AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CLOUD COMPUTING: BENEFITS AND RISKS OF MOVING FEDERAL IT INTO THE CLOUD

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT

AND THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

JULY 1, 2010

Serial No. 111–79

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

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

58–350 PDF WASHINGTON : 2010

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

EDOLPHUS TOWNS, New York, *Chairman*

PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MIKE QUIGLEY, Illinois
MARCY KAPTUR, Ohio
ELEANOR HOLMES NORTON, District of Columbia
PATRICK J. KENNEDY, Rhode Island
DANNY K. DAVIS, Illinois
CHRIS VAN HOLLEN, Maryland
HENRY CUELLAR, Texas
PAUL W. HODES, New Hampshire
CHRISTOPHER S. MURPHY, Connecticut
PETER WELCH, Vermont
BILL FOSTER, Illinois
JACKIE SPEIER, California
STEVE DRIEHAUS, Ohio
JUDY CHU, California

DARRELL E. ISSA, California
DAN BURTON, Indiana
JOHN L. MICA, Florida
JOHN J. DUNCAN, JR., Tennessee
MICHAEL R. TURNER, Ohio
LYNN A. WESTMORELAND, Georgia
PATRICK T. McHENRY, North Carolina
BRIAN P. BILBRAY, California
JIM JORDAN, Ohio
JEFF FLAKE, Arizona
JEFF FORTENBERRY, Nebraska
JASON CHAFFETZ, Utah
AARON SCHOCK, Illinois
BLAINE LUETKEMEYER, Missouri
ANH 'JOSEPH" CAO, Louisiana
BILL SHUSTER, Pennsylvania

RON STROMAN, *Staff Director*
MICHAEL MCCARTHY, *Deputy Staff Director*
CARLA HULTBERG, *Chief Clerk*
LARRY BRADY, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT

DIANE E. WATSON, California, *Chairman*

PAUL E. KANJORSKI, Pennsylvania
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
HENRY CUELLAR, Texas
JACKIE SPEIER, California
PAUL W. HODES, New Hampshire
CHRISTOPHER S. MURPHY, Connecticut
MIKE QUIGLEY, Illinois

BRIAN P. BILBRAY, California
AARON SCHOCK, Illinois
JOHN J. DUNCAN, JR., Tennessee
JEFF FLAKE, Arizona
BLAINE LUETKEMEYER, Missouri

BERT HAMMOND, *Staff Director*

CONTENTS

	Page
Hearing held on July 1, 2010	1
Statement of:	
Charney, Scott, corporate vice president, trustworthy computing, Microsoft Corp.; Daniel Burton, senior vice president, global public policy, Salesforce.com; Mike Bradshaw, director, Google Federal, Google Inc.; Nick Combs, chief technology officer, EMC Federal; and Gregory Ganger, professor, electrical and computer engineering, director, Parallel Data Lab, Carnegie Mellon University	81
Burton, Daniel	96
Bradshaw, Mike	108
Charney, Scott	81
Combs, Nick	117
Ganger, Gregory	128
Kundra, Vivek, Federal Chief Information Officer, Administrator for e-Government and Information Technology, Office of Management and Budget; David McClure, Associate Administrator, Office of Citizen Services and Innovative Technologies, General Services Administration; Cita Furlani, Director, Information Technology Laboratory, National Institute of Standards and Technology; and Gregory Wilshusen, Director, Information Security Issues, Government Accountability Office	10
Furlani, Cita	37
Kundra, Vivek	10
McClure, David	23
Wilshusen, Gregory	49
Letters, statements, etc., submitted for the record by:	
Bradshaw, Mike, director, Google Federal, Google Inc., prepared statement of	110
Burton, Daniel, senior vice president, global public policy, Salesforce.com, prepared statement of	98
Charney, Scott, corporate vice president, trustworthy computing, Microsoft Corp., prepared statement of	84
Combs, Nick, chief technology officer, EMC Federal, prepared statement of	119
Connolly, Hon. Gerald E., a Representative in Congress from the State of Virginia, prepared statement of	151
Furlani, Cita, Director, Information Technology Laboratory, National Institute of Standards and Technology, prepared statement of	39
Ganger, Gregory, professor, electrical and computer engineering, director, Parallel Data Lab, Carnegie Mellon University, prepared statement of	130
Issa, Hon. Darrell E., a Representative in Congress from the State of California, prepared statement of	8
Kundra, Vivek, Federal Chief Information Officer, Administrator for e-Government and Information Technology, Office of Management and Budget, prepared statement of	13
McClure, David, Associate Administrator, Office of Citizen Services and Innovative Technologies, General Services Administration, prepared statement of	26
Towns, Chairman Edolphus, a Representative in Congress from the State of New York, prepared statement of	3
Watson, Hon. Diane E., a Representative in Congress from the State of California, prepared statement of	72
Wilshusen, Gregory, Director, Information Security Issues, Government Accountability Office, prepared statement of	51

CLOUD COMPUTING: BENEFITS AND RISKS OF MOVING FEDERAL IT INTO THE CLOUD

THURSDAY, JULY 1, 2010

HOUSE OF REPRESENTATIVES, COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM, JOINT WITH THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT,

Washington, DC.

The committee and subcommittee met, pursuant to notice, at 10 a.m., in room 2157, Rayburn House Office Building, Hon. Edolphus Towns (chairman of the committee) presiding.

Present from the Committee on Oversight and Government Reform: Representatives Towns, Watson, Cummings, Connolly, Quigley, Cuellar, Murphy, Foster, Chu, Issa, Bilbray, Jordan, Chaffetz, and Luetkemeyer.

Present from the Subcommittee on Government Management, Organization, and Procurement: Representatives Watson, Connolly, Cuellar, Murphy, Quigley, Bilbray, and Luetkemeyer.

Staff present: Krista Boyd, counsel; Linda Good, deputy chief clerk; Velginy Hernandez, press assistant; Adam Hodge, deputy press secretary; Carla Hultberg, chief clerk; Marc Johnson and Ophelia Rivas, assistant clerks; Mike McCarthy, deputy staff director; Amy Miller and Gerri Willis, special assistants; Jenny Rosenberg, director of communications; Leneal Scott, IT specialist; Mark Stephenson, senior policy advisor; Lawrence Brady, minority staff director; John Cuaderes, minority deputy staff director; Jennifer Safavian, minority chief counsel for oversight and investigations; Adam Fromm, minority chief clerk and Member liaison; Kurt Bardella, minority press secretary; Benjamin Cole and Seamus Kraft, minority deputy press secretaries; Justin LoFranco, minority press assistant and clerk; Christopher Hixon, minority senior counsel; Hudson Hollister, minority counsel; and John Ohly, minority professional staff member.

Chairman TOWNS. The meeting will come to order.

Thank you for being here.

The purpose of today's hearing is to examine the benefits and risks of cloud computing for the Federal Government. At the most basic level, cloud computing is Web-based computing whereby computing resources are shared and accessible over the Internet on demand. In this way, cloud computing is like most utility services.

Before the electric grid was developed, business owners who wanted to use machinery also needed to produce enough energy to run that machinery. That meant investing heavily to build and maintain a power source. The electric grid revolutionized the coun-

try by centralizing the resource and allowing businesses to simply purchase electricity.

Cloud computing promises the same for computing power. Instead of building and maintaining an entire IT system in-house, businesses can purchase computing power and tap into that resource over the Internet.

Cloud computing is a very real technology that the Federal Government has already begun to embrace. The Federal Cloud Computing Initiative and an online cloud computing storefront were launched in September 2009.

I have read that the Government-wide implementation of cloud computing will be a decade-long journey. It is the job of this committee to ensure that journey is well thought out, that the benefits and risks are fully examined, and that there are comprehensive plans in place to ensure that we do this the right way, the first time around.

The shift to cloud computing offers the Federal Government tremendous promise, but it is not without risk. The balance between risk and reward is an important one and I hope to get a better understanding of that balance today.

It is clear to me that security and privacy are real concerns. Our natural impulse is to hold the things we value close to us, but cloud computing requires entrusting data to others. The law's current focus on the physical location of data also presents unique privacy and legal challenges.

A major benefit of cloud computing is the potential for significant cost savings. It makes sense: cloud computing allows agencies to pool resources and pay only for the computing power that they actually use.

I look forward to today's hearing, to a thorough examination of the Federal Cloud Computing Initiative, and to addressing the emerging legal and policy issues that Federal cloud computing presents. I want to thank all of our witnesses for appearing here today and I really look forward to your testimony.

At this time, I would like to yield 5 minutes to the ranking member of the committee, the gentleman from California, Congressman Issa.

[The prepared statement of Chairman Edolphus Towns follows:]

HOUSE COMMITTEE ON
OVERSIGHT & GOVERNMENT REFORM

CHAIRMAN EDOLPHUS TOWNS

OPENING STATEMENT

"Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud"

July 1, 2010

Good morning. Thank you all for being here today.

