agency CIOs over IT acquisitions

---

[1] GAO, *Information Technology: Agencies Need to Strengthen Oversight of Billions of Dollars in Operations and Maintenance Investments*, GAO-13-87 (Washington, D.C.: October 2012).

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

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

would help, ensuring that officials who are most aware of existing IT assets and needs are empowered to make the necessary acquisitions.

This discussion should not focus solely on what the Government alone can do better. Obviously, we in the private sector have an important role to play. Based on my experience, I know that industry can and regularly does assist agencies in the goal of better managing existing assets, as well as constantly evaluating new technologies that can increase efficiency. Industry can provide IT solutions that decrease duplicative technology and empower a Government buyer to make smarter decisions. Here, an important part of the answer lies in new, cloud-based delivery models that allow agencies to dynamically select and consume the IT they need. This is but one benefit of cloud computing, which offers federal customers IT that is always kept up to date at the cloud provider's location, thus making the update process transparent and convenient for the end user. Files and data can be stored remotely and automatically backed up. A move to the cloud enables agencies to modernize and better control their IT resources and to do so within their operating expense budgets rather than through large capital expenses. However, it is important that federal customers make thoughtful and accountable decisions when selecting cloud computing service providers to make sure that trusted vendors will protect the Government's highly sensitive data. In addition, while the cloud offers many efficiencies, it is not a substitute for federal departments and agencies effectively managing their own networks. Even machines and devices that use cloud services over Federal Government networks must be authorized, secured, updated, and otherwise properly managed.

Industry can also help agencies reduce the costs of existing assets by providing solutions that modernize back-end technology and facilitate best practices for better managing these assets. In fact, reducing the costs of operation and maintenance of legacy systems may not be so much a problem of bad or outmoded software as it is a matter of smarter management and deployment of IT assets. For example, in a 2011 report, Gartner, a technology research firm, found that if software configuration and user customization are managed at the system administrator level, operating and maintenance costs can be nearly halved in comparison with leaving user PCs unmanaged.[4] The report also noted that money is often wasted on under-implemented management systems, and that software ownership costs are by themselves a small fraction of the total cost of ownership. Through appropriate use of inventory controls and configuration management, the report found, the average total cost of ownership per PC can be reduced from $5,795 to $3,310 per year.[5] Further, with adoption of Application and Desktop Virtualization Technologies when mission-appropriate, total cost of ownership per PC can be reduced another thirty percent.[6] Industry can work with individual agencies to assess the best strategies for

---

[4] Frederica Troni et al., *Desktop Total Cost of Ownership: 2011 Update*, Gartner Report No. G00208726 (November 16, 2010).

[5] *Id.*

[6] Frederica Troni & Terrence Cosgrove, *Total Cost of Ownership of Traditional Software Distribution vs. Application Virtualization, 2011 Update*, Gartner Report No. G00211177 (March 17, 2011); Frederica Troni & Mark A. Margevicius, *Total Cost of Ownership Comparison of PCs With Server-Based Computing, 2011 Update*, Gartner Report No. G00209456 (December 14, 2010); Frederica Troni et al., *Total Cost of Ownership Comparison* (continued...)

achieving such savings given each agency's particular missions and needs, and the Government can make sure that CIOs and acquisition officials have the flexibility and incentives to implement those strategies.

Finally, industry can provide solutions that enable agencies to optimize resources in a way that is tailored to agencies' specific missions. For instance, the private sector has deployed innovative solutions that have greatly increased the efficiency of commercial data centers.[7] Similarly, to take an example from my recent experience, the Army, Air Force, and Defense Information Systems Agency were able to save an estimated $100 million per year[8] by entering into a Joint Enterprise Licensing Agreement or JELA to access the latest Microsoft technologies and support IT priorities such as datacenter optimization, standardization, interoperability for all three agencies, and utilization of cloud computing. However, this example also illustrates that consolidation must be done with each agency's business needs and strategic goals in mind. The Army-Air Force JELA was a successful effort because the CIOs communicated about their resources and needs and worked directly with industry to produce a solution that made sense for their specific situation, including special security needs for the Department of Defense. Such consolidation would be ill-advised if the result is to compromise any agency's mission or unique requirements.

II. Agencies are able to acquire the most cost-effective and successful IT solutions when industry is able to work collaboratively with agency CIOs and procurement officials to bring to bear existing commercial technologies and tailor those technologies to meet agency-specific missions and needs.

Not only is the Government generally required to purchase commercial items when available and to perform market research to determine if such items are available,[9] but experience has shown that the purchase of such products can provide effective IT solutions at a significantly lower cost

---

of PCs With Hosted Virtual Desktops, 2011 Update, Gartner Report No. G00209403 (December 14, 2010).

[7] For example, Microsoft's recently expanded or newly built data centers make use of air-side economizers to improve cooling efficiency, and have made other impressive improvements in energy efficiency and service continuity. Christian Belady, *2012's Big Moments in the Microsoft Cloud* (December 31, 2012), http://www.globalfoundationservices.com/posts/2012/december/31/2012s-big-moments-in-the-microsoft-cloud.aspx (last visited January 16, 2013). Mark Forman, former administrator for e-government and IT at OMB recently said that the predominant approach to data center consolidation used by the Government will result in little net savings. Frank Konkel, *Forman: FDCCI Cost Savings Are 'Smoke and Mirrors,'* FCW (November 29, 2012), http://fcw.com/articles/2012/11/29/fdcci-savings.aspx (last visited January 17, 2013).

[8] Tim Greene, *DOD Saves $100M a Year with New Microsoft Licensing Deal*, Network World (January 4, 2013), http://www.networkworld.com/news/2013/010413-dod-microsoft-265517.html (last visited January 17, 2013).

[9] *See* Federal Acquisition Streamlining Act of 1994, Pub. L. No. 103-355, 108 Stat. 3243 (1994); FAR Part 10.

than custom IT developed specifically for an agency. It is in the Government's best interest to acquire such custom-made solutions only when commercially available solutions are clearly inadequate to meet Government requirements. The history of federal IT procurement provides many examples of agencies' well-intended custom IT development programs that were wisely scrapped due to high cost, low performance, or both.[10]

However, for the Government to successfully utilize commercially available technologies, it must also buy commercial items in as commercial a manner as possible. For this to occur, agency CIOs, the CIO Council, procurement officers, and industry must collaborate more closely to fully understand the commercial abilities of the private sector. As emphasized by the Office of Federal Procurement Policy and the previous U.S. CIO,[11] such collaboration is particularly important when Government is developing its requirements for future acquisitions, so that the Government understands what can be obtained from the commercial market in current form or in a manner that can be customized to agency needs. Facilitating direct communication between industry and agency CIOs is critical, as CIOs are uniquely aware of the IT needs of their own agencies and can communicate those needs when they report to the CIO Council, as they are required to do.[12] This creates an opportunity for identification and coordination of similar needs, as well as innovation and customization to meet unique needs.

In my own work, I have seen how industry can work with agencies to adapt commercial devices and services to meet the myriad missions that the Federal Government must accomplish. For example, in response to the Air Force's need for better and more affordable rehabilitation tools for our wounded warriors, Microsoft and the Air Force are currently collaborating to identify ways in which the Xbox Kinect, a mass-market, off-the-shelf game controller which, unlike traditional hand-held controllers, recognizes movements, gestures and speech, can be adapted to meet the specialized needs of the Air Force's medical community as a rehabilitation tool for our wounded warriors. The Xbox Kinect costs about $110 on the mass commercial game market, yet given its substantial development costs, it would cost orders of magnitude more than that if marketed exclusively as a medical rehabilitation device. We are also exploring how to use Kinect technology to help our warfighters in other ways, such as helping defeat IEDs, and we are

---

[10] For example, in 2010 the OMB halted the acquisition of all federal IT financial systems because agencies were purchasing custom built financial management packages that "too often cost more than they should, t[ook] longer than necessary to deploy, and deliver[ed] solutions that [did] not meet [an agencies] business needs." Office of Management and Budget, *Memorandum for Heads of Executive Departments and Agencies* (June 28, 2010), available at http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m-10-26.pdf.

[11] Office of Federal Procurement Policy, *'Myth-Busting 2:' Addressing Misconceptions and Further Improving Communication During the Acquisition Process* (May 7, 2012), http://www.whitehouse.gov/sites/default/files/omb/procurement/memo/myth-busting-2-addressing-misconceptions-and-further-improving-communication-during-the-acquisition-process.pdf; Vivek Kundra, U.S. Chief Information Officer, *25 Point Implementation Plan to Reform Federal Information Technology Management* (December 9, 2010), https://cio.gov/wp-content/uploads/downloads/2012/09/25-Point-Implementation-Plan-to-Reform-Federal-IT.pdf.

[12] *See* 44 U.S.C. § 3603(b)(4).

working under a cooperative agreement with the Army to use Kinect technology to help estimate potential threat levels from pedestrians. These examples illustrate how economies of scale in the commercial market can be leveraged to meet the highly specific needs of federal customers.

We commend efforts by the Government to encourage agencies to optimize and modernize their IT resources using creative collaboration with industry to identify and adapt the best available commercial technology. We also support efforts such as FedRAMP, to provide standardized approaches for determining the security of cloud-based services.

We would caution, however, that a top-down, lead-agency IT acquisition model should be avoided. Centering acquisition authority in one outside agency that does not intimately understand the specific needs of individual agencies could create a needlessly cumbersome process that could make it more difficult for industry and agency customers to work together in an agile and creative way to meet mission needs.

We also recommend that the Government avoid mandating any new acquisition structures focused on procuring so-called "commodity IT," for several reasons. First, it is not clear what precisely is meant by the term "commodity IT," or why an additional term beyond "commercially available off the shelf" (COTS) is needed. To the extent that there is an assumption that IT services or devices could be generically interchanged, there turns out to be very little IT that is truly a "commodity." Even widely used IT technologies are rarely so generic that they can be bought interchangeably like pencils or copier paper. Something as ubiquitous as email is not a commodity, as demonstrated by GSA's recent awards for email-as-a-service, where GSA appropriately designated seven different varieties of email service, depending on the privacy, security, cost and other legal and mission needs of specific agencies. In our experience, the email needs of a soldier on the battlefield with a disconnected device, for example, are vastly different from those of a field inspector for the USDA or a criminal justice official making communications with a prosecution task force. The best-value email solution for each of these users will be quite different, and procurement policy should not only recognize that, but encourage industry and Government to tailor solutions when appropriate.

Second, products such as pencils or cleaning supplies are static and do not undergo the rapid, nearly daily technological change that cloud-based services undergo. Assuming that an IT service is static and not evolving is no more valid than assuming that the mission of a Government worker is static and not evolving.

Third, attempting to categorize certain IT products as a commodity overlooks the increasing prevalence of "IT-as-a-service," which by moving more IT into the cloud makes IT an operating expense, rather than a capital expense, thus enabling it to be re-scaled and redeployed very quickly. Implementing procurement policy that ignores this trend, which is being adopted aggressively within the private sector, would run counter to emerging industry best practices and decrease the Government's ability to obtain the most effective IT solutions. For this reason, strategic sourcing, a system typically used for items that truly are commodities, such as office or cleaning supplies, is less likely to be effective or even necessary in the realm of information technology.

Industry is ready and eager to bring to bear best-in-class commercial IT solutions to meet agency missions, and we and our competitors work every day to out-innovate each other in this regard. But a model that focuses on commodity IT may actually cut against the benefits that can be realized by purchasing commercially available IT. Devices and services available on the commercial market have varying levels of complexity and quality. The commercial market provides a wide range of options for agencies to select and adapt IT solutions that meet an agency's specific needs. Policies that require agencies to procure cookie-cutter technology based on a one-size-fits-all standard would ignore many commercially available and cost effective solutions that can better meet the needs of agencies, and might keep some sophisticated commercial innovators out of the federal market.

III. Federal customers receive the greatest return on an IT investment when the focus is on the total life-cycle cost of ownership and best value, and when selection and evaluation of IT assets is done using neutral criteria consistent with federal competitive procurement norms.

Agencies are generally required to select IT solutions that maximize best value for the Government.[13] One of GAO's recent reports supports the OMB recommendation that agencies need to evaluate the "life-cycle costs" of IT investments.[14] What this means, as the Committee is aware, is that a short-term emphasis on initial acquisition cost that ignores the total cost of ownership will increase the Government's overall IT costs. IT acquisition reforms need to recognize that the "best value" solution will vary on a case-by-case basis, and should require agencies to be clear in defining more precisely what will constitute the best value IT solution for a particular IT mission. And when a CIO's office defines best value precisely, the Government should ensure that procurement officials within agencies adhere to those definitions when actually making purchase decisions.

In those instances where all things really are otherwise equal among COTS IT products and services, then cost (over the expected lifetime of the technology) will be the driving factor. But in many other instances, the needs of the mission will require an examination—and likely a careful balancing—among a number of potentially competing interests, including cost, availability, redundancy, security, accessibility, privacy and other factors.

Different technologies as well as different licensing models need to be considered and evaluated against neutral criteria to decide which model will provide the best value for the federal customer in a specific situation. The then-U.S. CIO, OFPP Administrator, and IP Enforcement Coordinator noted that "as program, IT, acquisition, and other officials work together to develop requirements and plan acquisitions, they should follow technology neutral principles and practices," which means "selecting suitable IT on a case-by-case basis to meet the particular operational needs of the agency by considering factors such as performance, cost, security,

---

[13] FAR 15.302.

[14] GAO, *Information Technology: Agencies Need to Strengthen Oversight of Billions of Dollars in Operations and Maintenance Investments*, GAO-13-87 (Washington, D.C.: October 2012).

interoperability, ability to share or re-use, and availability of quality support."[15] As part of a transparent, fair and cost-effective technology selection and evaluation process, in which the competition is full and open to all competitors, we recommend that neutral factors such as the following be used:

1. Total cost of ownership/operation over the anticipated lifecycle for the technology;
2. Security/resiliency of the technology against attack or unauthorized access, including applicable requirements such as IT security controls, authorization and monitoring (FISMA), patient privacy (HIPAA), confidentiality of criminal justice records (CJIS), and educational privacy (FERPA);
3. Privacy implications for both citizens and Government users who interact with the technology;
4. Accessibility of the system to those with disabilities;
5. Integrity of records maintenance, such that they can be archived and retrieved intact for future reference as authoritative proof of final agency actions;
6. Data portability to allow for interaction between data systems, citizen access to data, and migration between service offerings; and
7. Openness of the technology in terms of utilizing globally recognized, interoperability standards.

Different factors will be more important to different federal customers, depending on the unique needs of the mission that must be satisfied. The Government should ensure that procuring agencies define clearly and transparently what factors will weigh most heavily in a determination of "best value" in a particular procurement. For example, the Acquisition Advisory Panel has noted "GAO and IGs concerns about ill-defined requirements in orders under interagency contracts" and recommended more up-front planning requirements before actual procurement occurs.[16] Increased transparency in the Government's requirements allows more competitors to enter the market, which provides the greatest range of cost-effective solutions for the Government. The Government similarly benefits from accepting commercial licensing terms where available.

Conversely, the Government should expect industry to be equally transparent in the acquisition process about how the devices and services being offered to the Government will satisfy the Government's more explicit best-value requirements. As Microsoft's General Counsel, Brad Smith, observed in a keynote address to a Washington, D.C. forum on Cloud Computing for Business and Society, "it shouldn't be enough for service providers simply to say that their services are private and secure. There needs to be some transparency about why that's the

---

[15] Vivek Kundra, U.S. Chief Information Officer, Daniel I. Gordon, Administrator for Federal Procurement Policy, Victoria A. Espinel, U.S. Intellectual Property Enforcement Coordinator, *Technology Neutrality* (January 7, 2011), http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/memotociostechnologyneutrality.pdf.

[16] Acquisition Advisory Panel, *Report of the Acquisition Advisory Panel to the Office of Federal Procurement Policy and the United States Congress* (January 2007).

case."[17] For example, the Government may feel it important to ensure that the sanctity of the data it entrusts to third parties will be preserved and to know what, if any, uses will be made of the data by the contractor host company. We, and our competitors, need to do better in this area so that our Government customers can be better buyers and guardians of data.

IV. Conclusion

Microsoft recognizes the importance of providing IT solutions that increase efficiency while still providing effective IT solutions to meet the needs of our federal customers. We look forward to continued collaboration with federal agencies to improve the management of existing IT assets, identify more cost-effective commercial technologies tailored to the needs of agencies, and provide IT solutions that will maximize best value and decrease the total cost of ownership for agencies. We also look forward to working with members of this Committee and other members of both the House and Senate as they consider ways to improve the Government's IT investment strategy. I thank you for your time and look forward to answering your questions.

[17] The Brookings Institution, *Cloud Computing for Business and Society* (January 20, 2010), available at http://www.brookings.edu/~/media/events/2010/1/20%20cloud%20computing/20100120_cloud_computing.pdf.

Chairman ISSA. I will recognize myself.

Mr. Niehaus, your statement, I got a little confused on, so let me see if we can straighten it out. I understand that government always starts off asking for COTS when they are told to and then distorts and mangles it to where no one would recognize it as commercial off-the-shelf. Is that what you are sort of saying?

Mr. NIEHAUS. Mr. Chairman, we fully embrace and support the term COTS, commercial off-the-shelf software.

Chairman ISSA. But I guess my questions is, are you saying there no such thing as COTS——

Mr. NIEHAUS. No.

Chairman ISSA. —because there shouldn't be or there is no such thing as COTS because the—particularly DOD as an example—is used to abusing the process of starting with COTS and then demanding changes that make it unique such that in your opening statement you even mention that DOD when using highly commercial software had to de-conflict within DOD with different security requirements?

MR. NIEHAUS. MR. CHAIRMAN, THE TERM COTS WE FULLY SUPPORT IN INDUSTRY. THE TERM COMMODITY IT WE DO NOT SEE AS AN INTERCHANGEABLE DEFINITION FOR COTS. WE BELIEVE THAT THAT TERM IS—WE DO NOT SEE THAT IN THE PRIVATE SECTOR TODAY——

Chairman ISSA. Okay. But let me follow up, because this is really the essence of what you said, and then I want to get to the other witnesses. Email is a commodity, isn't it?

Mr. NIEHAUS. I don't believe that, Mr. Chairman.

Chairman ISSA. Okay.

Mr. NIEHAUS. I believe email, for example, under the GSA BPA, there were seven different lots awarded for that based off of different requirements. And there were very few vendors that were able to satisfy all of those lots under that agreement. A true commodity would be able to support all of them equally.

Chairman ISSA. I think what makes me snicker just a little bit is, in the private sector, to the business world, and one time a few years ago I was over in the committee next door and I dispassionately implied that Lotus Notes didn't exist anymore and I was quickly told that the White House was still using it, basically, and spending a lot of money on it. And IBM made it very clear that they still had a thriving business in legacy software, because some lawyers hadn't given up on it and, therefore, we were spending millions to maintain it.

Let's go back again. At any given time, things like email, Microsoft being a market leader in it, Google, obviously, having a market share and a few others, in the private sector, to the gentleman sitting next to you, if I asked him if that was a commodity in his business, would he say yes or no?

Mr. NIEHAUS. The question is directed to me?

Chairman ISSA. I am asking you. I will get to Mr. Klayko.

Mr. NIEHAUS. I would say that by definition it is not a commodity.

Chairman ISSA. I am not trying to mistreat you, but I want to represent the time. Mr. Klayko, I am taking a big risk here. In the private sector, to CEOs at businesses, do you view it as a commodity that you buy what meets your needs, or that you feel you

have to design your own email system around your company's culture?

Mr. KLAYKO. We buy what is available.

Chairman ISSA. Now, I am going to chance that the VMware model is you don't make up your own email, is that right?

Mr. BOURGEOIS. That is correct. And you, Mr. Chairman, demonstrated an understanding of our core technology and how it fits into the scheme of consolidation. But on the matter I would say two quick things. One, call it what you want, but an x-86 server with a certain amount of memory and a certain amount of CPU is exactly the same as another one that has the same capability and capacity. And so whether you would call it commodity or not, there is a certain degree, and because technology is evolving rapidly more and more every day of capabilities that are essentially not important to the overall solution and could be automated and carried out in a very rapid fashion.

Chairman ISSA. And doesn't your company basically process that processing power and say, if I am going to have a bigger machine, I am going to have 12 different operating systems on it, or four, because I want to leverage the maximum efficiency of both the CPU and the DASD.

Mr. BOURGEOIS. And that is the second point I was going to go to. So the first point is that the technology exists to be able to pool the resources together and share them among many different applications, which, as the previous panel described, that there is a tendency of legacy in the industry to keep things vertical and siloed, which drives up the cost structure. And the second shift is away from an operating system-centric approach to applications and solutions to a more cloud or virtual data center-centric approach, and that in itself lends itself to an increasing uniformity of the solution, so that the overall underlying components don't matter as much.

Chairman ISSA. And, Mr. Niehaus, I just want you to understand, I am not disagreeing with you that government finds a way to make nothing COTS and nothing commercial, but when the GSA went out for emails, every email system that they found acceptable happened to be commercial off-the-shelf. So the commodities were in fact different flavors of branded product.

Mr. NIEHAUS. Correct. I want to be clear, Mr. Chairman, that I am not disputing commercial off-the-shelf software is valuable and ideal for government. The term commodity is not a phrase that I experience in the private sector. And so without more clear definition, and if commodity means commercial off-the-shelf software, then that certainly is a discussion we should have.

Chairman ISSA. I appreciate that, and if I could have an additional minute.

Mr. Klayko, I want to follow up with you and finally. I am very sensitive of the fact that before I came here I had the honor of serving as chairman of the Consumer Electronics Association and I was on the board of EIA. Should the government make a concerted effort to reach out to standards organizations and leverage them instead of saying, I want to D–Link 24-port switch or equivalent. Is that really where we need to get out of this lazy tendency to say this would work or equivalent and say, what is the standard

and can we leverage organizations in which maybe all these companies belong to have a common statement?

Mr. KLAYKO. I think it would go a long way with simplifying the procurement process, the deployment process, the manageability. If you deploy to open standards you can take advantage of the innovation as it comes along over time. I have heard lots of facts and figures today, and as a taxpayer, I have to be honest, my hands were sweating. Some of the statements were appalling. I will just go on record. And we know that these are issues. We ought to try to address them.

Open standards will not fix all of them, but it goes a long way, because you put a baseline and it actually encourages competition and innovation. Competition and innovation, as you know, encourages better price performance.

Chairman ISSA. Thank you.

And I now recognize the ranking member, and thank you for your indulgence.

Mr. CUMMINGS. Oh, no problem.

You all heard the testimony earlier with regard to personnel in government, people being sophisticated, that kind of thing, problems that you heard about earlier in the second panel. I am just wondering, did you have any comments on those, such as it seems to be a—you know, I sat here and I said to myself they sounds like it is too big to be successful. And I am just curious, do you have any comments? That is, our whole government IT situation. Any comments?

Mr. KLAYKO. I will take a swing at it.

Mr. CUMMINGS. Yes, take a swing.

Mr. KLAYKO. It is a pretty big question, pretty broad. I think you have to continue and invest in people at the end of the day. There are various aspects of technology deployment. I am a very big believer in people. I think there is a myth that all the private sector gets all the smart people. I think that is a myth. The fact of the matter, I think there is equally number of smart, intelligent, as well as highly trained people in the government.

I compete very rigorously for people in the technology world. In Silicon Valley is vicious. It got to a certain point where I couldn't find enough people, so what I ended up doing, I created my own university where I had to get people in and I had to train them because you can't continue to steal from each other so you have to go ahead and change that formula.

I think we can do that in the government also. I think the quality of the people are fine. The people that want to be here are here. The issue is you have to give them the tools and you have to retool them like any other. You don't drive a car 100,000 miles without changing the oil a few times and putting a few other maintenance items in. I think that is no different than the people.

Mr. BOURGEOIS. Thank you. Obviously, you heard in my opening statement that I believe that a continued investment in people, both on the acquisition side and on the IT side, is an absolute necessity. But make no mistake, as you point out, the problem is larger than the people. The culture needs to evolve as well, and that includes the culture in the programs that tend to have a lot of IT money that is made in many cases outside of the purview of the

CIO, and then the culture in the CIO organization themselves, in particular with how the organization is empowered to carry out the full IT mission and responsibilities of the agency.

So your point is well taken. But if the culture can evolve and the additional investment in the training of the workforce continues, and some other techniques which I consider under the culture of modularization, as we heard Mr. VanRoekel testify, and much smaller deliverables happening much faster but working in succession towards an overall goal, which, by the way, is a mission goal, not an IT goal, then I do believe that the problem can be—there can be success in spite of the challenge.

Mr. CUMMINGS. You can imagine when taxpayers hear the kind of figures we have heard here today and to hear the failures, they got to get upset. And then what happens is that they then say, you know, government can't do things right. And some kind of way we have to rightsize—I mean, we have to figure out ways to make sure. That is why I was asking the panel earlier about when you get people who are doing things the right way, how do you encourage that and how do you spread it around? Because people have to have faith in their government. And that is so important. And when you hear these kind of figures like Mr. Duncan was saying, it gets to be I am sure for some very discouraging. That is why I was wondering if this thing is so big that we can't control it?

Mr. NIEHAUS. Well, the prior witnesses really hit on a point that resonates with my experience across public sector and even in private sector that an empowered CIO that is given a clear swim lane, a set of responsibilities, authority and accountability can make great things happen.

The examples that were cited about the VA, for example, we recently renewed a very ambitious and creative agreement with them and have won the opportunity to take them to the cloud for their email. That was done by an empowered CIO. Also we commend when CIOs across agencies like the Army and the Air Force and DISA can come together and agree on shared requirements and have the authority to make those decisions, they can do great things.

Mr. CUMMINGS. Were you all surprised when Mr. Powner said that he asked for operations that were functioning properly, seven agencies, and I think he said three of them couldn't name any. I mean, did that surprise any of you all? Hello?

Mr. KLAYKO. I would say I don't know what the metrics are, and so I think part of that comes back, there is probably an expectation that comes back. I believe you can't manage anything if you don't have metrics associated with it, so I don't know what the metrics they were going. Because I can actually hear the same people say they are perfect. So it depends on what the metrics they are looking at.

Mr. CUMMINGS. So your university, I mean, I assume you invest quite a bit in that university. And what does "university" mean?

Mr. KLAYKO. We teach kids what they don't learn in college. They get book smart in college but they don't understand business and how to get things done. And we tell them, let me make sure you understand one thing when you come to work here, that you are entitled to nothing. You compete. So it is a life lesson, and that

is what this is about. So we put them through a short quarterly program and then we have a mentor actually take them through how do you operate and get things done. So there is a lot of other people that are doing it very effectively. Ours is one that we need to do it to instill change in our culture.

Mr. CUMMINGS. How many employees do you have?

Mr. KLAYKO. We have about 5,000 employees.

Mr. CUMMINGS. Thank you.

Chairman ISSA. Thank you.

With that, we recognize the gentleman from Virginia, Mr. Connolly.

Mr. CONNOLLY. Thank you, Mr. Chairman.

Chairman ISSA. I am sorry. If you wouldn't mind, the other gentleman.

Mr. CONNOLLY. Of course not. I would be honored.

Chairman ISSA. I apologize. You snuck up on me, John. We recognize the gentleman from Florida, Mr. Mica.

Mr. MICA. Thank you. And we will get to Mr. Connolly in just a second.

Mr. CONNOLLY. I am only too happy to have you go first, Mr. Mica.

Mr. MICA. Thank you. Thank you.

We heard the OMB CIO say that he didn't see any impediments as far as the law. Are any of you aware of any changes that we need to make in the law that would help us in this whole process? Anything?

Mr. BOURGEOIS. I don't know if I would specifically say there are changes in the law, and I am definitely not an expert on the laws themselves. What I would say is that in how those existing laws have been operationalized is just a mess. So if it can be simplified quite a bit.

Mr. MICA. The other thing is he cited himself that he would give an agency the authority to move ahead and they would take the paper and wave it around, but there is some problems in getting the authority transmitted to the agency, so there is some disconnect. He says he has the law and the authority to do that, but it is not happening. So that is some of what you are referring to?

Mr. BOURGEOIS. I am not sure I am familiar——

Mr. MICA. First of all, thank you all. I come from the private sector. I have been on this committee a long time and others, and for the private sector to come forward and testify like you are doing, I appreciate it very much. Sometimes they are very reticent for retribution or anything you say may be held against you and all of that. But this is important, and our purpose isn't to bash them, it is to try to see how we move this forward.

Mr. BOURGEOIS. Let me give my best example from my experience when I was an executive CIO at the U.S. Patent and Trademark Office. So in terms of empowerment, yes, and I mentioned specifically in my opening statement that I had the full authority that the Clinger-Cohen Act defines. And that was in some ways given to me by the Under Secretary at the agency, but also in terms of how we carried out our planning for IT investments, it was part of the budget process for the agency.

There were five executives that ran the agency: The Commissioner for Patents, the Commissioner for Trademarks, the CFO, the Deputy Under Secretary and myself, the CIO. And everything started with what the agency wanted to accomplish—reducing pendency, improving quality of patents, transparency and dissemination of information, and so on. Every dollar of IT investments was tied to one of those objectives. Whether it was a maintenance of an existing legacy application or it was a brand new thing like that new system that we implemented, you know, new 10 years ago, to take the Patent Office completely electronic, it was all tied to a mission objective and by virtue of that planning and how we executed it, we carried out the Clinger-Cohen responsibilities in concert with each other for the good of the mission. I don't see that happening in many other agencies today.

Mr. MICA. Well, I talked about having the law in place and then the policy to execute that and someone executing it, then the personnel. And I think you also mentioned the staffing level and we have talked a little bit about that. I was concerned that they may not be able to attract the best personnel or retain them. Sometimes you can get them and you teach them and the next thing you know they are out the door and they are earning big bucks somewhere else. I am not sure exactly how we legislate that, but I think we can look at the incentives and the packages and things that we can offer that might make a difference. Do you think that would be——

Mr. BOURGEOIS. Again, from my experience as a CIO in the Federal government, there are existing tools that can be used to address this challenge of expertise and attracting and retaining the right workforce. But also, make no mistake, it is a moving target. So as technology evolves now, those systems and capabilities that are in place today have to evolve with it. And there are things that I utilized as a CIO that are not very well known, like the SL designation to hire high-end technical experts on par with private sector expertise and then challenge them with metrics and reward them through performance capabilities when they delivered the results. This can happen today, but it does require the buy-in of the head of the agency.

Mr. MICA. There are lots of specifics, and I don't have much time, but I was fascinated by your just sort of quick analysis of the consolidation of the data centers. They are trying to consolidate 1,200 out of 3,000. What do you think the real number could be and what we could achieve there? Just one little example.

Mr. BOURGEOIS. The consolidation effort to date has been a critical first step, but there is really just the tip of the iceberg in what it has been able to accomplish. The reason is, as Mr. VanRoekel described, the legacy is applications that have infrastructure dedicated to them. The first step has somewhat consolidated them. For example, if you include back office applications, the GAO estimates more than 2,200 investments at $9.1 billion in back office applications. There is no question that there is billions of dollars of potential through consolidation of those applications.

Mr. MICA. I love your phrase I will conclude with elimination of duplication of applications. Has a certain ring to it. Thank you. I yield back.

Chairman ISSA. I thank the gentleman.

And we now go to probably the most dedicated consolidator of these stations, the author of the legislation, Mr. Connolly.

Mr. CONNOLLY. Thank you, Mr. Chairman, and welcome to our panel.

You know, picking up on the concern Mr. Mica and others and the chairman have mentioned about personnel, Mr. Klayko, you have been a CEO, and I served 20 years in the private sector in Federal contracting in IT. Might it be a fair statement that the way we are treating Federal employees is going to make it more difficult moving forward to recruit and retain, especially highly skilled sets; freezing salaries for 3 years, raiding their benefits to help finance other unrelated things, public disparagement of their public service and their worth. Is that how you would manage your workforce?

Mr. KLAYKO. No. I mean, you have to go ahead and create a culture that you want people to come to work every day. And there is a lot of other ways to go ahead and do that. So I think you have to create a culture in the government that people want to come to work, make a difference, and then put performance metrics in place, they go ahead and they get rewarded for their performance.

Mr. CONNOLLY. Thank you.

And Mr. Bourgeois, I saw you shaking your head. I assume as a former Federal employee, a CIO, you concur with Mr. Klayko?

Mr. BOURGEOIS. I will be very brief. I absolutely concur with that. You want to create an environment that folks want to come to work every day, and the scenario that you described that is happening doesn't exactly do that.

Mr. CONNOLLY. I agree.

Mr. Niehaus, you talked about best value. Could you explain a little bit more, when you talk about best value, what are you referring to?

Mr. NIEHAUS. The main concept from our perspective is the total cost of ownership. This is an industry accepted. I mentioned Gartner, for example, as one of the main reference points. In industry for a lot of years there was a focus on just lowering acquisition price. I think I heard it earlier today where throwing more IT made things more productive, you know, more better. And there wasn't enough looking backwards on how are we managing the legacy systems that we are building and how are we monitoring their success.

So the concept now is really focused on looking at total cost of ownership and holding CIOs accountable for delivering on that total cost of ownership, measuring it, so it is not just acquisition, but it is how much does that system cost to maintain, and what is the roadmap for that system after it is 5 years old, 3 years old; can you move it to the cloud, is it open data systems, et cetera?

Mr. CONNOLLY. And that is my next question to you, you have anticipated it. Why is it that often maintaining a system costs more than the original acquisition?

Mr. NIEHAUS. Because the way that requirements were built may not have been in as much collaboration with the private sector around best standards, open standards, commercial off-the-shelf software. What can the industry that is building the software do and deliver on a long-term that all of industry accepts. And when

you have that, and there is inherently a roadmap that allows you to start planning towards the future. Mr. VanRoekel talked about the depreciation of assets and how that in the private sector is something that you plan toward so that you can use your P&L to actually unlock investments for modernization instead of using it as a defense of existing spending.

Mr. CONNOLLY. And the chairman has talked about some very antique systems, legacy systems.

Mr. NIEHAUS. Absolutely.

Mr. CONNOLLY. The chairman and I are working together along with the ranking member, Mr. Cummings, on some legislation, and one of the things we are working toward is empowering CIOs. Would you and your colleagues at Microsoft welcome that as obviously a vendor and provider to the government, I mean? And presuming that we consolidate 243, which is way too many, but what is left, what kind of empowerment ought they to have from your point of view?

Mr. NIEHAUS. From our perspective the most successful projects are the ones that are closest to the mission and mission focus, and that means also the CIO that is empowered closest to the mission. As Congressman Davis stated, I don't know if we know that a certain number is too many or too little per agency. It is about the right swim lanes and the accountability so that you can measure the success of that CIO.

The missions that the DOD performs are myriad. The U.S. Department of Agriculture has food inspectors and various others. It is not necessarily right to think that one CIO would be able to have expertise in designing mission systems for each one of those. So the goal would be to know that you are working with an accountable and empowered CIO focused and close to that mission to make them successful.

Mr. CONNOLLY. Final word, Mr. Bourgeois, I want to give you an opportunity to expand. When you were at Patent and Trade, you gave us an example that worked and you said then that is how we got to Clinger-Cohen, but then you said, but I don't know many other examples of that in the Federal family. Could you elaborate on that. Why not? What were the unique attributes of Patent and Trade that apparently weren't transferable to other agencies?

Mr. BOURGEOIS. I am glad you couched the question that way because it does give me the opportunity to point out that in one way it was, you know, full authority over the IT budget, and that was all IT expenditures across the agency, and that included the business applications used by all of the examiners and all the other staff. Most CIOs in the Federal government are called CIOs, but they are really chiefs of infrastructure, because the business applications are funded and implemented, managed by some program somewhere else. So that is a key capability.

Also the full authority and responsibility of hiring and firing and incentivizing and managing all of the IT people and IT classifications throughout the entire agency. So there were these other control factors in place through HR, through contracting and other means throughout the office, that if things were happening in the rogue IT organization in the business units, they would come back

to me as the CIO and I could go talk to my peer, we could correct it and get it back on track.

Mr. CONNOLLY. I thank the chair.

Chairman ISSA. Thank you. I would like to do just one short additional round.

Mr. Klayko, since you are the only person that currently is not working for a company, I am going to take advantage of your temporary lack of conflict potentially, although pride is the greatest conflict sometimes in an answer. But in your years of selling products and services, didn't you try to decommoditize what you sold while the buyer tried to commoditize. Today you have in a sense told us in your opening statement that in fact the worst thing to do is to buy into the decommoditization. In other words, when I ask for a Cisco router or equivalent or a D–Link router or whichever brand, I am buying into somebody's decommoditization by definition. Isn't that pretty much what you said?