The purpose of today's hearing is to examine the benefits and risks of cloud computing for the federal government. At the most basic level, cloud computing is web-based computing whereby computing resources are shared and accessible over the Internet on demand. In this way, cloud computing is like most utility services.

Before the electric grid was developed, business owners who wanted to use machinery also needed to produce enough energy to run that machinery. That meant investing heavily to build and maintain a power source. The electric grid revolutionized the country by centralizing the resource and allowing businesses to simply purchase electricity.

Cloud computing promises the same for computing power. Instead of building and maintaining an entire IT system in house, businesses can purchase computing power and tap into that resource over the Internet.

While the concept might sound like something out of a science fiction novel, when you think about it, most Americans already use some form of cloud computing. I'm sure most of the people in this room have used some web-based email service, social networking site like Facebook or Twitter, or photo and video-sharing site like Flickr and YouTube. Indeed, many of us in Congress are using those tools to communicate with our constituents.

Cloud computing is a very real technology that the federal government has already begun to embrace. The Federal Cloud Computing Initiative and an online cloud computing storefront were launched in September 2009.

I've read that the government-wide implementation of cloud computing will be a decade-long journey. It's the job of this Committee to ensure that journey is well thought out, that the benefits and risks are fully examined, and that there are comprehensive plans in place to ensure that we do this the right way, the first time.

In the same way that common standards improved efficiency and safety for the electric grid, standards are needed for cloud computing to ensure security, promote interoperability, and support data portability. I

believe strongly that doing this right the first time will require strong public-private collaboration, particularly on standards development.

The shift to cloud computing offers the federal government tremendous promise, but it is not without risk. The balance between risk and reward is an important one and I hope to get a better understanding of that balance today.

It is clear to me that security and privacy are real concerns. Our natural impulse is to hold the things we value close to us, but cloud computing requires entrusting data to others. The law's current focus on the physical location of data also presents unique privacy and legal challenges.

A major benefit of cloud computing is the potential for significant cost savings. It makes sense – cloud computing allows agencies to pool resources and pay only for the computing power that they actually use. Cost savings estimates vary widely from 25-99% of IT operating costs. I'd like to know why those figures vary so widely and what can we really expect to save?

I look forward to today's hearing, to a thorough examination of the Federal Cloud Computing Initiative, and to addressing the emerging legal and policy issues that federal cloud computing presents. I want to thank all of our witnesses for appearing here today and I look forward to hearing their testimony.

Mr. ISSA. Thank you, Mr. Chairman. I too am looking forward to this important hearing. I too am expecting that if you and I are still serving here on the dais in 10 years, we will still be holding hearings on some portions of this.

I base that on a hearing we had just a week ago, in which we recognized that half way through a contract that saved the American people, through its government, huge amounts of money if we implemented new contracts the GSA had negotiated for telecommunications, ones that offered high Internet speeds, better telecommunication, better redundancy, and new features, were not implemented, even though they would save money, because, of course, bureaucrats move slowly.

So today, as we hear about cost savings, I will not yawn. I will not pretend to be disinterested. But I will not be a true believer from the dais that cost savings will drive this move to cloud computing. I will be particularly interested in details as to how companies believe that they can implement guaranteed security in a cloud environment.

As all of you know, we do not guarantee security; we have breaches every week, every month, sometimes every day in government. And even here in the Capitol, the Chinese mainland government has repeatedly breached and taken confidential information from the House. They regularly are able to penetrate our security.

So as we look to the Internet through a Web browser, we need to do better, not just as good as we are doing here today.

Often said, history does not always repeat itself, but it very often rhymes. Today, as we start looking at cloud computing, at my age, I find that it is rhyming rather humorously. When I began my career, we were still using NCR–500's. We would put as many of those card reading computers as close as we could to the source, and they would run the cards back and forth, distributing to us punching machines so that we could prepare our jobs and then go to that massive and expensive product and have it run.

By the time I was a young officer, I was running a DEC facility with PDP–11/45s and DEC–10's, wonderful computers that could multitask, that could have multiple clients at one time, that could load-share and balance, that could distribute priorities of who needed what and when. But yet it was still sending to the big machine and the machine deciding what we would get when.

As we look at the cloud, there is no question that we can look at the cloud as thousands, millions of computing devices available to us to load-share. Or, in the rhyming way, we can look at it as simply dejâ vu all over again. In fact, the cloud, in any configuration, is nothing but a return to those DEC–10 machines. You can have different sizes; you can have dual processors; you can share multiple across. We once had 14 PDP–11s all deciding, with one central arbitrator, who got what load when, for what computing in order to keep us in real time.

All of this has been done before, but not nearly at the scale it is being done. And, in my case, all of my previous history in the military was a closed system, an extremely closed system. Today we are going to talk about an open system, one in which encryption over a public line is our guarantee, and our only guarantee, that

the data flowing back and forth will remain in the hands of those that it came from and is intended to go back to.

I look forward to hearing how we can, and should, implement both public and, often, private cloud computing systems; how the Government can, once and for all, recognize that owning a computer is not as important as owning computer power time, something that, 30 or 40 years ago, everybody understood that owning time on a computer was what you did, not in fact owning a computer.

But weaning the Federal Government off of the idea that they have endless arrays of PCs and servers all within a server room that they can walk to will take time and will take initiative by this committee. So because this is a Government-wide problem, we believe, the chairman and I, that this is a government oversight solution that must be pushed through day after day, Congress after Congress.

With that, Mr. Chairman, I yield back the balance of my time and thank you for this hearing.

[The prepared statement of Hon. Darrell E. Issa follows:]

EDOLPHUS TOWNS, NEW YORK
CHAIRMAN

DARRELL E. ISSA, CALIFORNIA
RANKING MINORITY MEMBER

ONE HUNDRED ELEVENTH 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) 225–5051
Minority (202) 225–5074

Statement of Rep. Darrell Issa, Ranking Member

"Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud"

July 1, 2010

Thank you, Mr. Chairman. I, too, am looking forward to this important hearing. I also expect that if you and I are still serving here on the dais in ten years we will still be holding hearings on some portions of this issue.

I cannot help but think about a hearing we had several weeks ago where we learned that a telecommunications contract nearly a decade old – and that was supposed to save the American people millions of dollars – was lagging far behind projected implementation. The new telecommunications system was supposed to offer faster, smarter, and more cost-efficient services, but of course those aspirations have not been realized.

Why? Because as we all know, bureaucracies move slowly.

So today when we hear about cost savings, I will not just roll my eyes and dismiss it as altogether impossible for the federal government to actually implement cost-saving technologies in a cost-efficient way. I am, however, doubtful that cost-savings are what will actually drive the implementation of cloud computing technologies.

I am particularly interested in learning how companies believe they can implement guaranteed security in a cloud environment. Experience informs us that we cannot even guarantee information security under the existing system of in house, firewalled servers using the most sophisticated form of data encryption. Almost every day in government, we have an information security breach. Our foreign competitors are daily seeking confidential information to give them an edge over the American economy. Even worse, our enemies are relentlessly barraging our systems, testing their weaknesses and exploiting our vulnerabilities. I look forward to hearing how cloud computing promises a more secure

platform to protect our nation's most sensitive and classified information from cyber terrorism.

Mr. Chairman, I must confess that I sense a bit of déjà vu today. When I began my career, we were still using MPR500s. We would put as many of those card-reading computers as close to the source as we could, and it would run the cards back and forth, distributing to us punching machines so we could prepare our jobs.

By the time I was a young Army officer, I was running a deck facility with PC1145s and Deck10. It was revolutionary for one computer to multi-task, and to serve multiple clients simultaneously. They could load share, and balance, and distribute priorities between users.

As we look at the cloud, there is no question about our capacity to serve thousands – even millions – of computing devices and load share. Ironically, the cloud in any configuration is simply a return to those Deck10 machines, though at a much more sophisticated and advanced level of information exchange. We are simply attempting to do the same thing we did when we first began implementing computers in both the federal government and in the private sector, only at a much greater scale.

There is one difference, however, between how we used to use load-sharing systems and how we are considering the use of cloud computing. Before, every system was a closed system. Today, we are talking about an open system in which encryption over a public line is our only guarantee of data security.

I look forward to hearing to hearing how we could implement both public and private cloud computing systems and how the government can, once and for all, recognize that owning a computer is not as important as owning computer power time. In fact, thirty or forty years ago, everyone understood.

We must wean the federal government off the idea that they have – or need – endless arrays of PCs and servers all within a server room than they can just walk down the hall to access. That effort will take time and unyielding initiative by this committee. And because this is a government-wide problem, we must only consider government-wide solutions. The solution will require a serious push -- day after day, month after month, year after year, and Congress after Congress.

With that, Mr. Chairman, I yield back the balance of my time and thank you for holding this important hearing.

###

Chairman TOWNS. I would like to thank the gentleman from California for his statement.

At this time, we would like to ask you to stand so I can swear you in.

Raise your right hands.

[Witnesses sworn.]

Chairman TOWNS. You may be seated.