Mr. KLAYKO. As a vendor?

Chairman ISSA. As a vendor you want to decommoditize. You want to have your brand matter and have it spec'd by name if possible. As a buyer I want everything to be pounds of wheat. I want everything to be as commoditized as possible. Isn't that essentially the relationship that is optimally the first thing that each of you is working toward?

Mr. KLAYKO. I mean, if you start at the opposite ends and work towards the middle, I think that is probably true. I looked at in many of the reviews I have done in the past why someone was chosen over another. You do loss reviews all the time. You have done it in private sector and so forth.

One of the things I find is in an IT environment, in any environment, the most feared word is delete. So nobody deletes anything. No one deletes data. They keep it forever. So you just get more and more and more and more and more and it becomes unmanageable and more difficult.

Chairman ISSA. That is why we need VM's Image Backup, is because it has gotten to be so much data we are backing up we don't have time to back it up as data.

Mr. KLAYKO. Yeah, but there is still that. And then the other thing what I found is there is a lot of fear. There is fear of making a change. Because right now, to your point, sir, where you said, you know, we are laying off people, there are no raises and so forth, so why do I want to put myself on the edge to make a recommendation to make a change if all of a sudden it doesn't work and it fails so I become the guy they shoot. So there is no incentive. We have the exact opposite incentive program that should be in place.

So we are starting at different points, but the membrane to get together, I am not sure we can if we can never align on that. It is very, very difficult. We have to eliminate the fear.

Chairman ISSA. Okay. I am going to do two last questions. Mr. Niehaus, I give you a little grief on this subject deliberately. Microsoft and a number of other well-known brand names in software deliver more than a commodity because they deliver the history, the predictability. Look, 1.0, everything fails, and 2.0 exists for the purpose of fixing everything that was wrong with 1.0 and 1.1 and 1.2. We get it, that you can't deal with people on a purely com-

modity basis. But from a government procurement standpoint, shouldn't our procurement reform be similar to Mr. Klayko's statement, which is quit spec'ing by definition what we need almost by brand name and spec it to the greatest extent by the minimum needs required, and then companies can come in and sell their ups and adds or additional features which often make the difference between two otherwise identical commodities.

Mr. NIEHAUS. Mr. Chairman, the way that we would look at it or the way that we see it is commercial off-the-shelf software is a great term and a great phrase and it means a lot and it is very accepted. The challenge is that where we are going today, or now and in the future, is cloud-based email systems, and we have agencies lining up to do that. That is not as simple as just taking the version of exchange server that is running that you already own and just putting it in the cloud and running it. It is actually new innovations. It is new capabilities. It is the ability to provide that warfighter a disconnected scenario downrange or a task worker in the field or a food inspector disconnected as well as an IRS worker fully connected.

Chairman ISSA. Sure. Those are certainly ups and adds. And, oh, by the way, when you went from an exchange based to clouds, I lost a few things, too. I made that transition. The fact is that you sometimes find things are slightly different because you have been using, if you will, undocumented features, and that is common that we find ways to make things work that were not in the plan, mailboxes that are blank for some reason that people look at in a different environment. And I appreciate that, and hopefully that is what we are going to continue looking at how to get right in this act.

Mr. Bourgeois, obviously I know a little bit about your product, probably enough to be dangerous. But earlier I think there was something that didn't get said properly, which is, isn't it true that one consistency within our movement, the government's movement to cloud, is underutilization. We can do what Mr. Connolly so much wants us to do, which is consolidate. But if we consolidate rather than to 100 servers doing 1,000 tasks and instead what we have is 1,000 servers each doing one task, we haven't really saved anything other than we have made the electric bill appear in one place. Isn't that to a great extent the other part of consolidation that we have to find a way to do?

Mr. BOURGEOIS. Mr. Chairman, that is very well said. I think that the consolidation effort includes multi-layers of the technology stack, and the majority of the efforts thus far have been focused on the core infrastructure layer when there is still—maybe the low hanging fruit has been picked and we have to reach up a little farther. There is still fruit to be picked there. But without a doubt there is an opportunity to actually rationalize the portfolio of IT investments, to take the 10 things that are doing the same thing and actually meld them into one and consolidate it at the same time.

Chairman ISSA. Thank you.

Any additional rounds? Mr. Cummings?

Mr. CUMMINGS. I yield to Mr. Connolly.

Mr. CONNOLLY. Thank you. Thank you, Mr. Cummings.

I actually just wanted to piggyback on your point, Mr. Issa, Mr. Chairman. I think we have to find sort of a happy medium. Take the chairman's point about emails. All right, maybe emails shouldn't be treated as a commodity, but you heard Mr. VanRoekel when he testified in my district in a field forum, he pointed out in an agency, he says 20, but I am pretty sure he said 36, but it was a lot of email systems. And you know how that happened. It didn't happen because there are 20 or 36 unique sets of demands on an email system. It grew up because my division got an email system and yours got one later. And so as a result we have all this stovepipe duplication, they can't talk to each other, and we are spending a fortune trying to fix it. Mr. VanRoekel pointed out he finally got one in place. Now, maybe that is too few.

So I just think that to the chairman's point, while we don't want to have a mentality that says no, no, one size has to fit all, god, is that a problem in government. On the other hand, we can't treat everything as unique or we will never save a dime and we will never get efficient.

Mr. NIEHAUS. Congressman, I completely agree with that. And a perfect example, and I don't know if Mr. VanRoekel is referring to this customer, but the USDA, for example, had that numerous 20-plus email systems. It was Microsoft that consolidated those into the cloud. So it is not that we are against this, by any means. The focus that we look at is making sure that we are continuing to meet the mission of government as it evolves. If the decision had been pick one of these, label it a commodity and everyone standardized on it, there wouldn't have even been a conversation about, well, what can the cloud offer? Can the cloud actually offer you a better value, a faster return on your IT investment, a lower total cost of ownership over time.

I think that is where we bring up the concern about the term commodity because we don't see it in the private sector but we do see commercial off-the-shelf software in the private sector, and we do completely agree on the focus of what are the standards of service and the standards of mission requirement that we can all agree are the core fundamental, and let's build around that and deliver solutions around that and fight to innovate among competitors.

Mr. CONNOLLY. And I do not spend a lot of time on this dais defending the chairman, but in this case I think there has been somewhat of a reaction to some of the draft language, and I don't think there is that much daylight frankly between how you just articulated it and how the chairman or I would articulate it.

Mr. NIEHAUS. I think that is certainly a welcome conversation and discussion for us to continue to support and have. Absolutely.

Mr. CONNOLLY. Thank you.

Chairman ISSA. As we close, I will tell a very short story. I remember all too well being in the military where we were driving military vehicles with military tires designed for combat, and somebody somewhere at DOD back in the seventies got the bright idea that they ought to buy a whole bunch of pickup trucks, standard, I believe they were mostly Dodge pickup trucks, and paint them green and use those to run back and forth on streets, on regular roads, to go pick up parts. It was an innovative idea. It saved countless millions of dollars and, quite frankly, some lives because

military combat vehicles on slippery roads, on hard surfaces, do not perform nearly as well.

Our goal with IT purchasing reform is in fact to recognize that Americans all buy automobiles which are commercial off-the-shelf. We are not claiming that a Cadillac—or I will use the now defunct Yugo—are in fact equal. But we do know that all of them are part of a commodity for transportation. We want to find a way to make sure that specific pieces of transportation are purchased that optimize the Federal need and that in every case possible we not ask somebody to set up a brand new auto company to produce a form of transportation.

And with that, I thank all of you for kicking off this process, being our first hearing, and we stand adjourned.

[Whereupon, at 4:40 p.m., the committee was adjourned.]

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143

Majority (202) 225-5074
Minority (202) 225-5051

Opening Statement
Rep. Elijah E. Cummings, Ranking Member

Hearing on "Wasting Information Technology Dollars: How Can the Federal Government Reform its IT Investment Strategy?"

January 22, 2013

Thank you, Mr. Chairman. I want to welcome all our witnesses here today, including our good friend and distinguished former Chairman, Tom Davis. It's great to see you.

I think this is an appropriate first hearing for this Congress. This is a good government hearing that gets right to core of our Committee's jurisdiction. Today we are examining federal spending on information technology. Our Committee has jurisdiction over the efficiency and management of government operations and activities, including procurement. It is our responsibility to ensure that the federal government is spending money wisely and efficiently. This includes federal spending on information technology.

The President's Fiscal Year 2013 budget projected that agencies will spend $79 billion on IT this year. The Government Accountability Office has found that agencies do not have adequate oversight of these investments. In a report last October, GAO found that five major agencies have not been using the proper safeguards to ensure that their investments in the operation and maintenance of IT systems are performing as intended. As GAO said, "Until agencies address these shortcomings, there is increased risk that these agencies will not know whether the multibillion dollar investments fully meet their intended objectives."

I look forward to hearing from Mr. VanRoekel, the Chief Information Officer, about the progress the Administration has made in improving the quality of IT investments, what is being done to improve oversight of those investments, and how overall spending is being reduced. In particular, I am interested in hearing about the Administration's efforts to improve the transparency of IT investments. I also look forward to hearing from industry leaders who can identify the challenges and opportunities we face in our efforts to improve the way the government invests in IT.

Finally, I want to applaud the work of our resident technology expert, Representative Connolly, the Ranking Member of the Government Operations Subcommittee. Mr. Connolly held a forum in his district last May that explored many of the same issues we will hear about today. He also has taken the lead in introducing legislation to reduce waste by consolidating federal data centers. The Administration's efforts on data center consolidation are expected to save the government $3 billion by 2015.

I believe it is time to modernize the way the government does business. This will require strategic investments in technology, but we should not overlook the importance of strategic investments in our workforce. Our acquisition community needs to have the tools necessary to effectively oversee increasingly complex systems from beginning to end. These professionals ensure that the government is a smart consumer.

Thank you, Mr. Chairman.

Contact: Ashley Etienne, Communications Director, (202) 226-5181.

"Wasting Information Technology Dollars: How Can the Federal Government Reform its IT Investment Strategy?"

Tuesday, January 22, 2013 at 1:00 p.m. in 2154 RHOB

Opening Statement of Rep. John Mica, Chairman, Subcommittee on Government Operations

- I want to thank Chairman Issa for holding this hearing. With a national debt level exceeding $16 trillion, we need to do everything we can to reduce unnecessary government spending.
- In its 2012 report on opportunities to reduce duplication in the Federal Government, the General Accountability Office highlighted the need to address potentially duplicative IT investments to avoid investing in unnecessary systems.
- GAO found that in fiscal year 2011, the federal government funded 622 separate Human Resources systems, 580 Financial Management systems, and 777 Supply Chain Management systems.
- So what we have is the various federal agencies – as well as offices within the agencies -- making separate investments in back office systems that perform the same function. And all this duplication comes at a significant cost. What we should be doing is aggregating demand among the agencies and offices to get the best price for various commodity IT products and services.
- We also waste money investing in systems that fail to become fully functional.
- GAO's written testimony today, for instance, cites several examples of wasteful IT spending by agencies within this own committee's jurisdiction. The National Archives and Records Administration poured $375 million into the development of an Electronic Records Archive system that has now been put to a halt. The Office of Personnel Management canceled its Retirement Systems Modernization program after a $231 million investment.

- Despite these failed investments, OMB recently abandoned the practice of including in the President's budget submission a summary of the extent of risk represented by major federal IT investments. According to a report issued by GAO last fall, the President's budget submission from 2007 to 2009 included an overview of the investment performance over several budget years of IT projects in need of management attention. But this practice was abandoned by the White House in its last four budget submissions.

- The unfortunate reality is that sixteen years following the signing of the seminal Clinger Cohen legislation that laid the foundation for the federal government's acquisition and management of IT -- and ten years after the E-Government Act was passed that established Federal Chief Information Officers -- program failure rates and cost overruns still plague between 72 and 80% of large government IT programs, according to industry sources.

- The first step in addressing any problem is determining who is responsible and holding them accountable. The Office of Management and Budget needs to take responsibility for the lack of coordination and intelligent investment in IT being done at the agency level. OMB has to be willing to step up and say that "The Buck Stops Here."

- So I am disappointed that the head of OMB's Office of Federal Procurement Policy –the federal government's acquisition chief – is not with us today, although he was invited to testify. But I am glad that we do have with us today from OMB the federal Chief Information Officer. I look forward to his testimony and that of the other witnesses.

Statement of Congressman Gerald E. Connolly (VA-11)
Committee on Oversight and Government Reform
Wasting Information Technology Dollars:
How Can the Federal Government Reform its IT Investment Strategy?
January 22, 2013

Chairman Issa and Ranking Member Cummings, thank you for holding today's important hearing to examine how we can enhance the Federal Government's procurement and deployment of information technology (IT) to best serve the American people. I believe the single most important step we can take to enhance the efficiency and effectiveness of government is closing the IT gap between the public and private sectors.

Today, Federal IT acquisition is simply too cumbersome, bureaucratic, and wasteful. To fix this critical weakness, I believe this Committee must focus on three critical factors, people, process, and culture.

With respect to people, or human capital, the bottom line is that if Congress refuses to strengthen the Federal acquisition workforce; then we might as well not even proceed with any other reforms. The Federal Government's performance is inextricably linked to the quality of our dedicated civil servants, yet Congress has refused to invest in our Nation's acquisition workforce, allowing it to deteriorate in terms of size and quality. By doubling contract spending over the past decade, while ignoring the need to empower agency's to recruit and retain talented acquisition personnel, Congress created the untenable situation we find ourselves in today – where we routinely spends billions of dollars on failed or antiquated IT projects.

As the U.S. Government Accountability Office (GAO) notes in its testimony, Federal agencies are set to invest more than $74 billion on IT investments in fiscal year 2013, with 73 percent, or $54 billion, of that investment solely devoted to operating and maintaining (O&M) antiquated and inadequate systems. According to GAO, Federal IT spending has risen to at least $81 billion for fiscal year 2012, yet agencies continue to incur frequent cost overruns and schedule slippages resulting in outdated systems that contribute little or nothing to accomplishing agency missions.

This is not a new phenomenon. I can still vividly recall a project I managed while at SRI, where I dealt with a succession of 14 – yes, 14 – separate contract officers on a single project! It was unbelievably frustrating to begin building momentum on a project only to encounter yet another new contracting officer who brought their own conception of the goals of the project, the contract itself, and little institutional knowledge.

Now it is important to bust one myth surrounding the public-private IT procurement gap that somehow the government simply cannot execute IT projects as well as the private sector. The reality is that a substantial amount of ill-advised, poorly performing IT projects are initiated in both the public and private sectors. The primary difference is that in the private sector, a significant number of these bad IT projects are terminated soon after they begin. In fact, a key characteristic of high-performing companies is that they kill approximately one-third of all new IT projects within the first six months.

(OVER)

Fortunately, there are signs that the Federal Government is catching up. The Department of Housing and Urban Development recognized early on that it lacked the skills and resources necessary to successfully implement HUD's Transformation Initiative investment, and subsequently eliminated 22 planned projects, which enabled HUD to more effectively manage 7 high priority ones.

In the 113th Congress, I am committed to continuing my bipartisan efforts to develop comprehensive Federal IT acquisition reform legislation that provides agencies with necessary authorities to effectively recruit and retain IT procurement personnel and program managers with particular attention paid to strengthening America's cybersecurity workforce. Further, presuming that agencies will continue to operate under constrained budgets for the foreseeable future, I believe it is also vital that we promote IT program management mobility to enable the right talent to be sent to the right agency at the right time – mitigating existing IT program management competency gaps.

In regard to process, the Federal Government must streamline how it buys critical technology assets. I have been working with Chairman Issa to develop a bipartisan, comprehensive reform bill that would represent the most dramatic overhaul of Federal IT procurement law since Clinger-Cohen was enacted sixteen years ago. At the moment, we are still in the development stages; however I am optimistic that we will be able to find common ground among all stakeholders. Further, I am confident that by authorizing Federal acquisition shops to adopt a more streamlined, agile, and modular IT contracting approach, we can save taxpayers billions of dollars by eliminating project disasters.

Finally, Congress must work with the Executive Branch to change the culture of agencies. The Federal Government must break free of its illogical preference for custom, cumbersome, and proprietary systems when more effective "light technologies" or shared services exist. Unfortunately, too many agencies still view IT assets as an opportunity to demonstrate their importance by demanding cumbersome systems that are built from scratch, and segregated from other antiquated systems. Leading private sector companies have achieved significant operational efficiencies through aggressive adoption of cloud technologies and Infrastructure-as-a-Service, while the Federal Government has gone in the opposite direction. For instance, consider data center management:

IBM reduced its data centers from 235 to 12. HP consolidated 14 data centers into 1, reducing energy consumption by 40 percent; Meanwhile, the Federal Government has gone from operating 432 data center in 1998, to 2,094 data centers in 2010. I have introduced legislation, the "Data Center Optimization Act," which would enhance the efficiency of data centers, resulting in more efficient data usage, and improved energy performance, and I am pleased that Chairman Issa expressed interest in incorporating my bill into our bipartisan IT reform act.

Of course, it is not sufficient to just improve the way we purchase IT assets. We must also encourage and reward innovative agencies that successfully take risks to deploy and use information technology in the most effective and efficient manner possible. It is very likely that agencies will continue to operate under shrinking budgets and declining resources for the foreseeable future. This budgetary reality – when combined with our aging boomer population – means that agencies will face unprecedented pressure to meet increasing service demands from the public while operating with less people.

I often have to remind my colleagues that in 1953 there was 1 Federal worker for every 78 U.S. residents, while today, this ratio has grown to about 1 Federal worker for every 145 U.S. residents. If the Federal Government is to avoid draconian cuts to critical services, the single most important tool we have is technology.

While it would be better not to find ourselves in this position, it is worth noting that because the public-private IT gap is so large; the potential upside is substantial. The Federal Government's historical shortcomings in IT may ironically give us a late-mover advantage, in which we can leapfrog costly, less efficient technologies and go directly to the less expensive, more powerful ones that act as an incredible force multiplier.

For instance, U.S. Customs and Border Protection recently launched the *Enforcement Link to Mobile Operations* project, known as ELMO cargo, which facilitates faster movement of perishable imports. As you all know, CBP inspections normally take place at ports of entry, with the subsequent release of cargo delayed until field personnel return to the office and enter inspection results into CBP data systems, a delay that can be very costly to fresh fruit and vegetable importers. With ELMO cargo, CBP Officers and Agriculture Specialists use handheld devices to immediately clear containers, speeding up release time by up to four hours, while maintaining a secure port.

The Federal Government has a long and cherished history serving as a leader in the creation and adoption of cutting edge technology – from constructing innovative transportation infrastructure such as the national railroad system in 19th Century or the Eisenhower Interstate System in the 20th, to the Defense Advanced Research Projects Agency's leadership in creating the internet that connects the globe today.

President Obama was absolutely correct in noting during his second inaugural address that "We must harness new ideas and technology to remake our government," and I share his belief that America "cannot cede to other nations the technology that will power new jobs and new industries – we must claim its promise." I want to thank the Chairman and Ranking Member again for holding today's hearing, and I look forward to hearing from the witnesses about how we can streamline and reinvent Federal IT acquisition to meet the challenges of the 21st Century.

-END-

For the record

Matthew A. Cartwright

PA-17

Opening Statement

Congressman Matt Cartwright

Full Committee Hearing on: "Wasting Information Technology Dollars: How Can the Federal Government Reform its IT Investment Strategy?"

January 22, 2013

Thank you, Chairman Issa and Ranking Member Cummings. It is my honor to be serving on the House Oversight and Government Reform Committee. I look forward to working with members of this Committee on both sides of the aisle to ensure that our government is functioning as efficiently and transparently as possible. It is my hope that our collective efforts can increase the government's accountability to our taxpayers and begin to renew the faith the American public places in its elected officials.

The choice of this topic for the first hearing of this 113th Congress is well chosen. This committee should work together to form a consensus around increasing efficiency in necessary government expenditures. The opportunities to cut waste are readily apparent in the field of Information Technology and this is clearly an area where

bipartisan progress can be made. As more and more of our information becomes available through digital media, establishing a strong spirit of technological innovation within the government can lead to massive savings in the future.

Unfortunately, it appears that many government agencies have been unsuccessful in this endeavor, as evidenced by the increasing share of IT spending devoted to operations and maintenance of pre-existing systems. This correlates with a decrease in spending on new and innovative advancements in the field of Information Technology. By continuing to misappropriate funding, we enter into a repetitive cycle of sub-standard IT services while attempting to catch up to the previous years innovations- innovations we were too busy maintaining old services to look into.

Despite the federal government's previous shortcomings, we have begun making progress in this important area, progress highlighted by the OMB's IT Dashboard. This type of oversight is key for ensuring that spending is being done in responsible ways, and the public's ability to access the Dashboard online is exactly the type of accountability and transparency we seek. The Government Accountability Office has

already credited the IT Dashboard with providing benefits for several agencies.

In addition, I commend the work of Congressman Connolly and his work on the Data Center Optimization Act which would be a huge leap forward in addressing this issue. I am also encouraged by the similarities to Chairman Issa's Federal Acquisition Reform Act and believe this serves as a great opportunity to work together. I am looking forward to doing my part to help enact these bills.

I look forward to working with my new colleagues on this committee to address this and several other important issues over the course of this congress.

Thank you Mr. Chairman.

Questions for the Honorable Steven VanRoekel
U.S. Chief Information Officer
Office of Management and Budget

Rep. Tammy Duckworth
Committee on Oversight and Government Reform
Hearing on "Wasting Information Technology Dollars: How Can the Federal Government Reform its IT Investment Strategy?"

---

1. **How does the centralized Federal IT acquisition process support military operations at the State level?**

   The Department of Defense is a key partner on the newly established Strategic Sourcing Leadership Council (SLSC) which, with OMB's leadership and support, is helping our largest purchasing agencies to coordinate efforts to better leverage the government's buying power, including for information technology. The Office of the Secretary of Defense manages a program management office within the Department to figure out the best ways to support the SSLC and maximize value on IT and other major purchases of common use good and services, including those that may be used to support the National Guard.

2. **Are there any safeguards that would ensure the State IT requirements, missions, such as under State active duty or Title 32 missions, can be given the same priority as the Federal forces under Title 10?**

   The Department of Defense formulates a top line budget that focuses on their overall mission and strategy for all DOD functions. We recommend that Department of Defense be consulted on their approach to this specific question.

Questions for the Honorable Steven VanRoekel
U.S. Chief Information Officer
Office of Management and Budget
Rep. Jackie Speier
Committee on Oversight and Government Reform
Hearing on "Wasting Information Technology Dollars: How Can the Federal Government Reform its IT Investment Strategy?"

---

1. **At the end of last year I sent a letter to this committee calling for an investigation of how a program like ECSS could get so far, cost taxpayers a billion dollars, and have so little to show for it. FOIA documents indicate OMB held at least three TechStat meetings with DoD officials about this program, but DoD never identified it as a high risk area in the IT Dashboard, and we really didn't know how badly the program was failing until it was cancelled. It seems like many processes failed here, but what does the ECSS program tell us about how OMB and agencies use the IT Dashboard and TechStat meetings? What steps is OMB taking to prevent this from happening again, as DoD struggles with what GAO assesses-and I agree-is a very risky acquisition portfolio of business enterprise systems?**

OMB shared GAO's concerns with ECSS OMB identified several critical program risks and worked directly with DoD leadership to hold multiple TechStat sessions (more than any other major DoD IT system), which focused on issues including:

- Growing cost estimates;
- Multiple program delays;
- Growing requirements and the shifting of complex requirements to later phases; and
- Appropriate allocation of resources and time for planned deliverables.

Large and complex ERP implementations are prone to delays and failure, and ECSS is a huge and complex system by any standard, on its own surpassing the entire IT budgets of many agencies. While undoubtedly errors in execution have been made, the failure of ECSS is at least in part attributed to other broader issues, including decentralized accountability, overly ambitious ERP implementations, and an acquisition system that was designed for other purposes. The result is IT systems that are obsolete by the time they are delivered, if they are delivered at all.

We believe OMB's intervention accelerated the termination of this program. And, while risk of delay and failure is inherent to ERP implementations, and agencies are ultimately responsible for taking concrete steps to removing structural barriers to success and continuing to hold TechStat sessions on troubled investments, we believe that OMB's leadership is reducing the risks of similar failures. For example, OMB has worked with agencies to ensure that there are clear lines of accountability and proactive governance boards, who make sure investment plans are realistic and that they remain on track. OMB also advises agencies to take lessons from the private sector and develop major systems using a modular approach, reducing risk and speeding time to delivery.

2. **I'm troubled by Mr. Powner's testimony questioning the accuracy and the reliability of the information in the IT Dashboard, and particularly his testimony about the Department of Defense's categorizing very troubled programs like the ECSS as low or moderate risk. Shouldn't it raise a red flag when agencies seem to be grading their programs on a curve? How do you explain this disconnect between the DoD's assessment of its programs and the GAO's concerns about significant risks? What efforts is your office taking to improve the accuracy of DoD's reporting to the IT Dashboard?**

   Chief Information Officer (CIO) evaluations are by conclusions formed by each agency's CIO independent of OMB's evaluation of specific investments. In conducting its own evaluation, OMB takes the CIO's assessment into account as only one of many factors it considers in assessing the health of an IT investment, including: data quality reports, rebaselining, and cost and schedule variance.

   OMB is aware that the process for forming CIO evaluations may vary between the agencies reporting to the IT Dashboard, and this is taken into consideration when analyzing trends and mixes of evaluations at a given agency. For example, in the specific case of ECSS, although the DOD CIO evaluation of this investment was a "3" (consistent with "moderate risk") at the time of its first TechStat, OMB observed that this was the lowest rated investment in the entire DOD portfolio, it was one factor of many leading to OMB's decision to hold the initial TechStat of ECSS.

   It is important to note that GAO has reported that the CIO evaluations as required by OMB have "increased quality of [agency] performance data, greater transparency and visibility of investments, and increased focus on project management practices" (GAO-13-98). GAO has also released at least three reports concluding that the IT Dashboard has increased transparency and oversight, and improved the accuracy of agency data. (GAO-11-831T, GAO-12-210, GAO-11-262)

3. **I believe that the lessons learned from PortfolioStats should be coming out next month, correct? Could you perhaps give us a preview of OMB 's findings?**

   The success of the PortfolioStat initiative was due in large part to the fact that there was not a one-size fits all solution. We asked agencies to use data and analysis to make decisions that would improve their organizations rather than applying a standard solution across the board.

   Additionally, the structure of the PortfolioStat session was extremely beneficial. Bringing together the Deputy Secretary and business executives of the agency allowed for clearer decision making and stronger deliverables.

   In year two of PortfolioStat, we are working to drive performance and management improvements so that agencies can continue to improve the maturity of their portfolio management and realize the savings, service improvements, and efficiencies from this maturation.

   Per the requirements of the PortfolioStat memorandum, M-12-10, OMB "will gather its own successes, challenges, and lessons learned through the process and update [the] memo and data

collection parameters accordingly each year."[1] We expect to complete and release that document during the first quarter of this calendar year.

4. **It appears OMB held approximately 59 TechStat meetings in 2010, 5 in 2011, and at least 6 in 2012. It was my understanding that TechStat was created, in part, because agency CIOs didn't have enough authority, and yet 2 years later OMB seems to be returning back to relying upon agency CIOs to assess risk and provide OMB management insights. I worry that OMB seems to be less engaged in accountability for these programs. Did TechStat fail, why did OMB move away from this initiative?**

   OMB considers TechStat to be a vital tool in assessing and improving the performance of agency IT investments, and we have continued our commitment to the TechStat process. OMB conducted 59 TechStat sessions in 2010, as well as trained over 1,000 agency personnel on the processes in every CFO-act agency in-person. After this in-depth training, agencies were better able to hold their own TechStat sessions. This has brought about the growth of TechStats throughout government and has enabled many more in subsequent years than would have been possible with an OMB-only approach. To-date, there have been over 500 TechStat sessions at agencies and OMB combined. OMB expects agencies to continue to leverage the model by conducting their own TechStats at both the Department and Bureau levels, and, as needed, OMB will continue to hold TechStat sessions as well.

5. **It seems like the agencies are still holding most of the cards when it comes to management of these programs, that they have access to more of the information, and that OMB has to largely rely on less timely reporting from the GAO and others to find out if there's really a problem going on with this program. Does OMB have the resources they need to challenge agencies' risk assessments?**

   While the IT Dashboard is a valuable and improved resource for information on the performance of Federal IT investments, we continue to rely on a wealth of other available information when it comes to assessing investment performance. OMB analysts continually engage directly with agencies, often with program managers, and have access to a wide variety of relevant and timely information when they need it. Agencies are accountable for the ensuring IT resources are used efficiently and effectively to deliver results to the American people.

6. **As FDCCI and PortfolioStat start to merge, what are the metrics for evaluating their success? Do savings come into play as a key measurable outcome?**

   Looking at the FDCCI and PortfolioStat efforts together yielded insights: to have the most impact in optimizing data centers, agencies must first rationalize their portfolio and application inventory; conversely, when rationalizing their portfolios, they must fully factor the impact on their data centers, or factor in plans to shift to cloud computing. When discussing these parallel efforts with the Federal CIO community, this relationship was apparent and we agreed that combining these efforts would yield the greatest results long-term.

---

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

An optimized infrastructure is a more comprehensive way of analyzing the use of resources than simply looking at the number of data centers closed. Lessons learned from PortfolioStat revealed that successful agencies focus both on optimizing data centers that remain open as well as closing duplicative data centers. OMB is currently working with agencies to better categorize the federal data center inventory and refine metrics to continue consolidation of the remaining data centers, while implementing measures that optimize existing data centers.

At this point in time, possible metrics for consideration include agency progress on closures and the extent to which an agency's data centers are optimized from a total cost of ownership perspective. This includes energy, facility, labor, storage, virtualization and cost per operating system measures as well as savings achieved from optimizing and consolidation data centers.

As we finalize these metrics over the next several months, specific metrics may be added, subtracted, or modified.

7. **Mr. Powner's testimony indicates that it's pretty difficult to estimate the risks of these acquisitions if agencies like DoD, VA, and the Treasury do not create operational analysis policy. What measures is OMB taking to encourage DoD, the VA, and Treasury to make more progress in this area?**

Evidence of operational analysis for all major fully operational and mixed life cycle investments is required to be submitted as part of the annual budget submission by the most recent OMB Circular A-11 budget reporting guidance (section 300.3). OMB acknowledges that this is an area for needed improvement and will continue to work with agencies through channels such as PortfolioStat to bring additional attention to this important issue.

Questions for the Honorable Steven VanRockel
U.S. Chief Information Officer
Office of Management and Budget
Rep. Darrell Issa
Committee on Oversight and Government Reform
Hearing on "Wasting Information Technology Dollars: How Can the Federal Government Reform its IT Investment Strategy?"

---

8. **The General Services Administration telecommunications contract program, known as Networx, has been in place since 2007. This contract provides significantly better pricing and enhanced technical capabilities compared to the previous FTS2001 contract. However, it appears some agencies are still struggling with the transition to take advantage of cost savings of buying better telecommunications for less. And as we talk about the cloud, obviously, if you don't have a low-cost, high-speed internet connection, you are going to also resist the cloud. What is the current status of the Networx transition and your vision of where we go from here regarding the future of government's communications infrastructure?**

   Agency transitions from FTS2001 contracts to Networx contracts was completed last year. The future plan for communications infrastructure is through a joint OMB-GSA effort called the Network Services 2020 (NS2020) that started mid-2012 with a third-party review of industry trends and emerging technologies, and is now proceeding with discussions of how to translate that to next generation service offerings using strategic sourcing acquisition solutions.

9.

   a. **FedRAMP (the Federal Risk and Authorization Management Program) is a standardized approach to cloud security certification that will save the government money, time, and staff by eliminating redundant individual agency security assessments. GSA claims it will save an estimated $200,000 per authorization. FedRAMP is a critical part of OMB's 25-point plan and cloud-first policy. This committee has taken note in the past of FedRAMP, a project your predecessor began. We thought and still believe that it shows great promise. And yet, we continue to hear complaints from the agencies and industry about the program's slow progress. In fact, it wasn't until late last month (12/27/2012) that GSA was able to approve its first cloud-computing service company. What is the current status of FedRAMP, and your vision for its future?**

      FedRAMP launched Initial Operating Capability (IOC) on June 6, 2012. Government Certification and Accreditation (C&A) timelines average at least six (6) months for traditional on-premise information systems at the FIPS 199 Moderate Impact level. The security measures required for large-scale Cloud systems are even more complex and are expected to take a minimum of six months. FedRAMP ensures consistency and enables government-wide re-use and leveraging of the authorization and assessment process, and will save significant time and resources by eliminating duplicative security assessments.

Since the FedRAMP was launched in June 2012, accomplishments include:

- Established a baseline that sets security standards for Cloud Providers.
- Developed standard processes and templates for defining security responsibilities.
- Accredited 16 independent Third Party Assessment Organizations (3PAOs).
- Established a Secure Repository for Cloud Providers to upload their security documentation, for Agencies to leverage.
- Received applications from over 80 Cloud Service Providers.
- Engaged with FedRAMP applicants to discuss expectations and to determine readiness.
- Conducted extensive training and provided cloud providers with documentation reviews and guidance to prepare for the security authorization process.
- Granted Provisional Authorization to two Cloud Service Providers.

The FedRAMP program office at GSA anticipates that additional Provisional Authorizations will be forthcoming with continued authorizations during FY 2013.

b. Some industry observers have raised a concern that there may exist, either real or perceived, organizational conflict of interest between the 3PAOs and the service providers. Under the current GSA FedRAMP program guidance, an inspection body that is an affiliate or subsidiary of a cloud service provider may serve as a 3PAO. How do you plan to ensure the integrity of this important program?

FedRAMP accredited Third-Party Assessment Organizations (3PAOs) are required to meet the International Standard Organization (ISO) 17020 standard for inspection bodies. This standard establishes management rules governing independence for inspection bodies and defines three types of inspection bodies:

- Organizations chartered exclusively for inspection purposes. These inspection bodies may apply for accreditation as 3PAOs under FedRAMP.
- Organizations that conduct inspection activities of non-parent suppliers, but may also advise or recommend on the design process. This type of inspection body can apply to be a FedRAMP 3PAO, but may not provide implementation recommendations or documentation guidance for any provider that they assess.
- An inspection body that is an affiliate or subsidiary of a cloud service provider. These organizations are prohibited from being 3PAOs under FedRAMP, given their inherent conflict of interest.

By establishing the Conformity Assessment process, the Federal Government has recognized a substantively strengthened assessment capability:

- Inspection Bodies are held to a standard that requires both independence and technical competence. The requirements are clearly defined; only those organizations that demonstrate compliance with all requirements are approved to perform assessments under FedRAMP. By providing a list of approved organizations that meet these strict criteria, FedRAMP ensures consistency and reduces the burden on Cloud Providers and Authorizing Officials to evaluate assessors.

- The FedRAMP program office has also established grounds for suspension and revocation from the program. If a Third Party Assessor is not adhering to the management principles that maintain independence, FedRAMP can suspend and ultimately revoke the assessor's status in the program.

GSA and NIST have worked in concert to establish the process, review the applications and accredit the assessors. Adherence to these principles require rigor; 16 organizations have been accredited based upon their conformity to these high standards, the quality of their management plan and their technical competence. The future vision of the program is to transition the administration of the 3PAO accreditation process to a privatized board. The primary goal of this effort is to create a robust pool of accredited assessors without placing unnecessary burden on the Federal Government. Through privatization, FedRAMP will retain the valuable characteristics of the program without the overhead.

10. **How many FTEs are there with the title "Chief Information Officer" at the 24 CFO Act agencies? The Congressional Research Service (CRS) identified 220 in 16 agencies (attached). CRS' list of 220 omitted the Air Force CIO organization, and did not include several CFO Act agencies, including: Department of Veterans Affairs, Environmental Protection Agency, the Department of State, USAID, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, and Social Security Administration. Please provide a break-down by Department or Organization.**

OMB provides an oversight role for the information technology investments of the Federal Government by evaluating agency information resources management practices and, as part of the budget process, analyzes, tracks, and evaluates the risks and results of all major capital investments for information systems. Additionally, OMB notifies an agency if it believes that a major information system requires outside assistance. OMB does not have a role in nor does it manage the direct hiring or the titling of positions for specific agencies.

OMB works directly with the CIO of the agency, who has information resources management as their primary duty and advises and assists the head of the agency and other senior management to ensure that IT is acquired and managed according to current legislation and policies.