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

Let me begin with you, Mr. Kundra. As you know, you have 5 minutes and, of course, at the end of 4 minutes the yellow light will come on, which means caution, and then 1 minute after that the red light will come on, and every place in the United States of America that means stop. So, Mr. Kundra, will you start?

STATEMENTS OF VIVEK KUNDRA, FEDERAL CHIEF INFORMATION OFFICER, ADMINISTRATOR FOR E-GOVERNMENT AND INFORMATION TECHNOLOGY, OFFICE OF MANAGEMENT AND BUDGET; DAVID McCLURE, ASSOCIATE ADMINISTRATOR, OFFICE OF CITIZEN SERVICES AND INNOVATIVE TECHNOLOGIES, GENERAL SERVICES ADMINISTRATION; CITA FURLANI, DIRECTOR, INFORMATION TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY; AND GREGORY WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

STATEMENT OF VIVEK KUNDRA

Mr. KUNDRA. Good morning, Chairman Towns, Ranking Member Issa. Thank you for the opportunity to testify today on cloud computing and the Federal Government's approach toward cloud computing. What I would like to do is draw your attention to the first slide that you see before you.

Earlier this week, the Obama administration focused on addressing some of the most persistent and structural issues we have faced as an administration when it comes to information technology. The U.S. Government is the largest buyer of IT on the planet. We spend approximately $80 billion annually on information technology systems.

Yet, as you see on this slide, I want to point to one example. The Department of Defense spent 12 years and $1 billion on deploying an integrated human resource system which ended up failing, and Secretary Gates said, essentially, that what we ended up with was an acronym that nobody could pronounce. Therefore, earlier this week, on Monday, we announced aggressive steps in terms of how we are going to confront some of these issues.

June of last year we deployed an IT Dashboard that shines light on every aspect of Government operations when it comes to information technology spending with literally the picture of every agency CIR right next to the IT investment that they are responsible for so the American people could see where they were in terms of cost, schedule, and whether they are meeting performance targets or not.

What we are doing is approaching this problem in three ways: No. 1, effective immediately, we are going to be reviewing the most troubled IT investments across the Federal Government as part of the fiscal year 2012 budget process and make decisions around where we need to halt, terminate, or turn around these investments; No. 2, effective immediately, we have halted future task orders on financial systems across the Federal Government for the CFO Act agencies to make sure that we are not throwing good money after bad money; and, No. 3, in the next 120 days, we are focused on making sure that we address some of the structural issues, understand what is going on, why, for the last 50 years, as we have tried to address some of these persistent problems, we continue to have spectacular failures in Federal IT.

On slide 2, what I want to draw your attention to is what the Federal Government has been focused on. Unfortunately, the number of data centers in the U.S. Government has gone from 432 to over 1,100 in a decade, while in the private sector IBM went from 235 data centers to 12. That is not sustainable in the long-term as we continue to plow capital in data center after data center.

The next slide shows how other industries have applied these innovations around utility models. As you pointed out, Chairman Towns, we have seen this happen in the electricity space, where every home used to have to use candles to light their homes, to where now they just plug into the grid. Or, with water, every home used to have to essentially have a well to get water; now what we see is the ability to turn on and off a tap to consume those resources.

That is one of the reasons we are moving toward the cloud environment. It is not just about cost, it is also about making sure that we are providing better service so CIOS are focused not on investing on yet another data center, but actually providing better services.

I want to point you to the next slide, which is a tale of two cities. In the first story, how the Government deployed an IT system versus how a private sector company deployed an IT system. When we deployed a Cash for Clunkers program, we deployed the traditional approach to IT, and as demand grew, the system was unstable and continued to crash over a 30-day period, and we had to literally reengineer the solution, buy new hardware and configure it.

Yet, a company called Animoto faced similar problem but was using cloud technology. With 250,000 new users enrolled over a 3-day period, they were able to scale from 50 virtual machines to over 4,000 virtual machines and supported, at peak times, 20,000 new users an hour.

What I want to point to in the next slide is what the Government has done so far in terms of making sure that we are focused on some of the security issues that you have raised; making sure that we are addressing some of the standards that we need to promulgate as a function of interoperability, data portability, and security; and procurement. And Dave McClure will talk about the procurement strategy and Cita Furlani will talk about our standards activities. But this work has been underway since April of last year.

I want to leave you with a closing slide that you see on slide 7. What you see on the left is a cave. This is where most of the Fed-

eral Government's HR records are. What you see on the right is what the American people expect from their Government. The culture in the Government historically has been there is a form for that, and the American people have to wait in line, hold on the phone, or they actually have to come in and submit these complicated forms.

Yet, in the private sector, what we have seen is innovation. And what we are trying to do is close that gap by making sure that we are responsibly and safely moving to a cloud environment.

Thank you for the opportunity to testify, and I look forward to your questions.

[The prepared statement of Mr. Kundra follows:]

STATEMENT OF VIVEK KUNDRA
FEDERAL CHIEF INFORMATION OFFICER,
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND
INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET

BEFORE THE
HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT

July 1, 2010

"Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud"

Good morning Chairman Towns, Chairwoman Watson and members of the Committee. Thank you for the opportunity to testify on "Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud."

Information technology (IT) has transformed how the private sector operates and has revolutionized the efficiency, convenience, and effectiveness with which it serves its customers. In our everyday lives, we can track the status of a shipment, buy goods and services, make travel, hotel and restaurant reservations, and collaborate with friends and colleagues – all online, anytime and anywhere.

Yet, when it comes to dealing with our government, we have to stand in line, hold on the phone, or mail in a paper form. The Federal Government has largely missed out on the transformation in the use of IT due to poor management of its technology investments. Government IT projects all too often cost millions of dollars more than they should, take years longer than necessary to deploy, and deliver technologies that are obsolete by the time they are completed.

To address these persistent problems, in June 2009 we launched the IT Dashboard, which allows the American people to monitor IT investments across the Federal government and shines light into government operations. However, it is not enough to simply shine a light on IT programs and hope that results will follow.

Building on the foundation of the dashboard, we launched TechStat Accountability Sessions in January 2010. A TechStat accountability session is a face-to-face, evidence-based review of an IT program with OMB and agency leadership. TechStat sessions enable the government to turnaround, halt or terminate IT investments that do not produce dividends for the American people.

Earlier this week, we announced three actions in the Administration's continuing effort to reform Federal IT.

- First, we are undertaking detailed reviews of troubled IT projects across the Federal Government. Where serious problems are identified, actions will be taken to correct the problems, including potential adjustments to Fiscal Year 2012 agency budgets.
- Second, we directed executive departments and agencies to refrain from awarding new task orders or contracts for financial system modernization projects – an area of persistent problems – pending review and approval of project improvement plans by OMB. Across the government, there are approximately 30 financial systems projects that are affected by this policy. The total cost expended on these projects is anticipated to be $20 billion over the life of these projects, with an approximate annual spend of $3 billion. OMB expects this new process to result in a significant reduction in these amounts.
- Third, we will develop recommendations for improving the Federal Government's IT procurement and management practices within 120 days and in consultation with agencies. These recommendations will help address the root causes of problems plaguing Federal IT projects by strengthening existing policies and procedures where appropriate, eliminating outdated and cumbersome rules, and focusing on proven best practices from inside and outside the Federal Government.

These actions reflect the Administration's ongoing commitment to closing the IT gap between the public and private sectors and leveraging the power of technology to improve the efficiency of government and deliver better services to the American people. The President has ordered a three year freeze in non-defense and national security programs in the FY 2011 budget and has ordered some agencies to reduce their 2012 budget request by five percent. To do more with less, we need game-changing technologies.

Cloud computing is one such technology.

Benefits of the Cloud

As the world's largest consumer of information technology, the Federal Government spends approximately $80 billion annually on more than 12,000 systems at major agencies.[1] Fragmentation of systems, poor project execution, and the drag of legacy technologies in the Federal Government have presented barriers to achieving the productivity and performance gains that can be found in the private sector's more effective use of technology. For example, over the past decade, while the private sector was consolidating data centers, the Federal Government increased its data centers from 432 to over 1,100, leading to redundant investment, reduced energy efficiency, and poor service delivery.

Cloud computing has the potential to greatly reduce inefficiencies, increase data center efficiency and utilization rates, and lower operating costs. It is a model for delivering computing resources – such as networks, servers, storage, or software applications.

There was a time when every household, town, farm or village had its own water well. Today, shared public utilities give us access to clean water by simply turning on the tap; cloud computing works in a similar fashion. Just like water from the tap in your kitchen, cloud computing services can be turned on or off quickly as needed. Like at the water company, there is a team of dedicated professionals making sure the service provided is safe, secure and available on a 24/7 basis. When the tap isn't on, not only are you saving water, but you aren't paying for resources you don't currently need.

The National Institute of Standards and Technology (NIST) defines cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[2]

Many organizations in the private sector and at state and local governments are already using cloud computing technologies to streamline their operations and improve delivery of services to their customers.