11. **SAM (the System for Award Management) is an e-Gov initiative that aims to integrate 10 different legacy acquisition systems into a single shared system in order to streamline processes, eliminate redundant data, and save taxpayer money. Late last fiscal year (9/2012), the initial launch of this system failed. Compounding the problem, September was the busiest time to award contracts and for the industry to be paid for services provided. What is OMB's role in managing government-wide acquisition systems such as the SAM system?**

When it was clear that SAM/IAE was not performing as planned, OMB performed a TechStat. Through the TechStat process, OMB provided recommendations, including encouraging the CIO to lead, shifting ownership, and strengthening governance. The IAE includes community governance, and OMB has recently reviewed and changed the existing governance based on lessons learned through the launch of SAM and the OMB TechStat. These changes will provide a more robust view into the business requirements and solutions recommended by GSA.

12. **The Federal Government uses a huge number of copies of COTS software such as Microsoft Windows or Office. When people move or change their computers, some of these licenses become dormant and become what is often called 'shelf-ware.' Some say we have numerous such shelf-wares but we do not know for sure because, despite the statutory requirement under the Clinger-Cohen Act for IT inventory, agencies do not have a comprehensive inventory of their IT assets. Moreover, even if an agency wants to utilize such shelf-ware or excess software licenses, they are often prohibited under the user-license agreement from transferring it to the other federal agencies. We have been told that the UK Government is structuring its software license agreements so that the entire UK Government is one user. What are your thoughts on this and how do you think the government can better manage its software user licenses so that there are no software licenses be purchase but do not use?**

OMB has followed the work of the UK closely in regards to COTS software purchases and the move to a single user model. The approach is quite interesting and there are a number of initiatives that are helping the UK better purchase at scale and reduce the number of duplicative contracts and licenses. In reviewing that model, due to the size and complexity of the U.S. Government, we must also ensure that this approach will actually save costs in the future while ensuring the appropriate level of service is maintained.

First, we believe CIOs should have control in determining when requirements need to diverge to meet specific business requirements and when the business should leverage the Intra-Agency Commodity IT Services called for in the Shared Services Strategy. M-11-29 specifically identifies that CIOs "must focus on eliminating duplication and rationalize their agency's IT investments. Agency commodity services are often duplicative and sub-scale ... The CIO shall pool their agency's purchasing power across their entire organization to drive down costs and improve service for commodity IT."[2]

We further emphasized this approach with the introduction of the PortfolioStat process. The intent with PortfolioStat is to require agencies to dig into the organization and ask the right questions about commodity IT spending. The outcome of that exercise was that agencies identified 98 opportunities to consolidate or eliminate commodity IT areas, ranging from the consolidation of multiple email systems across an agency to the reduction of duplicative mobile or desktop contracts. The work done in these areas will better standardize agency hardware will provide a model for use in the area of commercial software and OMB will continue to work with agencies in the coming year to address this issue.

This past December, OMB issued guidance, Memorandum 13-02, to strengthen the way agencies pool their resources to leverage the government's buying power and take strategic sourcing to the

[2] http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-29.pdf

next level.[3] This memorandum establishes a Strategic Sourcing Leadership Council (SSLC) comprised of the seven largest buying agencies and calls on them to identify and develop at least 15 new government-wide strategic sourcing solutions that their agencies will commit to using over the next two years. The highly collaborative process that the SSLC is using will allow us to shape strategies and vehicles to meet the collective needs of our agencies which, in turn, will increase the likelihood of agencies being able to successfully transition to government-wide vehicles in lieu of relying on their own.

In the end the result that OMB is seeking to implement is behavioral change—we believe that empowering CIOs to better analyze and evaluate investments will lead to a leaner, more efficient government and will free resources to innovate.

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

From: Jeff Rangel, Brocade Communications Systems, Inc.
To: Representative Jackie Speier

Subject: Brocade response to questions submitted by Rep. Jackie Speier (D-CA) for the Record House Oversight and Government Reform Committee

Hearing on January 22, 2013, "Wasting Information Technology Dollars: How Can the Federal Government Reform its IT Investment Strategy?"

Question 1. The privacy of consumer data is a very important issue to me. As Government is transitioning to the cloud, how can it ensure that vendors are able to protect its highly confidential data?

Brocade Communications shares your concern for the privacy of consumer data and the protection of consumers, users, or owners highly confidential data. As a private entity charged with protecting information about our business, our employees, our partners, and our customers, we also seek to ensure the security of this data in cloud environments.

Cloud computing and the networking that enables it offer tremendous financial and efficiency benefits to those entities, both public and private, that deploy them. In order to realize those benefits fully, certain data must be protected according to its sensitivity. Today protection and security of information in the cloud is multifaceted including technology, governance, policy, and compliance. The technology to secure networks and IT environments is available today and has been safely securing our Government's most sensitive information, including classified information, for years.

Various standards are in place to define levels of protection that are needed for certain types of data, and to define the characteristics of that protection. These include security guidelines as prescribed by the National Institute of Standards (NIST) under Federal Information Security Act (FISMA) and in compliance with Federal Information Processing standards (FIPS). This includes encryption standards like FIPS 197 and wireless communication standards like FIPS 140-2. (

As Government transitions to the cloud, it will establish specifications for vendors concerning security and privacy requirements, referencing those standards described above, when appropriate. Government will also specify physical security standards for facilities that house data centers, including surveillance, barriers to entry, access controls, and fire suppression. It will require personnel clearances similar to, or in accordance with, guidelines issued by the Defense Security Service (DSS). Government will specify security practices for mobile devices and user authentication methods that can access the protected information in the cloud while complying with the Homeland Security Presidential Directive 12 (HSPD-12). Employees must verify their identity and security classifications using secure and reliable forms of identification, such as Common Access Card (CAC) and Personal Identity Verification (PIV).

Question 2. I am concerned that the transition to the cloud includes sufficient protections to protect the privacy of consumer data. What security requirements should CIOs create for vendors?

CIOs should set security requirements according to the type and sensitivity of data they are protecting. CIOs will move applications and information to cloud-based solutions according to the sensitivity of the information. They will choose between private clouds or public clouds based how that information has been classified. Brocade believes that most Federal Agencies will use a hybrid of private and public cloud solutions for their operations; however, all of these will be enabled by networking. As an example, information that can be readily obtained under the Freedom of Information Act (FOIA) could easily be moved to public clouds while classified national security information would reside on private clouds under strict governance by the agency.

CIOs will establish security requirements as specified in our previous response and will leverage the security requirements already specified in certifications including:

- Common Criteria: The Department of Defense's Common Criteria for Information Technology Security Evaluation.
- FIPS: Federal Information Processing Standards.
- FISMA: Federal Information Security Act and guidelines furnished by National Institute of Standards and Technology (NIST).

CIOs will leverage accreditation processes and testing authorities to include:

- FedRAMP: Federal Risk and Authorization Management Program accreditation standards
- JITC: Department of Defense's Joint Interoperability Test Command certification testing.

Microsoft Corporation
Microsoft Innovation & Policy Center
901 K Street, NW 11th Floor
Washington, DC 20001

Tel 202-263-5900
Fax 202-263-5901
http://www.microsoft.com/

Microsoft | Innovation & Policy Center

February 13, 2013

Mr. Darrell Issa, Chairman
Committee on Oversight and Government Reform
2471 Rayburn House Office Building
Washington, DC 20515

Mr. Elijah Cummings, Ranking Member
Committee on Oversight and Government Reform
2471 Rayburn House Office Building
Washington, DC 20515

Ms. Jackie Speier, Member
Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Issa, Ranking Member Cummings, and Representative Speier:

Thank you again for the opportunity to testify before the Committee on Oversight and Government Reform on January 22, 2013 at the hearing entitled, "Wasting Information Technology Dollars: How Can the Federal Government Reform its IT Investment Strategy?" We at Microsoft appreciate your attention to this important matter. We look forward to continuing the conversation as the Committee on Oversight and Government Reform considers Chairman Issa's draft legislation, the Federal Information Technology Acquisition Reform Act (FITARA).

We also appreciate the opportunity to answer the following questions from Representative Speier that Chairman Issa forwarded in a letter dated January 30, 2013:

1) *The privacy of consumer data is a very important issue to me. As Government is transitioning to the cloud, how can it ensure that vendors will be able to protect its highly confidential data?*

2) *I am concerned that the transition to the cloud includes sufficient protections to protect the privacy of consumer data. What security requirements should CIOs create for vendors?*

Summary:

As Government is transitioning to the cloud, questions like Representative Speier's become important: how to ensure that vendors will be able to protect highly confidential Government data and data collected from the citizens of this country. We believe that all of our customers need to carefully weigh a range of core considerations in every decision about the acquisition or use of technology. This is especially true of the Government, which often serves as a steward of highly personal data, including tax filings, student data, and health care records. Not only is much of this data confidential, the protection of some data is also critical to national security.[1]

---

[1] "Consumer Email and Government: A Dangerous Mixture," by Jeff Gould, Peerstone Research, Monday, April 2, 2012, http://www.safegov.org/2012/4/2/consumer-email-and-government-a-dangerous-mixture, visited February 12, 2013.

Microsoft Corporation
Microsoft Innovation & Policy Center
901 K Street, NW 11th Floor
Washington, DC 20001

Tel 202-263-5900
Fax 202-263-5901
http://www.microsoft.com/

Microsoft | Innovation & Policy Center

While we address both privacy and security implications of cloud computing in this letter, it is important to note that these are, in fact, two distinct issues. For example, just because a service provider has the ability to keep data secure (e.g., to prevent a breach of security), does not mean that the service provider's policies ensure privacy and prevent the data from being used for unrelated or unintended purposes. Microsoft is proud that its business as a cloud services provider is distinguished from some other providers in that Microsoft's broader business does not depend on the collection and monetization of our customers' private information for advertising purposes.

For our government customers, we believe the key to ensuring the sanctity of highly confidential data is to adopt meaningful baseline security and privacy controls across all cloud offerings. Once those baseline standards have been established and communicated, it is important to empower agency CIOs to evaluate the "best value" of a potential IT investment by examining core factors, including security, privacy, and accessibility, rather than merely looking at simple cost comparisons. The weighting of those factors should be mission-focused, a step best suited for agency CIOs who know the missions of their agencies and the requirements needed to support them. Agencies should transparently communicate their needs to the market, as well as how different evaluation factors will be weighed to meet those needs. Those offering cloud services to the Government should then have a reciprocal obligation to demonstrate in an equally transparent manner how the services they offer meet the Government's needs.

Discussion:

The Government should require certain baseline security and privacy requirements for Government use of cloud-based services. FedRAMP is an important step in this direction. Once those requirements have been established and clearly communicated to the market, then agency CIOs should have the freedom to select from among vendors offering services that meet the baseline requirements. CIOs are best positioned to decide what additional requirements are necessary to provide the best value to the missions of the agencies they serve.

However, when CIOs are considering investing in new technology, and particularly where highly sensitive data is at stake, "best value" means more than price. I discussed this issue in my written testimony:

> The then-U.S. CIO, OFPP Administrator, and IP Enforcement Coordinator noted that "as program, IT, acquisition, and other officials work together to develop requirements and plan acquisitions, they should follow technology neutral principles and practices," which means "selecting suitable IT on a case-by-case basis to meet the particular operational needs of the agency by considering factors such as performance, cost, security, interoperability, ability to share or re-use, and availability of quality support."
>
> As part of a transparent, fair and cost-effective technology selection and evaluation process, in which the competition is full and open to all competitors, we recommend that neutral factors such as the following be used:

Microsoft Corporation
Microsoft Innovation & Policy Center
901 K Street, NW 11th Floor
Washington, DC 20001

Tel 202-263-5900
Fax 202-263-5901
http://www.microsoft.com/

Microsoft | Innovation & Policy Center

1. Total cost of ownership/operation over the anticipated lifecycle for the technology;

2. Security/resiliency of the technology against attack or unauthorized access, including applicable requirements such as IT security controls, authorization and monitoring (FISMA), patient privacy (HIPAA), confidentiality of criminal justice records (CJIS), and educational privacy (FERPA);

3. Privacy implications for both citizens and Government users who interact with the technology;

4. Accessibility of the system to those with disabilities;

5. Integrity of records maintenance, such that they can be archived and retrieved intact for future reference as authoritative proof of final agency actions;

6. Data portability to allow for interaction between data systems, citizen access to data, and migration between service offerings; and

7. Openness of the technology in terms of utilizing globally recognized, [interoperable] standards.

Different factors will be more important to different federal customers, depending on the unique needs of the mission that must be satisfied. The Government should ensure that procuring agencies define clearly and transparently what factors will weigh most heavily in a determination of "best value" in a particular procurement.

Agency CIOs will need to ensure that the cloud service provider can protect that data from security breaches or leakages, as well as ensuring that the IT provider can demonstrate that customer or user data won't be used for any unauthorized purposes. Vendors should be required to show how they will meet these essential requirements. . . . [Vendors should also be required] to describe in advance exactly what uses they will and will not make of customer and user data.[2]

Microsoft takes the security of its cloud offerings very seriously. Our various cloud services adhere to a wide range of standards, many of which are independently verified and intended to demonstrate the rigorous processes we have in place to manage cyber risks for our cloud customers. For example, we

[2] Written Statement of Chris Niehaus, Director, Office of Civic Innovation, Microsoft Corp. before the Committee on Oversight and Government Reform at the hearing entitled, "Wasting Information Technology Dollars: How Can the Federal Government Reform its IT Investment Strategy?" January 22, 2013

Microsoft Corporation is an equal opportunity employer.

Microsoft Corporation
Microsoft Innovation & Policy Center
901 K Street, NW 11th Floor
Washington, DC 20001

Tel 202-263-5900
Fax 202-263-5901
http://www.microsoft.com/

Microsoft | Innovation & Policy Center

have implemented robust data privacy and security measures in Office 365, our cloud-based business productivity software.

> Office 365 provides secure access across platforms and devices, as well as premium anti-spam and antivirus technologies that are automatically updated to protect against the latest threats. The security features and services associated with Office 365 are built in, reducing the time and cost associated with securing . . . IT systems. At the same time, Office 365 enables [users] to easily control permissions, policies, and features through online administration and management consoles so you [users] can configure Office 365 to meet . . . specific security needs.
>
> . . .
>
> Microsoft has been providing online services for many years. Microsoft Global Foundation Services (GFS), the group responsible for hosting Office 365 and all of Microsoft's online services, started in 1994 with the introduction of MSN and has grown to include some of the world's most well-known Internet properties. The online services infrastructure layer (GFS) is regularly audited by respected third party organizations. Through our comprehensive approach to security and privacy, Microsoft Global Foundation Services has obtained ISO 27001 and EU Safe Harbor certification and successfully completed SAS 70 Type II audit. Office 365 is based on proven technology, representing the latest generation of what was formerly known as Business Productivity Online Services (BPOS) with hundreds of thousands of satisfied customers.
>
> . . .
>
> Microsoft recognizes that security is an ongoing process, not a steady state—it must be constantly maintained, enhanced, and verified by experienced and trained personnel; supported by up-to-date software and hardware technologies; and refined through robust processes for designing, building, operating, and supporting our services.[3]

The questions from Representative Speier have implications beyond the issue of whether or not the personally identifiable data and communications held by a cloud provider on behalf of a Government agency will be adequately protected against malicious attacks or accidental disclosures. They also address the "privacy of consumer data." The Government should think carefully not only about how citizen data will be secured, but whether any unrelated or secondary uses of that data should be permitted by the cloud provider in furtherance of its own business interests. Microsoft, for example, has made clear to customers that it is willing to make the following commitment, and Microsoft believes that Government Requests for Proposals (RFPs) should require all competitors to do so as well:

---

[3] Office 365 Security White Paper, http://g.microsoftonline.com/0BXPS00EN/1167, visited February 12, 2013.

Microsoft Corporation
Microsoft Innovation & Policy Center
901 K Street, NW 11th Floor
Washington, DC 20001

Tel 202-263-5900
Fax 202-263-5901
http://www.microsoft.com/

Microsoft | Innovation & Policy Center

> Offeror's online service shall use data that customer provides through its use of the online service only to provide and maintain the service for the customer. Offeror's online service shall not capture, maintain, scan, index, share or use customer data stored or transmitted by the service, or otherwise use any data-mining technology, for any non-authorized activity or non-government purpose. Offeror's online service shall not use customer data stored or transmitted by the online service for any advertising or other commercial purpose of Offeror or any third party. Offeror's online service will be logically separate from its consumer online service. Customer data, data in Offeror's consumer online services, and data created by or resulting from Offeror's scanning, indexing, or data-mining activities, will not be commingled unless expressly approved by Customer in advance.

Secondary use of data by a cloud provider is an important consideration for the Federal Government. Citizens are often required to share sensitive information with the Government in order to comply with the law. In addition, citizens have a constitutional right to freely communicate with and petition their Government. Such exchanges may be hampered if citizens feel that information shared with the Government may be subjected to some unrelated commercial use by a vendor providing cloud services.

To address these concerns about the secondary use of data by vendors, we offer the following recommendations from Karen Evans, former Administrator of the Office of Electronic Government and Information Technology (IT) at the Office of Management and Budget, and Jeff Gould, an expert in technology publishing and IT market research. They recommend that public sector cloud customers should:

> 1. Update agency PIAs [Privacy Impact Assessments] to ensure that data storage and use at all technical layers from storage through applications comply with existing statutes, regulations, policies and procedures.
>
> 2. Create an audit program to ensure appropriate segregation of government data at all levels (e.g. host, network, application, and platform). GSA, through its existing FedRAMP program, should require TPAOs [Third Party Assessment Organizations] to publish their audit results and opinions so that Congress and the public may verify that the cloud providers are meeting the terms of their Federal contracts.
>
> 3. Require the adoption and publication of privacy policies for government customers that expressly ban the collection or processing of end-user information for purposes

Microsoft Corporation
Microsoft Innovation & Policy Center
901 K Street, NW 11th Floor
Washington, DC 20001

Tel 202-263-5900
Fax 202-263-5901
http://www.microsoft.com/

Microsoft | Innovation & Policy Center

(such as advertising or marketing) that are unrelated to the intended state purpose in their privacy policies and PIAs.[4]

Conclusion:

Again, on behalf of Microsoft, I want to thank you and the other Members of the Committee on Oversight and Government Reform for your continued leadership on the issue of Federal IT acquisition reform. We appreciate having had the opportunity to participate in the hearing you held last month and to answer the questions offered by Representative Speier. We look forward to continuing the dialogue in an effort to ensure that the Government gets the best value for its IT dollars, which includes considerations not only of cost, but of privacy and security as well.