---

[1] http://www.whitehouse.gov/omb/assets/egov_docs/FY09_FISMA.pdf (Appendix 1, Table 1)
[2] http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc; see Appendix for further details

In the private sector, for example, a web-based multimedia production company used the cloud to allow anyone with access to an Internet connection to create their own fully customized, professional-quality, "TV-like" videos. Consumers upload audio, photos, and videos to the web which are then analyzed and processed with advanced post-production techniques as used in television and film. The resulting videos can then be shared with friends and family across the world. The cloud allowed for a rapid response when demand jumped from 25,000 users to over 250,000 users in three days, eventually reaching a peak rate of 20,000 new customers every *hour*. Because of the cloud, the company was able to scale from 50 to 4,000 virtual machines in three days to support increased demand on a real-time basis.[3]

In contrast, the Car Allowance and Rebate System (CARS, more commonly known as "Cash-For-Clunkers"), failed under peak loads. To process the anticipated 250,000 transactions, the National Highway Traffic Safety Administration (NHTSA) deployed a customized commercial application hosted in a traditional data center environment on June 19, 2009. When dealer registrations began on July 24, 2009, demand far outstripped initial projections, and within three days, the system was overwhelmed, leading to numerous unplanned outages and service disruptions. Ultimately, approximately 690,000 CARS transactions were processed. However, lacking the ability to scale rapidly, system stability was not achieved until August 28, over a month after registrations started coming in.[4]

By using cloud computing services, the Federal Government can gain access to powerful technology resources faster and at lower costs. Ultimately, this will allow the Government to better serve the American people and focus on mission-critical tasks instead of on purchasing, configuring and maintaining redundant infrastructure.

Moving to the Cloud

We recognize that the shift to cloud computing will not take place overnight. While cloud computing has the potential to provide tremendous benefits, we are still in the early stages of a decade-long journey. As we move to the cloud, we must be vigilant in our efforts to ensure the security of government information, protect the privacy of our citizens, and safeguard our national security interests. The American people must be confident that their information is safe in the cloud. Therefore, we are being deliberate in making sure the Federal Government's journey to the cloud fully considers the advantages and risks associated with cloud

[3] http://blog.rightscale.com/2008/04/23/animoto-facebook-scale-up/
[4] http://www.cars.gov/files/official-information/CARS-Report-to-Congress.pdf, pg.10-12

technologies, by defining standards and security requirements. The following represent key milestones in the Administration's deliberate approach:

- **April 2009 –** Cloud Computing Program Management Office (PMO) established at the General Services Administration (GSA). The Cloud Computing PMO is responsible for coordinating the Federal Government's cloud computing efforts in key areas, such as security, standards, acquisition, and is developing the governance approaches necessary to effectively engage with Federal agencies for the safe and secure adoption of cloud technology.
- **May 2009 –** Industry Summit conducted with the private sector to explore the risks and benefits associated with cloud computing.
- **November 2009 –** Security and Standards Working Groups convened to better enable agencies to collaborate on these topics. The Security Working Group serves as the central organization for identifying, aggregating, and disseminating security and standards concerns, solutions, and processes impacting the implementation and adoption of available cloud computing. The Standards Working Group is charged with establishing a framework and roadmap to drive standards to facilitate interoperability, portability, and management for cloud computing services.
- **February 2010 –** Initiated development of a government-wide security certification and accreditation process for cloud computing solutions.
- **May 2010 –** "Cloud Computing Forum and Workshop" hosted by NIST to initiate engagement with industry to collaboratively develop standards and explore solutions for cloud interoperability, portability, and security. Attendees included a broad range of participants from standards bodies, state and local governments, academia, and leading security, hardware, software, and cloud services providers.

Security & Privacy

As we increasingly leverage technology to deliver services to the American people, we cannot lose sight of the fact that we operate in an inter-connected environment, in which new threats arise daily. To realize the full benefits of the digital revolution, the American people must have confidence that sensitive information is not compromised, their communications with the government are secure, their privacy and civil liberties are protected, and that the Federal infrastructure is not compromised.

To advance the security posture of the Federal Government, the Administration is taking a number of actions. Shifting from an outdated, compliance-based process to a performance-

based approach and automated tools will enable agencies to continuously monitor security-related information from across the enterprise in a manageable and actionable way. Efforts such as the National Cybersecurity Education Initiative will improve the effectiveness of the cybersecurity workforce. Developing an integrated plan for research and development will encourage innovation in game-changing technologies in coordination with industry and academia.

Cloud computing, like any technology, has inherent benefits and risks. Some of the challenges we face as the government moves towards greater adoption of cloud computing include ensuring clarity of data ownership, meeting the requirements of privacy regulations such as those for health records, data recovery following a disaster or cyber attack, long-term storage, records management and data viability. Additionally, vendor dependence, sharing of computing resources, and concerns related to multi-tenancy are all risks often associated with cloud computing. There is a common misperception that these are all new risks, brought on by the use of third-party resources to operate government systems.

However, the Federal Government currently uses a wide array of external providers and shared services to support its employees and to deliver services to the American people. From public telecommunications networks to agency data centers, Federal agencies make use of commercially operated facilities and networks every day. And many agencies currently make use of systems that are contractor owned and/or operated on behalf of the Federal Government. In fact, agencies reported the use of 4,186 contractor systems in FY 2009.[5]

The adoption of new technologies in the Federal government takes place within a framework of risk management at the Department and Agency level. The Federal Information Security Management Act of 2002 (FISMA) requires agency heads to implement security controls commensurate with risk, after a cost-benefit analysis. Once a possible business use is identified for a given technology, agency Chief Information Officers and Chief Information Security Officers assess risk using a framework of Federal laws and guidance that includes FISMA, Federal Information Processing Standards (FIPS), and NIST guidance as reflected in NIST Special Publications (SP) 800 series.

[5] http://www.whitehouse.gov/omb/assets/egov_docs/FY09_FISMA.pdf; Appendix 1, Table 2

In April 2010, OMB issued memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*[6], which instructs agencies to develop automated risk models and apply them to the vulnerabilities and threats identified by security management tools. In the case of cloud computing, we expect these risk models to vary based on the specific cloud deployment model used (e.g., private cloud versus public cloud). Agencies will incorporate these risk models into their business decision-making processes and use them to inform the development of comprehensive agency risk management plans that address issues such as continuity of service, quality control, and long-term preservation of data to support Federal records requirements.

While the decisions to use cloud computing are made at the agency level by agency Chief Information Officers and Chief Information Security Officers, the potential benefits of cloud computing won't be fully realized if every agency independently reviews and certifies solutions. The current fragmented certification process – where agencies independently conduct certifications and accreditations on the same products – is redundant, and adds both time and cost to an already complex procurement process.

This is why we directed NIST to establish a technical process for centralized certification to provide common security management services to Federal agencies. The process supports the development of common security requirements and performs authorization and continuous monitoring services for government-wide use, enabling Federal agencies to rapidly, securely and cost-effectively procure technologies. Agencies can realize these benefits by leveraging the security authorizations provided through a joint authorization board. The board will provide both initial and ongoing assessment of risk on behalf of the government as systems are continuously monitored throughout their lifecycle.

Additionally, GSA is working to streamline acquisition processes for cloud computing technologies. The goal is to provide an efficient acquisition process that minimizes redundancy, delay, and administrative burden and supports agencies in the safe, secure and timely adoption of cloud computing technologies.

Closing the IT Gap

We have been deliberate in engaging government, industry, and academia to ensure a broad range of views are considered as we develop a comprehensive approach to cloud computing.

[6] http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-15.pdf

The Federal Chief Information Officers Council, in partnership with the GSA and NIST, is working on a government-wide strategy for the safe and secure use of cloud computing services for release by the end of calendar year 2010.

We are also working closely with the National Association of State Chief Information Officers (NASCIO) to streamline procurement processes, develop standards, and ensure the safe and secure adoption of cloud computing technologies.

Additionally, we are asking agencies to reflect their data center consolidation plans and analysis of cloud computing alternatives in their FY 2012 budget submissions.[7]

Cloud computing reflects the commoditization of IT services and follows naturally from the combination of cheaper and more powerful processors with faster and more ubiquitous networks.

Investments in the private sector have led to historic productivity gains. In their daily lives, the American people can receive services on line rather than in line. They expect the same from their Government. Unfortunately, the IT gap contributes to a vastly different experience. When the American people deal with their Government, they are confronted by a culture that says "there's a paper form that" versus one that says "there's an app for that" when dealing with the private-sector.

Cloud computing is not a silver bullet, but offers a transformational opportunity to fundamentally reshape the operations of government and close the IT gap. The Obama Administration is committed to leveraging the power of cloud computing in a safe and secure manner to help close the technology gap and deliver results for the American people. Thank you again for the opportunity to appear today and I look forward to answering your questions.

[7] http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-19.pdf

Appendix – Characteristic of Cloud Computing

Below is from NIST's Cloud Computing Definition (Version 15), available via: csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

Essential Characteristics:

- **On-demand self-service.** A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- **Broad network access.** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- **Resource pooling.** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- **Rapid elasticity.** Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- **Measured Service.** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Deployment Models:

- **Private cloud.** The cloud infrastructure is operated solely for one organization. It may be managed by the organization or a third party and may exist on premises or off premises.
- **Community cloud.** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security

requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premises or off premises.