Best wishes,

Chris Niehaus,
Director, US Office of Civic Innovation
Microsoft Corporation

[4] "U.S. Government Users Should Insist On The Same Privacy Protections As Europeans," by Karen Evans, KE&T Partners, Jeff Gould, Peerstone Research, Wednesday, October 24, 2012, http://www.safegov.org/2012/10/24/us-government-users-should-insist-on-the-same-privacy-protections-as-europeans, visited February 12, 2013.

United States Government Accountability Office
Washington, DC 20548

February 13, 2013

The Honorable Darrell Issa
Chairman
The Honorable Jackie Speier
Committee on Oversight and Government Reform
House of Representatives
Washington, DC 20515

Subject: *Federal Information Technology (IT) Investment Management*

This letter is in response to questions you sent us following the January 22, 2013 hearing on the management of federal IT investments.[1] At the hearing, we discussed results and recommendations from our selected reports that focused on key aspects of the federal government's acquisition and management of IT investments. 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,

David A. Powner
Director, Information Technology
Management Issues

Enclosure

cc: Alexia Ardolina, Assistant Clerk

[1]GAO, *Information Technology: OMB and Agencies Need to Fully Implement Major Initiatives to Save Billions of Dollars*, GAO-13-297T (Washington, D.C.: Jan. 22, 2013).

Post-Hearing Questions for the Record

Submitted to Mr. David Powner, GAO

From Rep. Darrell Issa

"Wasting Information Technology Dollars: How Can the Federal Government Reform its IT Investment Strategy?"

January 22, 2013

1. You testified that when GAO conducted a study on the critical factors underlying successful IT projects (GAO-12-7), three of the agencies surveyed could not provide GAO with a single successful IT project. Please identify the three agencies, describe how much money they spend annually on IT, and summarize their recent dashboard performance.

The three departments that were unable to identify an IT investment that met the criteria for our study[2] were the Departments of Agriculture, Health and Human Services, and Justice.

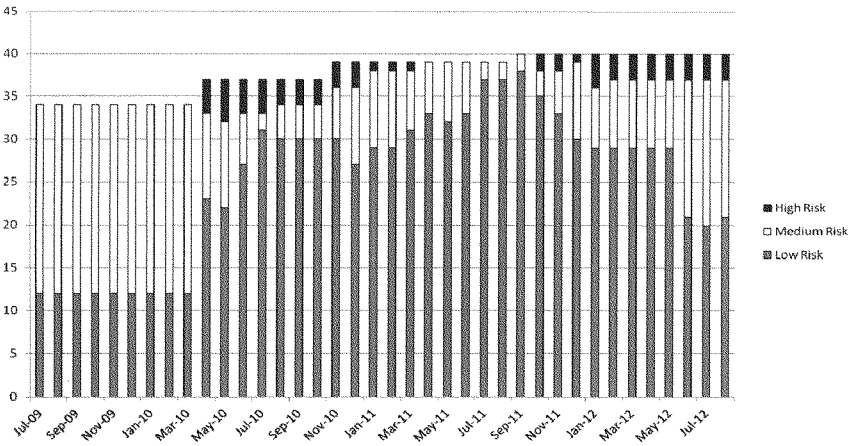
As reported by the departments to the Office of Management and Budget, the departments are planning to spend the following in fiscal year 2013 on IT:

- The Department of Agriculture: $2.6 billion
- The Department of Health and Human Services: $7.1 billion
- The Department of Justice: $2.7 billion

The Chief Information Officers (CIO) of all three departments rated the majority of their investments as low or medium risk. Since June 2012, the Department of Agriculture had an increase of investments moving from low risk to medium risk. Additionally, the Department of Health and Human Services rated most of their investments as low risk in the same time period. Similarly, the Department of Justice rated the majority of their investments as low or medium risk and reported no high risk investments since May 2012. The following figures for each department depicts the number of investments at each rating level for the end of each month from July 2009 through July 2012, as reported on the federal IT Dashboard.

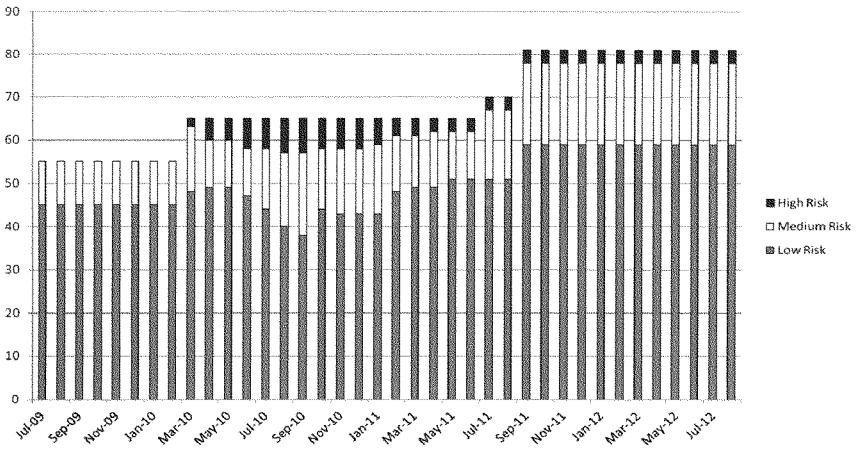
[2]GAO, *Information Technology: Critical Factors Underlying Successful Major Acquisitions,* GAO-12-7 (Washington, D.C.: Oct. 21, 2011).

CIO Ratings for Major IT Investments at the Department of Agriculture



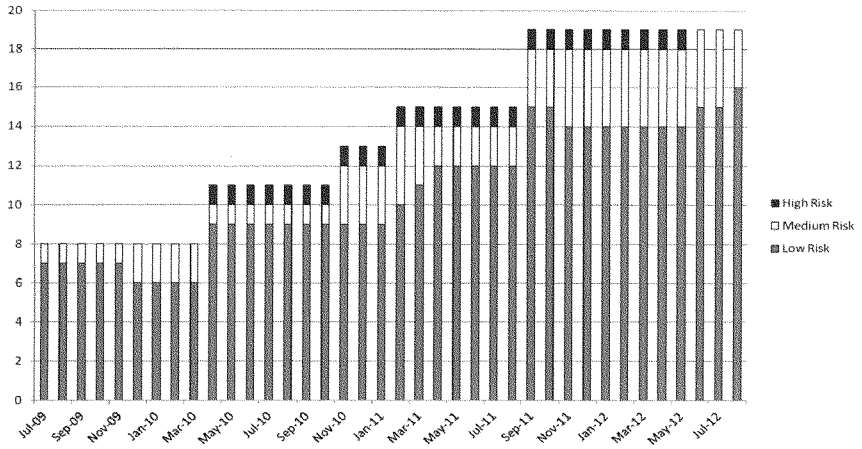
Source: GAO analysis of IT Dashboard data.

CIO Ratings for Major IT Investments at the Department of Health and Human Services



Source: GAO analysis of IT Dashboard data.

CIO Ratings for Major IT Investments at the Department of Justice



Source: GAO analysis of IT Dashboard data.

Post-Hearing Questions for the Record

Submitted to Mr. David Powner, GAO

From Rep. Jackie Speier

"Wasting Information Technology Dollars: How Can the Federal Government Reform its IT Investment Strategy?"

January 22, 2013

1. At the end of last year I sent a letter to this committee calling for an investigation of how a program like ECSS could get so far, cost taxpayers a billion dollars, and have to little to show for it. FOIA documents indicate OMB held at least three TechStat meetings with DOD officials about this program, but DOD never identified it as a high risk area in the IT Dashboard, and we really didn't know how badly the program was failing until it was canceled. It seems like many processes failed here, but what does the ECSS program tell us about how OMB and agencies use the IT Dashboard and TechStat meetings? What steps is OMB taking to prevent this from happening again, as DOD struggles with what GAO assesses—and I agree—is a very risky acquisition portfolio of business enterprise systems?

Our October 2012 report on the IT Dashboard showed that opportunities existed to improve transparency and oversight of investment risk at our selected agencies.[3] The report specifically found that selected ratings for DOD's investments did not appropriately reflect significant cost, schedule, and performance issues reported by GAO and others. Similar to ECSS, we noted that three DOD investments experienced significant performance problems and were part of a GAO high-risk area (business systems modernization), but they were all rated low risk or moderately low risk by the DOD CIO. For example, in early 2012, we reported that Air Force's Defense Enterprise Accounting and Management System (DEAMS) faced a 2-year deployment delay and an estimated cost increase of about $500 million from an original life-cycle cost estimate of $1.1 billion (an increase of approximately 45 percent), and that assessments by DOD users had identified operational problems with the system, such as data accuracy issues, an inability to generate auditable financial reports, and the need for manual workarounds.[4] However, DOD's CIO rated DEAMS low risk or moderately low risk from July 2009 through March 2012. Therefore, we recommended that DOD ensure that its CIO ratings reflect available investment performance assessments and its risk management guidance.

Regarding the steps OMB could take, we recommended that OMB analyze agencies' investment risk over time as reflected in the Dashboard's CIO ratings and present its analysis with the President's annual budget submission in order to ensure that OMB's preparation of the submission accurately reflects the risks associated

---

[3]GAO, *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).
[4]GAO, *DOD Financial Management: Reported Status of Department of Defense's Enterprise Resource Planning Systems*, GAO-12-565R (Washington, D.C.: Mar. 30, 2012); and *DOD Financial Management Implementation Weaknesses in Army and Air Force Business Systems Could Jeopardize DOD's Auditability Goals*, GAO-12-134 (Washington, D.C.: Feb. 28, 2012) .

with all major IT investments. OMB concurred with our recommendation. If implemented, this step could aid OMB in holding agencies accountable for providing accurate ratings on the Dashboard.

2. Mr. Powner, it seems like GAO has noted several times the lack of data and inventory that would allow for an accurate assessment of cost savings for data consolidation and cloud computing efforts, or really developing an efficient strategy moving forward. What do you believe to be the major hurdles for agencies' implementing this and other GAO recommendations?

Our recent data center consolidation report[5] noted several challenges that agencies have faced in implementing these efforts. Specifically, for data center consolidation, we found that the agencies' inventories were incomplete due to challenges in gathering data center power usage information, a key component of calculating planned consolidation cost savings; and more broadly, problems providing good quality asset inventories, as OMB requires. OMB requires both a master program schedule and a cost-benefit analysis as key elements of agencies' consolidation plans, but none of the selected agencies we evaluated had complete schedules or cost estimates. We therefore reiterated a recommendation from our prior data center consolidation report[6] that OMB require agencies complete the missing elements in their consolidation inventories and plans. In addition, we recommended that select agencies implement recognized best practices when completing required program schedules and cost-benefit analyses.

[5]GAO, *Data Center Consolidation: Agencies Making Progress on Efforts, but Inventories and Plans Need to Be Completed,* GAO-12-742 (Washington, D.C.: July 19, 2012).
[6]GAO, *Data Center Consolidation: Agencies Need to Complete Inventories and Plans to Achieve Expected Savings*, GAO-11-565 (Washington, D.C.: July 19, 2011).

February 8, 2013

The Honorable Congresswoman Jackie Speier
2157 Rayburn House Office Building
Washington, DC 20515-6143

Dear Congresswoman Speier:

Thank you for your questions related to the hearing before the Committee on Oversight and Government Reform on January 22, 2013 entitled "Wasting Information Technology Dollars: How Can the Federal Government Reform its IT Investment Strategy?" I sincerely appreciate the opportunity to testify before the Committee and share my thoughts on this very important matter.

Thank you for forwarding your follow up questions. As a former CIO in the Federal government and former head of a component Agency, I have tremendous passion and desire to help my former employer improve the effectiveness and performance of IT investments for the good of the American taxpayers.

I have provided my written responses to your thoughtful questions herein. I also offer to meet with your key staff members, or yourself, to discuss these responses in more detail at your convenience. My contact information is provided below for this purpose. Thank you again for the opportunity to provide additional information in response to your questions.

Sincerely,

/s/
Douglas J. Bourgeois
VP & Chief Cloud Executive
VMware U.S. Public Sector
1902 Campus Commons Dr., Suite 510
Reston, VA 20191
dbourgeois@vmware.com

1. As a former CIO, what OMB efforts do you see as most important? What efforts do the most to strengthen CIO effectiveness and accountability? Do you see any of the efforts as potentially counterproductive?

As you know, OMB plays a substantial role encompassing broad management and budget authorities across the federal government. From an IT management perspective, OMB has established a set of policies and initiatives that are generally very supportive of the CIOs' efforts. Initiatives such as the 15 Point Implementation Plan and the Federal Data Center Consolidation Initiative have set an appropriate direction for IT program and performance improvement. Still other initiatives such as Continuous Monitoring and FedRAMP appear to be headed in the right direction and show considerable promise, albeit more slowly than some would desire. These initiatives simply require continued guidance and support to ensure the overall objectives are met and value is commensurate with the level of effort. For example, the FedRAMP initiative, while widely recognized as a significant step forward, slows progress and innovation because once the Authority to Operate (ATO) has been issued, the service provider is reluctant to make any changes or improvements to the technology environment which would require another round of testing which drives up costs.

Another area for continued support by OMB is the effort to consolidate data centers across the Federal government. This effort has been successful in driving a smaller and less complex technology footprint across the Federal data center landscape and saving money. But this effort only scratches at the surface of the cost savings opportunity. By GAOs estimate, the Federal government invests in about 2,271 "back office" applications such as supply chain, human resources, finance, and planning. In the aggregate, these applications cost about $9.1 billion. Expanding the emphasis for the consolidation initiative beyond the infrastructure into these common applications would substantially increase the cost savings opportunity.

In addition, OMB efforts to improve CIO accountability also appear to have had measured

success. The TechStat, PortfolioStat, and IT Dashboard may require some additional improvements to be most effective, but these clearly have created an environment of increased accountability and established additional incentive for performance. OMB could do more to recognize that, at times, overall IT program performance can be affected by decisions made within large programs across the agency level. OMB could address this gap by developing policies that bring major program executives and the CIO closer together in a joint accountability model, where applicable. In many cases, the success of an initiative that has a major IT component relies equally upon the leadership, commitment and collaboration of the CIO and key program executives. Any efforts to address accountability must take this organizational reality into consideration.

Another area where OMB could do more to facilitate success would be in the area of culture. As I mentioned in my opening statement and written testimony, the culture in both IT and acquisition organizations needs to change. Any meaningful improvements to the IT acquisition environment must be supported by leadership from OMB. In my written testimony, I expressed the need for the culture to become more services based. For such a change to occur, IT acquisitions need to become more outcome oriented based on a standard framework for normalization of services, costs, and performance across the spectrum of commodity services. These and the other changes necessary for this transformation to occur will require considerable leadership across the government, including OMB.

2. You mention that the U.S. Patent and Trademark Office and NASA have employed crowd sourcing to make historical performance information more transparent. What is your understanding from the lessons learned from that effort, particularly when it comes to having proper controls in place to ensure there is proper competition?

Over the past five years, NASA has offered the *NASA Tournament Lab* (NTL) as a competitive crowd sourcing platform. Government agencies including the U.S. Patent and Trademark Office, and government programs such as the Networking and Information Technology Research and Development (NITRD) program, have successfully leveraged NTL to efficiently and fairly execute competitions. Some of the lessons learned that have been identified regarding the use of proper controls for ensuring proper competition include:

1. Competitions must provide broad and meaningful incentives including monetary, recognition, and non-monetary awards to ensure a diverse and sizable pool of competitors. In addition, it is not sufficient to award only a first place winner; other awards must be offered to encourage future participation from a large pool of competitors. In addition, similar to current Small Business Administration programs, the competitions should offer additional "set-aside" awards for individuals deemed socially or economically disadvantaged.
2. Much like in traditional contracting, competitions must be properly structured in terms of definition, scope, and deliverables. Ambiguities in any aspect of the competition plan lead to poor results from competitors and dissatisfaction from clients.
3. Candidate competitors must go through a vetting process. This process may be a self-certification process, or it may be performed with greater rigor and documentation executed by an independent party. For example, the crowd sourcing platform vendor may provide a process for competitors to demonstrate proof of citizenship or residency. The crowd sourcing platform vendor then warrants competitor's citizenship to the government.
4. The crowd sourcing platform must have transparency. Agencies must be able to see which competitors plan to compete, they should have the ability to anonymously monitor competitor's work progress, and they must be able to review and confirm suitability of winning solution(s).

5. Security is paramount towards ensuring proper competition. Information must be tightly controlled through obfuscation or abstraction on high-security areas of an application so that the crowd can build upon solutions without the Government exposing secure assets (process, "intellectual property," and data). Additionally, the software code solutions must go through stringent security reviews; both from the crowd sourcing vendor and the Government, before approval and acceptance of software code.

It is important to note that the crowd sourcing platform vendors must have the ability to apply various "filters" to determine which participants in the crowd may be eligible to participate in a competition. These filters could be very thorough and include U.S. citizenship, U.S. based location, various levels of security clearance, widely varying areas of expertise, and historical performance just to name a few. In addition, from a competitive standpoint, the larger the crowd the more competitive the acquisition will be so it is also important to ensure that the platform provider has a strong capability and track record of gaining qualified participants in the crowd.

3. The privacy of consumer data is a very important issue to me. As Government is transitioning to the cloud, how can it ensure vendors will be able to protect its highly confidential data?

The privacy of consumer data is very much a key concern with the Government's transition to the cloud. Government and private sector information privacy and security professionals have been vocal from the beginning regarding the need for adequate controls protecting data that is stored and accessed in the cloud. As a result, efforts including The Federal Risk and Authorization Management Program (FedRAMP) and the Cloud Security Alliance were implemented to help CIOs, CISOs, CSOs, and other executives understand the risks involved

with moving to the cloud. These programs provide guidance and state requirements that must be met to protect personally identifiable information (PII) and confidential data in the cloud.

In particular, FedRAMP provides a specific set of requirements, which a cloud vendor must be assessed against and independently certified by designated third-party assessors. Using a formal assessment process, cloud vendors must demonstrate they are compliant with the requirements put forth by FedRAMP, including the security of data. The assessment process uses a set of security controls in accordance with Federal Information Security Management Act (FISMA), using a baseline of the National Institute of Standards (NIST SP 800-53.) So while there is definitely legitimate concern in moving data to the cloud, Federal information technology leaders and vendors have a set of programs and standards they can follow to protect the privacy of consumer data.