- **Public cloud.** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- **Hybrid cloud.** The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Service Models:

- **Cloud Software as a Service (SaaS).** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- **Cloud Platform as a Service (PaaS).** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
- **Cloud Infrastructure as a Service (IaaS).** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Chairman TOWNS. Thank you very much for your testimony.

Mr. McClure is the Associate Administrator of the General Services Administration's Office of Citizens Services and Innovative Technologies. Welcome, Mr. McClure.

STATEMENT OF DAVID McCLURE

Mr. MCCLURE. Thank you, Chairman Towns, Ranking Member Bilbray, all the other committee members here this morning. Thanks for having me testify in front of you on what the General Services Administration is doing to assist in the adoption of cloud computing.

I think Vivek has done a good job in outlining for you what we see as some of the tremendous benefits of cloud computing being adopted in the Federal Government.

At GSA, we also believe that the adoption of safe and secure cloud computing by the Federal Government represents a huge opportunity for us in terms of getting access to more modern technology and lowering the costs that we are spending on technology; and various forms of cloud computing are already in place in the Federal Government today.

Quick example, at GSA we have put the Government's main primary information portal, USA.gov, into a cloud computing environment last year. We are already reaping the benefits in terms of a more reliable uptime from the system; we have lowered our overall computing costs by an estimated $1.7 million; and we actually have raised the security posture of the system by going to a more reliable security arrangement with our cloud provider. So it does have tremendous benefits.

As you also know, GSA plays a lead role in the President's sustainability agenda. We anticipate that cloud computing will be a major factor in reducing the environmental impact of technology and also will help achieve some of our national sustainability goals. Cloud computing can be part of an overall strategy to reduce the need for these multiple data centers that we have all over the Government and the energy they consume. So we see it helping improve services by lowering the cost and also maintaining a better environment compared to the redundant and often needlessly redundant brick and mortar data center structures that we have in place today.

As part of our leadership in the cloud computing environment, we have stood up a cloud computing program management office, it is housed in my office at GSA. It provides the technical and administrative leadership for the administration's cloud computing initiatives.

We support the design and operation of cloud procurement vehicles; we look at ways in which we can identify enhancing security requirements, working closely with NIST, as well as with OMB; we have facilitated the adoption of these requirements in the last few months; we also sponsor some cloud demonstration projects from a piloting perspective so that we can demonstrate how this technology can be effective before going full bore; and we are engaged in data center analysis and strategy planning with OMB as part of our responsibilities with the PMO as well.

I think we also play a huge role in disseminating information throughout the Government on just what is happening in cloud computing. We are a knowledge repository for examples, best practices, and things that have really worked for us to date.

So let me just highlight real quickly a few of those areas for you. I think one of the most significant challenges we face in cloud computing is certainly in the security area. Agencies are concerned about the risk of housing data offsite, in a cloud, if federally mandated security controls and accountabilities are not in place.

The Federal CIO, our cloud PMO, the CIO Council, which has a security working group, and NIST have come together to try to tackle that problem. We have developed a process and corresponding security controls that have been agreed to by multiple agencies. We are calling this program FedRAMP. It provides a uniform Government-wide risk management approach for enterprise level IT systems and it will enable agencies to either use or leverage existing security authorizations.

Mr. Chairman, this is a first in the Federal Government, and it should greatly reduce our security cost; it should enable rapid acquisitions of solutions; it should reduce agency levels of effort; and it should shift the focus of security to monitoring and protecting our computing environments.

GSA is working with NIST and the CIO Council to make sure that this program is put in place and we will be piloting several things through FedRAMP to get it up to speed with some improvements as we test it out.

The second area is providing newly commercial-provided cloud services via a Web site called Apps.gov. This is the primary responsibility of GSA. It is modeled on GSA product and service acquisition storefronts; it provides an easy, simple way to find, research, and procure commercial cloud products and services. And we feel like that has been a real benefit to Federal agencies both in the softwares of service area and soon to be in infrastructures of service for cloud computing.

A new class of Internet-based applications have also come onboard called Web 2.0 that focus on delivering information to diverse communities. Many of these solutions are Web-based and many are also hosted in the cloud. We at GSA are making sure that we are providing, as common tools to agencies, social media Web 2.0 tools that are completely policy compliant with all Federal privacy and security policies, and it gives them an advantage in terms of doing this independently on their own. And I think we have already achieved some significant cost savings by putting some of these in place Government-wide.

So cloud computing, from our perspective, has the ability to fundamentally reshape how we are approaching Government operations and how we are using computing power for business process improvement and citizen service delivery support. It can also shift the focus to the added value use of information, which I think is what our next decade is truly about; and do this in a very cost-effective way in today's digitally oriented world.

Chairman TOWNS. Mr. McClure, could you sum up?

Mr. McCLURE. Yes. And, third, I think it frees up some resources for us to really focus on some of the real information needs of the Government as well.

So, in general, I think we are supporting the effort the best way we can with some of our procurement activities and some of our best practices support, and I think these are adding up to really advance the computing cause. Thanks.

[The prepared statement of Mr. McClure follows:]

STATEMENT OF

DR. DAVID MCCLURE
ASSOCIATE ADMINISTRATOR
OFFICE OF CITIZEN SERVICES AND INNOVATIVE TECHNOLOGIES
GENERAL SERVICES ADMINISTRATION

BEFORE THE

HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT

JULY 1, 2010

Chairman Towns, Chairwoman Watson, and Members of the Committee, I am David McClure, Deputy Administrator, Office of Citizen Services and Innovative Technologies at the General Services Administration (GSA). Thank you for the opportunity to appear before you today to discuss GSA's role in supporting development and deployment of cloud computing technology.

Cloud computing enables convenient, rapid, and on-demand computer network access—most often via the Internet--to a shared pool of configurable computing resources (in the form of servers, networks, storage, applications, and services). Quite simply, it is the way computing services are delivered that is revolutionary. Cloud computing allows users to provision computing capabilities rapidly and as needed; that is, to scale out and scale back as required, and to pay only for services used. Users can provision software and infrastructure cloud services on demand with minimal, if any, human intervention. Because cloud computing is based on resource pooling and broad network access there is a natural economy of scale that can result in lower costs to agencies. In addition, cloud computing offers a varied menu of service models from a private cloud operated solely for one organization to a public cloud that is available to a large industry group and the general public and owned by an organization that is selling cloud computing services.

At GSA, we think the adoption of safe and secure cloud computing by the Federal government presents an opportunity to close the IT performance gap. Various forms of cloud computing solutions are already being used in the federal government today to save money and improve services. Let me illustrate with just a few examples:

- The Department of the Army Experience Center in Philadelphia is piloting the use of a customer relationship management (CRM) tool. The Center is a recruiting center that reaches out to young people who are interested in joining our armed forces. The Center wants to move to real time recruiting and to use tools and techniques that are familiar and appeal to its young demographic. They are using a CRM provided by SalesForce to track recruits as they work with the Center. Since the tool integrates directly with e-mail, Twitter and Facebook, recruiters can maintain connections with potential candidates directly after they leave the Center. The Army estimated that to implement a traditional CRM would have cost $500,000. The cloud-based solution has been implemented at the cost of $54,000.

- The Department of Energy is evaluating the cost and efficiencies resulting from leveraging cloud computing solution across the enterprise to support business and scientific services. The Lawrence Berkeley Lab has deployed over 5,000 mailboxes on Google Federal Premiere Apps and they are now evaluating the use of Amazon Elastic Compute Cloud (EC2) to handle excess capacity for computers during peak demand. The Lab

estimates that they will save $1.5 million over the next five year in hardware, software and labor costs from the deployments they have made.

- Finally, my own agency – GSA has moved the primary information portal, USA.gov, to a cloud-based host. This enabled the site to deliver a consistent level of access to information as new data bases are added, as peak usage periods are encountered, and as the site evolves to encompass more services. By moving to a cloud, GSA was able to reduce site upgrade time from nine months to one day; monthly downtime improved from two hours to 99.9% availability; and GSA realized savings of $1.7M in hosting services.

In addition to improved services, GSA anticipates that cloud computing will be a major factor in reducing the environmental impact of technology and help achieve important sustainability goals. Effective use of cloud computing can be part of an overall strategy to reduce the need for multiple data centers and the energy they consume. Currently, GSA is supporting OMB in working with agencies to develop plans to consolidate their data centers. Using the right deployment model – private cloud, community cloud, public cloud, or a hybrid model – can help agencies buy improved services at a lower cost within acceptable risk levels, without having to maintain expensive, separate, independent and often needlessly redundant brick and mortar data centers.

In February 2010, the Federal CIO announced the Federal Data Center Consolidation Initiative. In it, he designated two Federal agency CIOs -- Richard Spires (DHS) and Michael Duffy (Treasury) – to lead the effort inside the Federal CIO Council. It also highlighted the following goals:

- Reduce the cost of data center hardware, software and operations
- Increase the overall IT security posture of the government
- Shift IT investments to more efficient computing platforms and technologies
- Promote the use of Green IT by reducing the overall energy and real estate footprint of government data centers

GSA has a significant leadership role in supporting the adoption of cloud computing in the federal government. We have concentrated our efforts on facilitating easy access to cloud based solutions from commercial providers that meet federal requirements, enhancing agencies' capacity to analyze viable cloud computing options that meet their business and technology modernization needs, and addressing obstacles to safe and secure cloud computing. In particular, GSA facilitates innovative cloud computing procurement options, ensures effective cloud security and standards are in place, and identifies potential multi-agency or government-wide uses of cloud computing solutions. GSA is also the information "hub" for cloud use case examples, decisional and implementation best practices, and sharing exposed risks and lessons learned. We have set up

the Info.Apps.Gov site as an evolving knowledge repository for all government agencies to use and contribute their expertise.

Let me briefly highlight how GSA is specifically providing execution capabilities to empower sensible cloud computing adoption in the federal government.

Federal Cloud Computing Project Management Office

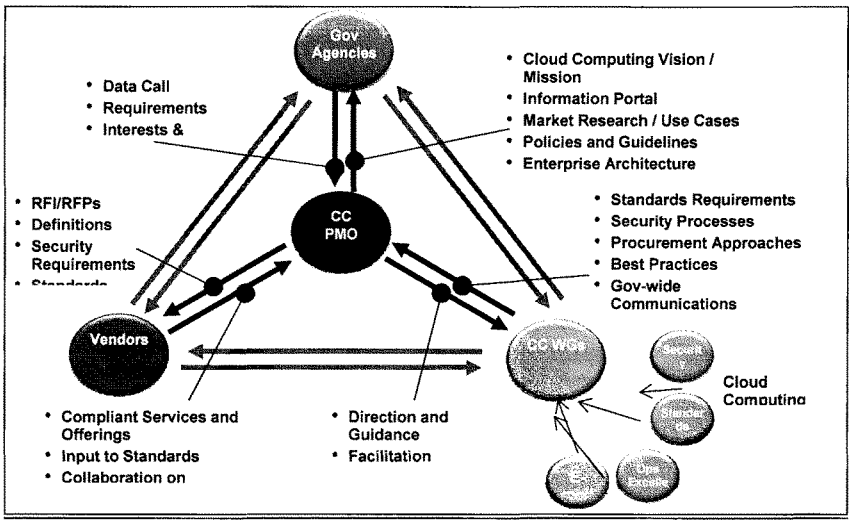
In March of 2009, the Federal Chief Information Officer (CIO) Council identified cloud computing as a priority for meeting the growing need for effective and efficient use of information technology to meet the performance and mission needs of the government. To assist in fostering cloud computing adoption, the Federal Cloud Computing Program Management Office (PMO) was created in April of 2009 at GSA. The PMO resides in the Office of Citizen Service and Innovation Technologies and is directed by Ms. Katie Lewin who directly reports to the Deputy Administrator for Innovative Technology, Mr. Sonny Bhagowalia. The Director of the PMO also meets weekly with the Federal CIO to report on progress, discuss risks and mitigations, identify promising cloud projects across the government and refine direction. The PMO also reports on its activities and results to the CIO Council Cloud Computing Executive Steering Committee (ESC). The ESC provides oversight for the Federal Cloud Computing Initiative and fosters communications among agencies on cloud computing. ESC Membership includes senior IT executives from across the entire Federal government.

The PMO provides technical and administrative leadership to cloud computing initiatives. PMO staff is drawn from GSA technical experts with some additional contractor support. The primary focus of the PMO is on the following activities:

- Support for the design and operation of the Apps.Gov cloud computing storefront and related cloud procurement initiatives
- Facilitating identification of key cloud security requirements (certification, accreditation, and authorization), particularly on a government-wide basis through a new FedRAMP initiative
- Promotion of current and planned cloud projects across the government
- Data center consolidation analysis, planning, and strategy support
- Development and open dissemination of relevant cloud computing information.

To augment their skill base, the PMO has formed working groups to address specific areas including security, standards and specific cloud-based solutions with government or multi-agency use, such as cloud based e-mail services. The working groups are composed of staff from across the government who bring expertise and interest to address specific obstacles or define paths to adoption. Each group is chaired by a government expert. The National Institute of Standards and Technology (NIST) led both the security and the standards

groups. The e-mail group is chaired by an expert from Department of the Interior.



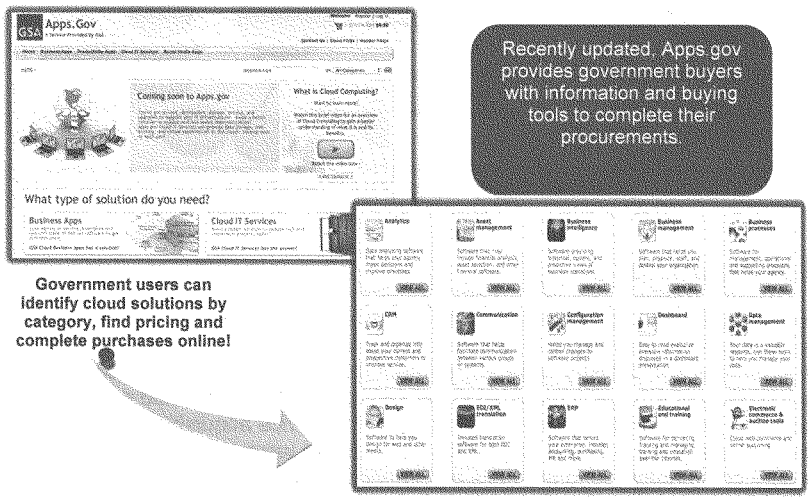
Cloud Computing PMO Operations

Cloud Procurement

Cloud services are usually offered and purchased as commodities. This is a new way of buying IT services and requires careful research on both government requirements and industry capability to meet demand. To assist agencies in buying new commercially provided cloud services, GSA established a website -- Apps.Gov -- modeled on other GSA product and service acquisition "storefronts." The purpose of Apps.Gov is to provide easy, simple ways to find, research, and procure commercial cloud products and services. Agencies can search for software as a service (SaaS) products categorized under 33 business purpose headings and get product descriptions, price quotes, and links to more information on specific products. Usage patterns to date indicate that agencies use this information to either directly buy SaaS products or, alternatively, as a source of marketplace research that is used to support cloud procurements using other vehicles such as GSA Schedule or GSA Advantage.

Apps.Gov also has information on no-cost social media applications that have agreed to "government-friendly" Terms of Service. When a user hits the SEND REQUEST button, they are linked to their agency's social media coordinator to complete the request for use of the tool in compliance with their agency's social media policy.

To support access to cloud-based Infrastructure as a Service (IaaS), the Cloud PMO works with the Federal Acquisition Service (FAS) at GSA. FAS has primary responsibility for operating on-line acquisition services that are available for government-wide use. In May 2009, the PMO issued a Request for Information (RFI) asking the marketplace how they would address cloud computing business models, pricing, service level agreements, operational support, data management, security and standards. The responses to this RFI were incorporated into a Request for Quote (RFQ) for Infrastructure as a Service capabilities and pricing. The result will be a multiple award blanket purchase agreement that agencies can use to procure cloud based web hosting, virtual machine, and storage services within a moderate security environment as defined by the Federal Information Security Act (FISMA). That RFQ closed yesterday and is currently in an evaluation stage.



Apps.Gov Storefront Screen Shot

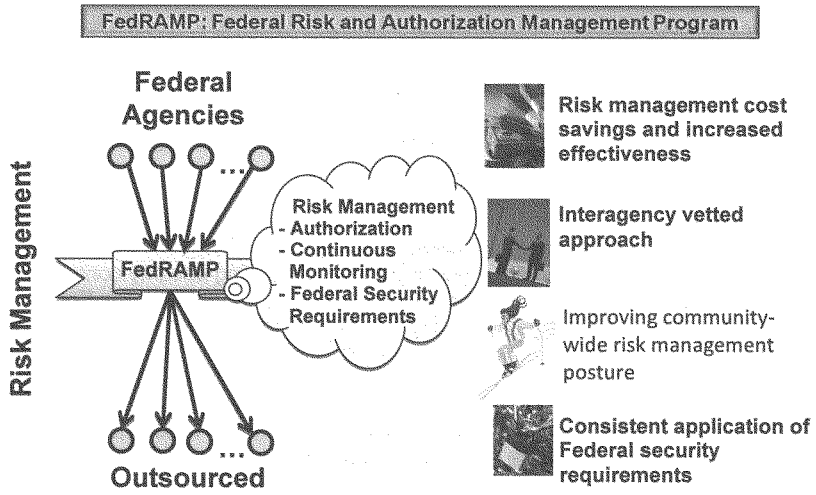
Cloud Computing Security

One of the most significant obstacles to the adoption of cloud computing is security. Agencies are concerned about the risks of housing data off-site in a cloud if FISMA security controls and accountabilities are not in place. In other words, agencies need to have valid certification and accreditation (C&A) process and a signed Authority to Operate (ATO) in place for each cloud-based product they use. While vendors are willing to meet security requirements, they would prefer not to go through the expense and effort of obtaining a C&A and ATO for each use of that product in all the federal departments and agencies. The PMO formed a security working group, initially chaired by NIST to address this problem. The group developed a process and corresponding security controls that were agreed to by multiple agencies – which we have termed as the Federal Risk and Authorization Management Program (FedRAMP).