In addition, the Government has the opportunity to embrace evolving technologies that are designed specifically to provide security commensurate with risk, even in a cloud model. Within the private cloud, the Government can leverage virtual networking and security technologies to ensure adequate security controls are in place for the most highly confidential data. These technologies work in concert with cloud management technologies to extend security policies and monitoring across networks and into other cloud environments that the Government may have an interest in using. Such technologies include, but are not limited to, a federated identity management solution that would most efficiently manage and control access to Government applications and data that crosses cloud environments.

4. I am concerned that the transition to the cloud includes sufficient protections to protect the privacy of consumer data. As a former CIO, what security policies should CIO's create for vendors?

The regulations and standards for protecting the privacy of consumer data continue to evolve as Government and industry continue to adopt the cloud model for delivering information technology services. Information technology security, and the protection of data, should be addressed from three aspects: people, processes, and technology. As a former CIO, I would expect cloud vendors to provide and adhere to the following security measures:

1. People: Cloud vendors should be required to complete annual training and certification on the identification, handling, and proper disposition of privacy data within their cloud. This includes educating cloud vendors on the procedures and protocols for identifying and detecting possible breaches in security. Cloud vendor personnel with potential access to privacy data should be made accessible to Government audits and inspections.

2. Processes: Cloud vendors must demonstrate they have sufficient oversight processes in place to protect privacy data. Processes include:

    a. The establishment of what cloud vendor personnel may have accesses to privacy data, for what purpose; and frequent reassessments of such access.
    b. Restrictive and transparent policies on the distribution, logging, retention, and backup of privacy data.
    c. The detection, notification, and coordination of privacy breaches with Federal authorities and specific Government entities affected by a privacy breach event.
    d. Contractual, written confirmation stating the Government owns all rights to data stored in the cloud vendor's cloud. Additionally, the agreement should state that the cloud vendor has no rights to the Governments data. Further, the cloud vendor should describe the process, format, and time frame for providing data back to the Government upon termination of a cloud vendor's partnership with the Government.

3. Technology: Perhaps the greatest advancements in the protections of privacy data will be achieved through new technologies and the way cloud vendors and Government apply those technologies. Some advancements in data protection technology which should be employed include:

    a. Protecting data "at rest" at all times. Traditionally, data has only been encrypted in transit (e.g. sending data from a database to a web page). Now, data can be relatively easily and inexpensively encrypted while stored in databases, files, and external media. In addition, the ability to encrypt data in memory is now becoming an affordable technology, which would then render data in the cloud encrypted at all times.
    b. Automatically detecting and preventing the improper transmission of privacy data outside a vendor's cloud through a practice called data loss prevention. Today, technologies exist which can identify patterns of privacy data, such as a social security number or data of birth, and will prevent the improper transmission of such data (e.g. to a USB thumb drive or Excel spreadsheet on a vendor's laptop) and log the incident for immediate follow-up by the proper security incident response personnel.
    c. Decreasing and obfuscating the "attack plane" through the use of Software Defined Networking (SDN) and Software Defined Data Centers (SDDC). Most attacks on information technology infrastructure occur to physical endpoint devices including computer servers, routers, and storage devices. Adding a complete layer of virtualization upon physical assets allows cloud vendors to constantly move the location, and therefore the traditional access points, of an attack. Virtualization makes it extremely difficult for hackers to continuously attack a specific information technology infrastructure access point.

Most importantly, and for the foreseeable future, I believe the best method of protecting the privacy of consumer data in the cloud will be for Government to use the hybrid cloud model. In general, the hybrid cloud model is recognition that Government should exclusively control certain applications and data within Government data centers (private clouds), while a public cloud vendor may maintain other Government applications and data with non-private or non-sensitive data.

Employing a Hybrid cloud allows the Government to determine the circumstances for which a Government computing workload, application, or dataset will be transferred from a private cloud to a public cloud vendor, and back again if needed. I believe the hybrid cloud model offers the Government the best flexibility and control for protecting consumer data.

CONSORTIUM FOR CITIZENS
WITH DISABILITIES

Submitted Testimony for House Oversight and Government Reform Committee Hearing on

Wasting Information Technology Dollars: How Can the Federal Government Reform its IT Investment Strategy?

Tuesday, January 22, 2013

On behalf of the Consortium of Citizens with Disabilities (CCD) Telecommunications and Technology Task Force we thank you for holding this hearing today, and appreciate the opportunity to submit written testimony.

CCD is a coalition of national disability organizations working together to advocate for national public policy that ensures the self-determination, independence, empowerment, integration and inclusion of children and adults with disabilities in all aspects of society. Since 1973, the CCD has advocated on behalf of people of all ages with all types of disabilities. CCD has worked to achieve federal legislation and regulations that assure that the 54 million children and adults with disabilities are fully integrated into the mainstream of society. The Telecommunications and Technology Task Force focuses on ensuring national policy on matters of telecommunications and technology, including assistive technology, helps move society toward our ultimate goal of full inclusion of all people with a disability.

People with disabilities can, and do, work in all areas of American society, including the federal workforce. They thrive when they fully participate, and in turn, the nation thrives. President Obama recognized the importance of the federal government in employment of people with disabilities when he issued Executive Order 13548 which stated, "As the Nation's largest employer, the Federal Government must become a model for the employment of individuals with disabilities."

Every day, accessible information technology systems (both hardware and software) allow people with a disability to be included in all aspects of federal employment. However, the key there is that the systems are accessible. If the systems fail to live up to the accessibility standards of Section 504 and 508 of the Rehabilitation Act, then the technology is not helpful for the person with a disability to fulfill their job requirements.

Unfortunately, even with Executive Order 13548, the federal government has not lived up to being "a model for the employment of individuals with disabilities."

A September 2012 report from the Department of Justice on the accessibility of federal government electronic and information technology found that while a significant amount of information technology is accessible for people with disabilities, there is still much progress that could be made to ensure accessibility. In fact at times, "...accessibility has often been an afterthought. Modifying existing technology to make it accessible is much more difficult and much more expensive than designing technology in an accessible manner in the first place."

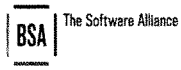
This is often a critical, but often overlooked point: to ensure the full benefits, in a cost effective manner, of accessible technology it is better to make the technology accessible at its introduction through universal design. Introducing technology and then making it accessible at a later time is a highly ineffective and cost inefficient way to produce something accessible. As one of the largest purchasers of information technology systems in the United States, and to follow through with being "a model for the employment of individuals with disabilities," the federal government needs to ensure that accessibility through universal design is included at the beginning when considering products to purchase, not after they have already been purchased. Doing so will ensure that the federal dollars spent on information technology systems is not spent inefficiently.

The CCD Telecommunications and Technology Task Force calls on the federal government and private entities to work with the disability community in the beginning, at the development stage, to ensure that the new technology is fully accessible to all. This will be a much more efficient way of doing business, and we as members of the task force stand ready to help.

A civil right without enforcement is just words on paper. That is why it is extremely important that the civil right to accessible technology be strongly enforced by the Department of Justice and other agencies within the federal government. First, we encourage the Department of Justice to continue, and even strengthen and be more consistent in, its work being done on enforcing laws requiring accessible technology. The Department should look to members of CCD, especially the Telecommunications and Technology Task Force, to help expose situations where civil rights to accessible technology are being violated as well as ways to address these violations. In addition, the Department needs to move forward with their web access regulations for the Americans with Disabilities Act as they would help ensure that people with disabilities have full access to the web to find employment, as well as use the resources on the web to fulfill their job duties. Finally, clear AND final regulations will go a long way to encouraging the use and production of accessible technology which will benefit people with disabilities, and all society.

Technology and its capacity to be used to create and expand employment opportunities for people with a disability, as well as deliver accessible and universally designed

materials is continually evolving. The federal government should be at the forefront of this movement through an efficient use of its information technology funding to purchase accessible information technology. We greatly appreciate the opportunity to submit this testimony, and stand ready to work with you and others in Congress, the Administration, and the private and public sector to ensure accessible technology is the first thought, and not an afterthought.



January 22, 2012

The Honorable Darrell Issa
House Oversight and Government Reform Committee
Rayburn House Office Building 2347
Washington, DC 20515

The Honorable Elijah E. Cummings
House Oversight and Government Reform Committee
Rayburn House Office Building 2235
Washington, DC 20515

RE: ICT Sector Trade Associations Comments on FITARA

Dear Chairman Issa and Ranking Member Cummings,

We are writing on behalf of TechAmerica, BSA |The Software Alliance, the Coalition for Government Procurement, the Information Technology Industry Council, and the U.S. Chamber of Commerce, organizations that collectively represent a diverse group of companies with deep expertise in the area of IT procurement. We applaud this committee for its tireless efforts to ensure that the government is procuring information technology efficiently and otherwise achieving the best value when it does so.

Our member companies agree with others that the government faces challenges in the way it manages its IT budgets and the operation of its existing networks, services, and systems. The solutions to these problems generally fall into three categories.

First, the government should ensure that it identifies and manages its existing IT infrastructure efficiently. The data center consolidation/optimization initiative and the decision to halt the development of new financial management systems in 2010 are important examples of hard decisions being made to further this effort. We believe that empowering agency CIOs with budgetary and hiring authority will support the development of better program management.

Second, the government should focus on the best value proposition associated with IT procurement. In constructing their IT acquisitions, agencies should continue to leverage full and open competition, as enunciated in the Competition in Contracting Act (CICA) of 1984. In this regard, agencies should ascertain the minimum needs of the particular mission being supported, fashion and weight requirements to ensure that the technology selected effectively meets those minimum needs, and make award decisions that achieve the overall best value for the government. In this way, the government will focus its acquisition process on mission success.

For example, some acquisitions will seek to procure for mission requirements that weight security or resiliency as more important that cost. Quantitative or adjectival weightings will allow agencies the ability to identify the value of those requirements so that, in making awards, they may assess the relative importance of those requirements, as compared to cost, in a rational manner, avoiding waste.

This approach avoids the hazard of picking technology "winners and losers" in a market that is quite dynamic. As then-U.S. CIO, Vivek Kundra, then-Administrator for Federal Procurement Policy, Dan Gordon, and U.S. Intellectual Property Coordinator, Victoria Espinel wrote in January 2011:

> *[A]s program, IT, acquisition, and other officials work together to develop requirements and plan acquisitions, they should follow technology neutral principles and practices. This means selecting suitable IT on a case-by-case basis to meet the particular operational needs of the agency by considering factors such as performance, cost, security, interoperability, ability to share or re-use, and availability of quality support.*
>
> http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/memotociostechnologyneutrality.pdf

Third, the government should leverage the use of commercial IT products and services to the maximum extent practicable. In so doing, the government should buy commercial items in a commercial manner wherever possible. If government-unique requirements are unnecessarily layered onto the procurement process, even commercial off-the-shelf (COTS) purchases can become more expensive for the government than they are for the private sector. In addition, to the extent that the government imposes unique terms, like licensing terms or other practices that are not common to the commercial market, it drives away potential market entrants, which shrinks the field of competition, mitigates downward pressure on prices, reduces innovative activity, and, as a result, undermines its ability to capture the panoply of benefits associated with buying commercial IT.

We believe that the solutions proposed in the discussion draft bill that has been circulated for comment require a full vetting to understand their impact and, assuming that their utility is demonstrated, their rational integration into the procurement system. We are fully supportive of the bill's provisions that would strengthen the role of agency CIOs and that would develop cross-government expertise in specialized areas of IT procurement. These provisions would advance the recommendations we have made above. At the same time, however, our member companies are concerned with provisions that would introduce new terms into the acquisition lexicon, treat IT as a new form of commodity, and concentrate buying power within a single centralized buying agency. In addition, it is not clear to us that these approaches would not undermine the ability of the agency CIOs to ensure that award determinations maximize the value to the government by supporting identified and weighted mission requirements. We are very concerned that there is not a complete alignment among government stakeholders on the problems being addressed with this proposed language, or whether the proposed process changes are superior to simply amending existing processes. Our member companies are concerned that, without further analysis in the context of the entire procurement system, the IT procurement provisions contained within the discussion draft risk unforeseen, deleterious effects over time, and as a result, may impede the ability of federal agencies to acquire and manage innovative IT solutions in efficient and cost-effective manner.

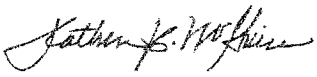
Although our member companies fully support the Committee's efforts to identify and address inefficiencies in the procurement process, we are concerned that the legislative proposal may be premature. Thus, we urge the Committee to utilize its oversight jurisdiction to promote a thorough examination of the issues being addressed prior to moving any legislation. In this regard, we note that, given the long hiatus between this proposed legislation and the last wholesale review of the

procurement system, the Committee may wish to consider sponsoring a multidisciplinary panel to review the entire acquisition process to identify key issues and solutions in a holistic fashion.

Thank you again for your efforts to focus on efficiency in the acquisition of information technologies and for the dialogue you have afforded on this proposal. Should you have any questions, please feel free to contact Trey Hodgkins of TechAmerica at thodgkins@techamerica.org.

Respectfully submitted,

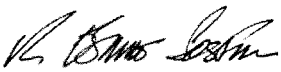
A.R. "Trey" Hodgkins, III
Senior Vice President, Global Public Sector
TechAmerica



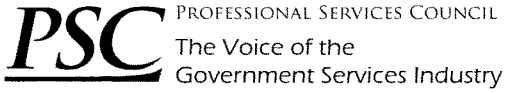
Katherine McGuire Vice President, Government Relations
BSA | The Software Alliance

Roger Waldron
President
The Coalition for Government Procurement

Andy Halataei
Director of Government Relations
Information Technology Industry Council



R. Bruce Josten
Executive Vice President, Government Affairs
U.S. Chamber of Commerce



STATEMENT FOR THE RECORD OF THE
PROFESSIONAL SERVICES COUNCIL

"Wasting Information Technology Dollars: How Can the Federal Government Reform its IT Investment Strategy?"

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES

JANUARY 22, 2013

4401 Wilson Boulevard, Suite 1110, Arlington, Virginia 22203 P: 703-875-8059 F: 703-875-8922 www.pscouncil.org

The Professional Services Council (PSC) commends the Committee on Oversight and Government Reform for holding this hearing and appreciates the opportunity to provide a written statement for the record. How the federal government invests taxpayers' dollars is always important, but as the nation faces fiscal uncertainty that will result in declining discretionary spending budgets, the need to ensure the government is investing wisely is now greater than ever. In light of these budget trends and anticipated austerity measures, it is essential that the government consider not only WHAT it invests in, but also HOW it invests its decreasing resources. Given the substantial government spending on information technology and the critical role it plays in agency missions, PSC is pleased that this committee, as well as the Senate Homeland Security and Governmental Affairs Committee and the administration, have undertaken initiatives to improve information technology management and acquisition.

For 40 years, PSC has been the leading national trade association of the government professional and technical services industry. PSC's more than 350 member companies represent small, medium, and large businesses that provide federal agencies with services of all kinds, including information technology, engineering, logistics, facilities management, operations and maintenance, consulting, international development, scientific, social, environmental services, and more. Together, the association's members employ hundreds of thousands of Americans in all 50 states.

Advances in technology have been occurring at a rapid pace in the private sector. Government leaders have been wise to recognize that such advances can improve how the government operates. Hence, the government has sought to make investments that allow federal agencies to tap into these advances to achieve their mission needs. Much of that reach into the private sector occurs through the federal acquisition process that enables the private sector to deliver cutting-edge, effective, and efficient solutions to meet important government challenges.

The current fiscal crisis is the biggest challenge facing the nation today. This budget environment will result in reduced funding across many different federal programs and activities. However, it also creates opportunities for leveraging private sector innovation, but only if the government makes sound policy decisions that foster the ability of the private sector to innovate for the government market and to readily make that innovation available to federal agencies. As the government makes tough decisions about <u>what</u> it must invest in, it must also be cognizant of <u>how</u> it does so. In terms of the federal acquisition process, this means buying smarter, buying more effectively and not focusing on short-term savings in lieu of more strategic, longer-term benefits and return on investment.

We have been pleased to work with this committee over the past several months on its IT review. As this committee continues to explore approaches to IT management and acquisition reform, PSC urges the committee to adhere to the following guiding principles. First, reforms must avoid a "one-size-fits-all" approach to IT acquisitions. Second, any acquisition policy changes should focus on expanding and preserving competition. Third, investments in the federal workforce are critical to ensuring success.

Avoid a One-Size-Fits-All Approach

Information technology solutions are comprised of a myriad of hardware, software, and services capabilities to meet an array of agency needs. While some solutions may require insignificant levels of technological development, others can be extremely complex. However, because of the broad definition of "information technology", it is important to avoid an approach that requires federal agencies to address vastly different solutions with the same management approach or acquisition processes. It is imperative that Congress, the administration, and companies providing information technology solutions to the government have a clear understanding of how the government categorizes and defines different segments of IT.

For example, the term "commodity IT" is being used by some to describe a subset of IT that could be targeted for strategic sourcing initiatives or purchased based on a preference for the cheapest offer. However, to date, the term "commodity IT" has not been defined consistently or adequately, which causes concern over proposals to mandate how such products or services are procured. Only after clear, widely adopted definitions of different types of information technology products, services, and solutions are implemented can there be an effective discussion about how best to procure these element. Policymakers must also not confuse "commodity IT" with "commercial IT." Many commercial IT solutions are by no means "commodities" since such solutions are often highly complex and require customization for individual users. Attempts to purchase complex commercial IT solutions based on the lowest-priced offer would increase program risk.

Expanding Competition

By far, competition is the single most effective means by which federal agencies can drive down their IT costs. Any information technology reform must focus on expanding the competitive ecosystem and preserving robust competition where it already exists. Reforms should closely examine unique government-imposed barriers that either drive competition out of the federal market or deter new entrants. Government-unique caps on contractor labor rates, excessive and unnecessary procedural, compliance or reporting requirements, and mandates for complex accounting systems are just some examples of such barriers to market entry and competition.

In addition, as IT solutions increase in complexity, so too should the government's focus on innovative and best value solutions. The private sector invests heavily in research and development on product and services in order to offer cutting edge solutions to both the commercial and government marketplaces. While such investments carry upfront costs, ultimately the innovation they provide and the realization of long-term cost savings are passed on to customers. The government's overreliance on lowest-priced solutions in turn forces companies to reduce their investments to identify innovative solutions. Therefore, when faced with challenges that require solutions using other than routine commodity purchasing, the government should rely on an acquisition plan based on a best value approach that permits a fair evaluation and trade off between price and technical capabilities.