FedRAMP is a government-wide initiative to provide joint authorizations and continuous security monitoring services for all federal agencies with an initial focus on cloud computing. By providing a unified government-wide risk management for enterprise level IT systems, FedRAMP will enable agencies to either use or leverage authorizations with:

- Vetted interagency approach;
- Consistent application of Federal security requirements;
- Improved community-wide risk management posture; and
- Increased effectiveness and management cost savings.

FedRAMP allows agencies to use or leverage authorizations. Under this program, agencies will be able to rely upon review security details, leverage the existing authorization, and secure agency usage of system. This should greatly reduce cost, enable rapid acquisition, and reduce effort.



FedRAMP has three components:

1. Security Requirement Authorities which create government-wide baseline security requirements that are interagency developed and approved. This will initially be the Federal Cloud Computing Initiative and ultimately live with the ISIMC Working Group.
2. The FedRAMP Office which will coordinate authorization packages, manage authorized system list, and provide continuous monitoring oversight. This will be managed by GSA.
3. A Joint Authorization Board which will perform authorizations and on-going risk determinations to be leveraged government-wide. The board will consist of representatives from GSA, DoD, DHS and the sponsoring agency of the authorized system.

GSA is working with OMB, security groups including the Federal CIO Council's Information Security and Identity Management Committee, and the marketplace to vet this program and ensure that it will meet the security requirements of the government while streamlining the process for industry.

Cloud Computing and Open Government

In the past decade, vast increases in the ubiquity and availability of storage space, bandwidth, and computing power have enabled a new class of Internet-based applications—broadly called "web 2.0"—that focus less on one-way delivery of information and more on enabling large, diverse communities to come together, share their wisdom, and take action. Increasingly, citizens—government's customers—simply expect to find the information they want and need through the use of the on-line social networks and platforms they are rapidly adopting and use as part of their everyday lives.

As our Administrator, Martha Johnson, noted upon being sworn in February 2010:

> *Hoarding and hiding information prevents citizens and civil servants from understanding and participating in the public process effectively...We at GSA can help change that. We can make the information more available, as a first step. And we can do much more. We can, and will, take advantage of emerging technologies for sorting, sharing, networking, collective intelligence, and using that information. Our goal is nothing short of a nation that relies not on select data and statistical boxing matches, but on accurate evidence that supports knowledge and wisdom.*[1]

Most of these new web 2.0 technologies and tools are available as cloud-based SaaS solutions and/or are hosted in cloud computing infrastructure environments. This allows the government to offer these tools and services in a very cost-efficient manner. Let me highlight a few examples:

- The **Common Open Government Dialogue Platform** is a project undertaken by GSA in response to the Open Government Directive's mandate that agencies "incorporate a mechanism for the public to provide input on the agency's Open Government Plan." Over the course of six weeks, GSA provided interested agencies with a no-cost, law- and policy-compliant, public-facing online engagement tool, as well as training and technical support to enable them to immediately begin collecting public and employee input on their forthcoming open government plans. Since then, GSA has worked to transfer ownership of the open government public engagement tool, powered by a cloud SaaS platform called IdeaScale, to interested agencies, in a manner that provided both policy and legal compliance, as well as support for sustained engagement. The tool was launched in February 2010 across 22 federal agencies and the White House Office of Science and Technology Policy; overall

[1] http://www.gsa.gov/Portal/gsa/ep/contentView.do?pageTypeId=10430&channelId=-24827&P=&contentId=29129&contentType=GSA_BASIC

resource investment was less than $10,000 – far less than the hundreds of thousands or millions of dollars that would have resulted from agencies independently pursuing and procuring IT solutions. The agencies' dialogue sites garnered over 2,100 ideas, over 3,400 comments, and over 21,000 votes during a six-week "live" period and the tool continues to be used by several agencies for a variety of other open government purposes.

- **USASpending.gov** is a source for information collected from agencies in accordance with the Federal Funding Accountability and Transparency Act of 2006. This public facing web site is a cornerstone of the Administration's efforts to make government open and transparent. Using USAspending.gov, the public can determine how their tax dollars are spent and gain insight into the Federal spending processes across agencies. It also houses the Federal IT Dashboard, which displays details on the nearly 800 major federal IT investments based on data reported to the Office of Management and Budget. This data is also now housed in a cloud infrastructure environment maintained by NASA.

- **Data.gov** is the central portal for citizens to find, download, and assess government data. It now hosts over 270,000 data sets covering topics ranging from healthcare to commerce to education. Data.gov was one of the first public facing government websites to deploy cloud computing successfully in government. It empowers citizens by allowing them to create personalized mash-ups of information from diverse sources (e.g., local school academic scores arrayed by education spending levels), solve problems (e.g., FAA flight time arrival information), and build awareness of government's role in activities affecting daily activities (e.g., food safety, weather, and the like).

- **Challenge.gov** is a government-wide challenge platform that will be hosted in a cloud computing infrastructure service to facilitate government innovation through challenges and prizes. This tool provides forums for seekers (the federal agency challenger looking for solutions) and solvers (those with potential solutions) to suggest, collaborate on, and deliver solutions. It will also allow the public to easily find and interact with federal government challenges. The platform responds to requirements defined in a March 8, 2010, OMB Memo, "Guidance on the Use of Challenges and Prizes to Promote Open Government" which included a requirement to provide a web-based challenge platform within 120 days. GSA is also exploring acquisition options to make it easier for agencies to procure products and services related to challenges.

- **Citizen Engagement Platform** will provide a variety of blog, challenge and other engagement tools to make it easy for government to engage with citizens, and easy for citizens to engage with government. The platform addresses agencies' need for easy-to-use, easy-to-deploy, secure and policy-

compliant tools. This "build once, use many" approach adds lightweight, no-cost options for agencies to create a more open, transparent and collaborative government with tools either hosted or directly managed by GSA.

Conclusion

Mr. Chairman, cloud computing has a promising future in transforming the federal government because of its ability to fundamentally reshape government IT operations used for critical government business process and citizen service delivery support. It can help shift our focus to value added use of the information we collect and provide cost effective services in a digitally and networked enabled world. Additionally, it has the potential to free up resources that have gone to support data centers and capabilities that are better leveraged across the community – at bureau, agency or cross-agency level. At GSA, we are supporting this transformation by leveraging cloud solutions and acquisitions on a government-wide basis wherever possible to maximize economies of scale.

Thank you for the opportunity to appear today and I look forward to answering questions from you and members of the Subcommittee.

Chairman TOWNS. Thank you very much for your testimony.

Ms. Furlani is Director of the Information Technology Laboratory at the National Institute of Standards and Technology. Welcome.

STATEMENT OF CITA FURLANI

Ms. FURLANI. Thank you, Chairman Towns and members of the committee. I appreciate the opportunity to appear before you today to discuss our role in the deployment of cloud computing technology in the Federal Government.

Our role is to promote the effective and secure use of the technology within Government by providing technical guidance and promoting standards. The three cybersecurity objectives, ensuring the confidentiality, integrity, and availability of information technology systems, are particularly relevant to cloud computing. These three objectives provide a technical foundation to help address the associated privacy requirements.

This cloud model that I have listed in my testimony is composed of five essential characteristics, three service models, and four deployment models, which are laid out fully in the written testimony.

The NIST cloud computing definition is the following: Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources, such as networks, servers, storage, applications, and services, which can be rapidly provisioned and released with minimal management effort or service provider interaction.

This definition has been broadly recognized and helps to clarify a complex emerging information technology paradigm. However, there is still much work to be done. We have initiated focused activities to develop Federal cloud computing security guidance, as well as to facilitate the development of cloud computing standards. The following are specific NIST efforts which promote the effective and secure use of cloud computing technology within Government: NIST held a cloud computing forum and workshop in May to engage stakeholders on ways to best accelerate the Federal Government's secure adoption of cloud computing. Over 500 stakeholders attended this event.

We are developing a cloud computing special publication which will provide insight into the technical benefits, risks, and considerations related to the secure and effective uses of cloud computing, and provide guidance in the context of cloud computing to provide interoperability, portability, and security. This publication will also identify future research areas in cloud computing.

As requested by OMB, NIST serves as the Government lead working with other Government agencies, industry, academia, and standards development organizations to leverage appropriate existing standards and to accelerate the development of cloud computing standards where gaps exist. We have initiated the Standards Acceleration to Jumpstart Adoption of Cloud Computing [SAJACC]. The SAJACC goal is to facilitate the accelerated development of high-quality standards and to reduce the technical uncertainty during the interim period before many cloud computing standards are formalized.