It is also important for policymakers to understand that competition exists not just within the federal marketplace but also among the federal agencies and that certain approaches to IT acquisition reform could jeopardize this competition. Today, federal agencies manage a number of governmentwide acquisition contracts (GWACs) for information technology solutions. GWACs are available to all federal agencies and provide several options for agencies to turn to for their IT needs. The use of GWACs has led to useful competition among GWAC owners who seek to manage their contracts effectively, deliver better solutions to other government clients, and reduce administrative and total costs associated with managing the acquisition process.

Conversely, a proliferation of GWACs offering identical services results in duplication and inefficiency across the government and creates an environment that drives up bid and proposal and transaction costs for vendors. It is crucial to strike an appropriate balance between the over expansion of similar GWAC offerings and the elimination of valuable competition between them. Strategic sourcing initiatives should retain some, but not all, GWACs, even though they may offer similar products or services to preserve competition and provide additional cost savings. However, the greatest risk to preserving competition between GWACs could be posed by poorly structured strategic sourcing efforts.

Invest in the Federal IT Workforce

If investments in federal IT solutions are to be successful, the government must adopt a holistic approach to managing its workforce and must invest in the workforce to ensure it has the capacity and capability to successfully carry out IT acquisitions and programs. Too often, the acquisition process is siloed into distinct segments of program and acquisition office responsibilities. In recent years, government has begun to recognize that the "total" acquisition workforce comprises more than just procurement personnel and that program offices play a critical role in the acquisition process. PSC recommends the government continue its focus in

this area and encourage increased collaboration between program offices, acquisition personnel and the vendor community so that a unified "team" approach is taken to IT acquisitions.

In addition, the government must bolster its efforts to educate, empower, and reward its acquisition workforce. Training efforts should focus on developing cadres of IT acquisition experts that, when engaged in a truly collaborative effort, understand the technical challenges and potential solutions, the acquisition approaches that offer the best chance for success, and how desired outcomes are tied to individual agency missions. In addition, training of government personnel must include a greater focus on how industry approaches investments in innovation, risk, and federal contracting. Such training should enable government personnel to understand business risk and what factors are included in companies' bid/no bid decisions, among other factors. Workforce training should also engrain critical thinking skills and foster opportunities for cross functional development that is the norm in the best of the private sector. Today's acquisition training is increasingly centered on the "dos" and "don'ts" of the Federal Acquisition Regulation (FAR). Understanding these rules is important, but the FAR purposely offers ample flexibility for acquisition personnel to adopt acquisition approaches based on sound business principles that lead to successful outcomes. In today's environment of low-price and excessive oversight, such flexibility is too rarely used, let alone encouraged. Developing critical thinking skills, empowering acquisition and technology personnel to collaboratively use their best professional judgments, and freeing them from the mentality that mistakes are unacceptable, may be among the most important steps that the government can take on the acquisition reform front. Lastly, for successful IT programs, credit for the success should be shared among the entire program, including acquisition personnel, and should be appropriately recognized and rewarded.

Conclusion

PSC welcomes this committee's initiative and we are encouraged by emerging initiatives elsewhere in Congress and the administration to explore information technology management and acquisition reforms. Given the large investment that the federal government makes in IT, it is logical that savings can be achieved through better management and more effective procurement practices. PSC encourages these initiatives to focus on reforms within current models and to take steps to adequately define different segments of IT before implementing changes to how each segment should be acquired. PSC also urges approaches that maximize competition within the private sector and that retain multiple, but not excessive, federal agency contract vehicles. Lastly, we recommend a continued focus on federal workforce training and development. For reform initiatives to be effective, industry must be viewed as a

partner and key stakeholder throughout the process. PSC looks forward to continuing to work with this committee and others on IT reform initiatives throughout the 113th Congress.

Statement for the Record,

The Honorable Robert C. Cresanti,

Vice President, SAP America, Inc.

Former Under Secretary of Commerce for Technology (2006-2007)

Committee on Oversight and Government Reform

United States House of Representatives

Tuesday, January 22, 2013, 1:00 pm

Statement for the Record,
Robert C. Cresanti,
Vice President, SAP America, Inc.

Committee on Oversight and Government Reform
United States House of Representatives

Tuesday, January 22, 2013, 1:00 pm

Chairman Issa, Representative Cummings, and Members of the Committee, thank you for the opportunity to share our insights on how the federal government can reform its IT investment strategy. SAP is the world's leading provider of business software. Our mission is to help companies and governments run better, and our vision is to help the world run better. Over the last 40 years, we have been innovation leaders in core business processes such as financial and human resource management. Today we continue to lead a new wave of innovation enabled by technology solutions including business analytics, in-memory computing, cloud computing, and mobility.

In the United States, SAP helps thousands of organizations be more agile and competitive in the global economy. In particular, SAP Public Services serves more than 3,800 public sector agencies in nearly all 50 states, from local school districts to statewide programs to the largest federal defense and civilian agencies. Some of our best-known public sector customers are:

- The US Army, US Navy and Defense Logistics Agency;
- Civilian agencies including the Departments of Agriculture, Interior, State and Treasury, plus US Customs and Border Protection, NASA, NIH and CDC;
- Many state and local government agencies from Orange County Public Schools to the City of Houston to the Commonwealth of Pennsylvania; and
- Many higher-education institutions including MIT, the University of Kentucky, Johns Hopkins and Boston University.

Private Sector Technology Solutions Can Offer a Remedy to the Federal Government's Fiscal Crisis

Technology is evolving at a pace we have never seen before. As Congress and the White House continue to debate tax increases and spending cuts, technology solutions are available today that could address well-documented inefficiencies, including fraud, waste, and abuse in government programs. GAO, agency Inspectors General, and other watchdog groups have uncovered billions of dollars in such losses across the federal government. In 2012, the federal government reported more than $100 billion in improper payments from federal programs—$64 billion alone from the Medicare and Medicaid programs. On the

revenue side, the IRS reported a "tax gap" in uncollected taxes of $385 billion in 2006, the most recent year for which data is available.

The private sector can offer a host of technology solutions to many of the government's fiscal challenges. Software technologies that analyze huge volumes of data at the speed of light are in regular use in the private sector, but have not been implemented in the government. I believe passionately that IT is part of the solution, because we know from experience that IT enables:

- Faster, more intelligent decision-making;
- Turning insight into foresight;
- Higher performance;
- Meaningful efficiencies and cost savings; and
- Greater transparency and accountability, which are essential to efforts to reform, consolidate and course-correct large government programs.

Below are a few areas in which proven private sector technology solutions could curb federal program inefficiencies and combat fraud, waste, and abuse.

Business Analytics. The private sector regularly applies sophisticated business analytics to swiftly identify fraud and abuse in business operations. For example, many companies conduct real-time analysis and/or intermittent recovery audits of large-scale transactions to identify fraud, mistakes, or unanticipated shifts in demand. The Technology CEO Council estimates that new analytical techniques could increase the rate at which errors are identified in payments from federal programs such as Social Security and Medicare by 40%, generating an incremental $200 billion over 10 years.

"Big Data" Analytics. The term "Big Data" refers to the growing volume of electronic information produced in the course of daily life. The federal government alone has spent hundreds of millions of dollars collecting data that is often used once and stored forever. US companies store enough data every year to fill 10,000 Libraries of Congress. In response, industry has created powerful new tools for managing and analyzing all that data, in terms of both volume and speed. "Big Data" analytics now make it possible to integrate and analyze large stores of data in myriad ways to glean actionable information and inform decision-making. For example, the SAP HANA in-memory technology removes entire layers of hardware from the solution stack and allows organizations to analyze massive amounts of unstructured data thousands of times faster than old disk-based systems. SAP worked with one of the world's leading medical-research hospitals to reduce the amount of time needed to analyze the DNA in cancer tumors from 3 days to 2 minutes. Patients and their families receive diagnoses much faster and therapies can be better tailored to each patient's particular condition.

At the macro-level, comparative effectiveness research that analyzes patient characteristics, cost, and outcomes of treatment can reduce interventions that do more harm than good and identify cases in which a specific therapy should be prescribed. A 2011 report by the McKinsey Global Institute identifies the healthcare sector as ripe for greater deployment of big data analytics. Better management of this data could make a significant dent in national healthcare expenditures—saving up to $165 billion a year, by one estimate—and lead to better patient outcomes.

Mobility. Our growing ability to make data and applications accessible to anyone, anytime, on any device is critical at a time when there are 5 billion mobile phone subscribers in the world, and more than 9 billion mobile apps downloaded to date. When we marry the benefits of anytime, anywhere, any-device connectivity with access to business data and applications, including real-time analytics—we achieve enormous gains in efficiency and productivity. In a recent GovLoop survey, close to 60% of the federal managers who responded said their organizations would roll out between one and four new mobile applications in the next 12 months. Another 10% said they were likely to introduce five or more mobile apps in the coming year. The most commonly mentioned reasons for adopting mobility in government were:

- Reducing costs;
- Improving communications with constituents;
- Improving internal communications; and
- Linking data and business processes.

The mobility trend raises several challenges for Federal CIOs and IT managers. For instance, the GovLoop survey revealed that the majority of government organizations would only support one kind of mobile device for employees. In response, many federal agency CIOs are looking at ways to enable "BYOD," or "bring your own device"—an example of empowered consumers and constituents driving technology trends.

Cloud computing. Public and private sector organizations want flexible ways to deploy technology without having to maintain expensive, onsite infrastructure. They want fast, flexible, cost-effective IT services on demand. Cloud computing—the delivery of on-demand computing resources, from software applications to data centers, over the Internet on a pay-for-use basis—offers many opportunities for government to consolidate and streamline operations, just as it does for business. Another recent study released in conjunction with the TechAmerica Foundation determined that cloud computing could save US businesses as much as $625 billion over five years, much of which could be reinvested in new business opportunities and jobs. Likewise, cloud computing promises billions of dollars in savings across the federal government while improving mission performance and creating good jobs in our economy.

We commend the Administration on its "Cloud First" policy and its efforts to work with agencies and business to make it a success. However, agency IT officials remain concerned about the security of information migrated to the cloud, with federal IT security professionals surveyed in 2012 reporting that less than a third of agency infrastructure is outsourced to cloud vendors. A federal program to provide a standardized approach to security assessment, authentication, and monitoring for cloud services has been slow to get off the ground. Private sector software technologies offer a vigilant, multilayered approach to security using scalable technical platforms that have met certification under multiple US and international security accreditation programs. Fully embracing a transition to the cloud, coupled with the use of well-established private sector security solutions, could yield significant savings.

Strategic Sourcing. Federal agencies and departments with independent procurement processes buy more than $550 billion worth of goods and services each year. Unfortunately, the federal government's IT procurement processes often take longer than the technology upgrades. This is a serious problem at a time when technology innovation cycles are getting shorter and costs are going down. The nature of new technology solutions means that large, complex deployments are no longer the norm. The government's acquisition processes have to evolve to address this new reality. Strategic sourcing—a process that moves a company away from numerous individual procurements to a broader aggregate approach—would allow agencies to achieve material savings. While the federal government has an initiative to foster strategic sourcing across the government, most agencies are still not taking advantage of it. The Administration's "Shared First" strategy promotes the use of existing and new strategic sourcing methods where agencies can combine their buying power for similar IT needs. As of November 2012, federal agencies identified 60 initiatives, totaling $34 million in annual cost savings and cost avoidance, to migrate to Shared Services. These savings are undoubtedly just the tip of the iceberg.

Collaboration and Co-Innovation: A Case Study in Public-Private Partnership in the Delivery of IT Solutions

Collaboration and co-innovation are consistent success factors in the application of all of these technology solutions. A very large and growing portion of SAP's business occurs in collaboration with other companies and, most importantly, with our customers. New solutions must extend the investment made in legacy solutions and embrace co-innovation and teamwork. Co-innovation is a hallmark of many of the technological advances happening in the private sector. SAP, along with Intel, NetApp, Cisco, and VMware, created a Co-Innovation Lab (COIL) to facilitate project-based co-innovation with members, enhancing the capabilities of members' technology solutions through an integrated network of worldwide expertise and best-in-class technologies and platforms. For example, SAP has set up a Big Data Partner Council that will co-innovate to produce solutions uncovering use cases and architectures that leverage the SAP real-

time data platform and "Hadoop"—a term referring to the software framework enabling applications to work with huge amounts of data stored on various servers. Hadoop's functions allow existing data to be pulled from various places—since data is no longer centralized, but distributed in places using cloud technology—and analyzed in myriad ways. The council will include a cross-section of companies, including startups, hardware vendors, software providers and technology services organizations that will collaborate with SAP on select projects. Combining SAP's real-time data platform with cloud and Hadoop technology solutions will deliver unmatched capabilities in next-generation Big Data applications and analytics.

In the same vein, we have found that the fastest and most powerful results occur when industry and government co-innovate to bring new possibilities to life through technology. The rise and convergence of new technology solutions are helping IT users achieve quantum leaps in efficiency, speed, and accountability.

Recovery.gov. A recent example illustrates the power of collaboration and co-innovation in technology solutions in the public sector. Congress and the Obama Administration created the Recovery Accountability and Transparency Board in 2009 to help ensure transparency and accountability in federal stimulus spending. The Board faced several challenges, including:

- Determining how to manage huge quantities of evolving data from a variety of sources about stimulus grants, loans, vendors employed, and jobs;
- Presenting this information to the public in an understandable way on any Internet-access device; and
- Not spending millions of dollars that the board did not have to create an entirely new infrastructure and business process to manage all this data.

To address these challenges, the Recovery Board turned to SAP and several other companies to launch a website called Recovery.gov, which takes a huge amount of program data from a variety of sources, analyzes it, and presents it to the public in a user-friendly online dashboard. The industry consortium launched Recovery.gov in just 11 weeks. As part of that effort, we worked with Amazon to base the solution in the cloud, a move that took 22 days and made history as the first federal agency website to launch in the public cloud.

SAP also worked with Apple, Google, and other companies to make the data accessible on a variety of mobile devices. As a result, you can download the Recovery.gov app on your smartphone and immediately track spending in states and local communities. More recently, the Recovery Board leveraged these technologies to create FederalAccountability.gov, which allows agencies to evaluate the fraud risk of each applicant seeking government funds. This solution, called FAST ALERT, was deployed in about three months. It enables

federal agency personnel to analyze many large data sets in real-time and identify instances of waste, fraud and abuse before they happen.

The Recovery Board experience is a success story in enabling better stewardship of taxpayer dollars while enhancing the public trust. We drew on the best of many organizations, both private and public; we helped the government be more agile; and we leveraged the megatrends of cloud, mobility, and Big Data to innovate for the common good.

Additional examples. These are just a few more examples of how public sector agencies are harnessing these technology solutions:

- At **USDA,** as a result of standardizing all financial management and accounting functions—and adding the HANA in-memory database and advanced business analytics—we anticipate reducing the amount of time it takes the Farm Services Agency to run critical financial reports from minutes to seconds. In an organization that runs thousands of financial reports a year, you can imagine the savings in time and money that can be put to other uses.

- At the **State Department** and the **US Patent Office**, SAP solutions provide a clearer picture of agency costs to deliver services and enable the development of better fee structures and business processes to support agency operations.

- At the local government level, the **City of Boston** is implementing a performance-management solution that allows managers to assign and track performance measures, generate fast reports and online dashboards, and share results with colleagues, lawmakers and the public. As part of the deployment—which occurred in a matter of weeks, not years—SAP hosted an "Innovation Jam" bringing together a wide array of solution providers and users to develop testable prototypes within a 24-hour period.

Recommendations to Improve Federal IT Management

We applaud the work being done by the Federal CIO, Steven VanRoekel, and public servants across all levels of government who are working with industry to improve the way the public sector acquires and uses technology. Progress is being made, and we especially applaud efforts to move forward on cloud initiatives, shared services, and the use of mobile technology. Still, as the GAO and others have reported, there is much more work to be done.

A number of reform panels over the last quarter-century have offered good ideas about better management of federal IT investments, but many of these ideas still

need to be implemented. SAP was a proud participant in several recent reform panels, including the TechAmerica Foundation's "GTO-21" Commission, "CLOUD^2" Commission, and Big Data Commission. Each of these commissions outlined a series of common-sense IT policy changes that all sides can agree on. We urge the Committee to examine these commission reports and to adopt their recommendations, which include:

- **Focusing on faster, more agile, incremental IT development using commercial, off-the-shelf technology.** Incremental change is less costly and less likely to get out of control, delivering value in months, not years, and helping prevent vendor lock-in and escalating costs as government's needs evolve and grow. (GTO-21)

- **Fostering an open dialogue between the government and its private sector partners** and "co-innovation" of the type that is often seen in the private sector. Congress and OMB should make it clear that public-private dialogue and collaboration are to be encouraged, not feared. On the industry side, big government contractors can improve dialogue by including key subcontractors and vendors from the start. (GTO-21)

- Demonstrating flexibility in **adapting procurement models to allow agencies to acquire cloud services and solutions**. Congress and OMB should demonstrate flexibility in changing budget models to help agencies acquire cloud services and solutions. (CLOUD^2)

- Establishing policies and processes for **providing fiscal incentives, rewards, and support** for agencies as they take steps towards implementing cloud deployments. (CLOUD^2)

- Examining existing organizational and technical structures across the federal government to **find and remove barriers to greater Big Data uptake** and taking action to accelerate its use. (Big Data)

- At the agency level, **identifying key business or mission requirements that Big Data can address**, exploring data assets across the government ecosystem within the context of these business requirements, and assessing current capabilities and architecture against what is required to support Big Data goals. (Big Data)

Conclusion

Many of these recommendations can be implemented under existing legal and regulatory frameworks. Using existing authorities, the federal government can work with the private sector to embrace technology solutions that can cut

wasteful spending without passing a single budget cut. We can help increase revenues without touching the tax code. We can help prevent waste and fraud before they occur. We can dramatically improve the delivery of government services in a consumer-driven world. Technology solutions are available today that could save taxpayers billions of dollars and bolster the nation's economic outlook. SAP has achieved breakthroughs like this for companies and governments at every level in the US and worldwide, and other technology partners are bringing their own innovations to bear. The rapid progress of technology makes it possible for government to improve its performance while saving money and increasing accountability. SAP appreciates the opportunity to be a leader and partner in that effort.

○