NIST, in a technical advisory role, supports the Federal interagency efforts which have been mentioned to the development of a

concept for a Federal approach to coordinate and apply consistent security authorization requirements for cloud computing systems. The NIST role is to provide guidance for a technical approach and process which is consistent with NIST security guidance in the context of the Federal Information Security Management Act.

NIST has also initiated a strategic virtualization laboratory effort to research and evaluate the security of virtualization techniques and to mitigate security vulnerabilities in virtualized and cloud systems. This will inform NIST cloud and virtualization guidelines.

We have also initiated a Modeling and Analyzing Complex Behaviors in Cloud Computing project. This project seeks to understand and predict behavior in large distributed information systems. In cloud computing, NIST is initiating a study of the applicability of our modeling and analysis techniques to computational clouds.

As you have just heard, this is a big effort. Thank you for the opportunity to testify today on NIST's role in the development and deployment of cloud computing technology. I would be happy to answer any questions you may have.

[The prepared statement of Ms. Furlani follows:]

Testimony of

Cita M. Furlani
Director
Information Technology Laboratory

National Institute of Standards and Technology
United States Department of Commerce

United States House of Representatives
Committee on Oversight and Government
Reform

"Cloud Computing: Benefits and Risks of
Moving Federal IT into the Cloud"

July 1, 2010

Chairman Towns, Chairwoman Watson, and Members of the Committee, I am Cita Furlani, the Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss our role in the development and deployment of cloud computing technology.

NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

As one of the major research components within NIST, the ITL accelerates the development and deployment of information and communication systems that are reliable, usable, interoperable, and secure; advances measurement science through innovations in mathematics, statistics, and computer science; and conducts research to develop the measurements and standards infrastructure for emerging information technologies and applications.

NIST works with federal agencies, industry, and academia to research, develop and deploy information security standards and technology to protect information systems against threats to their confidentiality, integrity and availability. NIST researches technologies such as identity management and verification, metrics for complex systems, automation of discovery and maintenance of system security configurations and status, and techniques for specification and automation of access authorization in support of many different kinds of access policies.

In addition to IT-related technology research, ITL is responsible for the development of, publishing, and providing explanatory support for Federal standards, guidelines, and best practices related to cybersecurity.

NIST's role in cloud computing is to promote the effective and secure use of the technology within government by providing technical guidance and promoting standards. The three cybersecurity objectives, ensuring the confidentiality, integrity, and availability of information technology systems, are particularly relevant as these are the high priority concerns and perceived risks related to cloud computing.

Although the power of modern cloud computing systems is new, the ideas behind cloud computing reach back through decades. In the early 1960s, researchers proposed the idea of computing as a utility, similar to other services such as gas or electricity. Around the same time, techniques to make a single computer appear to be many separate "virtual" computers were developed and implemented on mainframe computers. Some of the building blocks for cloud computing were in place, but performance and costs were barriers, and networking was inadequate. Years of hardware advances were needed to close the gap. By the 1990s, the Internet had made grid computing possible: many computers working together on a single problem over a network. By the 2000s, the term cloud computing was being used to describe computing services delivered

over a network, and, in 2010, a substantial and growing number of vendors are developing cloud computing offerings for government, industry, and the general public.

Before discussing ongoing NIST efforts which are directed toward promoting secure and effective use of cloud computing, I refer to the widely-cited NIST definition of cloud computing[1]. Computer scientists at NIST developed this definition in collaboration with industry, academia and government and we expect it to evolve over time as the cloud industry and cloud technology matures:

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Essential Characteristics:

- *On-demand self-service.* A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

- *Broad network access.* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

- *Resource pooling.* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

- *Rapid elasticity.* Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

---

[1] The NIST Definition of Cloud Computing, Version 15, Peter Mell and Tim Grance, October 7, 2009.

- *Measured Service.* Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Service Models:

- *Cloud Software as a Service (SaaS).* The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

- *Cloud Platform as a Service (PaaS).* The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

- *Cloud Infrastructure as a Service (IaaS).* The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

- *Private cloud.* The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

- *Community cloud.* The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premises or off premises.

- *Public cloud.* The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

- *Hybrid cloud.* The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

  Note: Cloud software takes full advantage of the cloud paradigm by being service oriented with a focus on statelessness, low coupling, modularity, and semantic interoperability.

This NIST cloud computing definition, most recently revised in October 2009, has been broadly recognized and helps to clarify a complex emerging information technology paradigm. However, there is still much work to be done.

NIST has initiated focused activities to develop federal cloud computing security guidance as well as to facilitate the development of cloud computing standards. Both are essential and must be considered in parallel in order to effectively support the secure implementation of cloud computing technology. NIST efforts respond not only to high priority security requirements, but to interoperability and portability requirements, which are interrelated with and essential to effectively address cloud computing security.

Following are specific NIST efforts which promote the effective and secure use of cloud computing technology within government by providing technical guidance and promoting the development of standards.

NIST recently held a Cloud Computing Forum and Workshop. The goal was to engage with stakeholders on ways to accelerate the federal government's secure adoption of cloud computing. Over 500 stakeholders registered for the event – which included representatives from industry, federal government, state governments, academia, and standards development organizations.

NIST is developing a cloud computing Special Publication which will use the definition of cloud computing as a frame of reference to organize and present analysis, recommendations and guidance. The document will provide insight into the technical benefits, risks, and considerations related to the secure and effective uses of cloud computing and guidance in the context of cloud computing: interoperability, portability, and security. The publication will also outline typical terms of use for cloud systems and will identify future research areas in cloud computing as well as recommendations. NIST will develop additional cloud computing Special Publications as research and analysis are completed.

As requested by OMB, NIST serves as the government lead, working with other government agencies, industry, academia, and standards development organizations to leverage appropriate existing standards and to accelerate the development of cloud computing standards where gaps exist. The expectation is that standards will shorten the adoption cycle, support cost savings and the ability to more quickly create and deploy enterprise applications.

Under the provisions of the National Technology Transfer and Advancement Act (PL 104-113) and OMB Circular A-119, NIST is tasked with the role of encouraging and coordinating federal agency use of voluntary consensus standards and participation in the development of relevant standards, as well as promoting coordination between the public and private sectors in the development of standards and in conformity assessment activities. NIST works with other agencies to coordinate standards issues and priorities with the private sector through consensus standards organizations such as the American National Standards Institute (ANSI), the International Organization for Standardization (ISO), the Institute of Electrical and Electronic Engineers (IEEE), the Internet Engineering Task Force (IETF), and the International Telecommunication Union (ITU). NIST leads national and international consensus standards activities in cryptography, biometrics, electronic credentialing, secure network protocols, software and systems reliability, and security conformance testing – all essential for secure cloud computing implementation.

NIST has initiated the Standards Acceleration to Jumpstart Cloud Computing (SAJACC) project. The SAJAAC goal is to facilitate the development of cloud computing standards. The analysis and results completed under SAJACC will be used to inform the cloud computing Special Publications described above. SAJACC refers to a strategy, a process, and a portal.

SAJACC was initiated to address a widely acknowledged need in the development and implementation of new complex technologies. Historically, a gap has existed between the time when standards are needed and the time when they become formalized. Complex standards such as the Portable Operating System Interface [for Unix] and current Internet standards have taken years to develop. This has occurred because the development of standards is dependent on the inherently time consuming process of broad participation and consensus building, is driven by technical innovation, and requires due diligence in order to produce a standard of quality and completeness such that it will be effective and broadly adopted.

The SAJAAC strategy is two-fold: 1) to accelerate the development of high-quality standards and 2) to reduce technical uncertainty during the interim adoption period before many cloud computing standards are formalized.

The heart of the SAJACC concept is the process of identifying and validating interim candidate interface specifications by testing against requirements which demonstrate portability, interoperability, and security for users of cloud systems. SAJACC is applying

the use case development method to define, refine, and interpret requirements in the form of behavioral scenarios which describe the interaction between people and computer systems. The project is currently formulating an initial set of twenty five use cases, and vetting these with cloud computing stakeholders in academia, government, and industry. After the use cases have been refined, they will be made available through a public website. In order to verify and demonstrate the test plan and execution process, NIST will conduct an initial set of validation tests against an initial set of legacy interfaces, and publish the results as an example of how future collaborative efforts could be accomplished.

Information exchange and visibility will be accomplished through a SAJACC website. This portal is planned as a public Internet-accessible repository of cloud computing use cases, documented cloud system interfaces (i.e., specifications which have not yet evolved to become formal standards), pointers to cloud system reference implementations (i.e., cloud computing systems where these specifications were incorporated as part of the implementation), and test results which show the extent to which different interfaces can support individual use cases (i.e., satisfy security, portability, and interoperability requirements.)

SAJACC by definition leverages, coordinates, and is heavily dependent on contributions from external stakeholders with an interest in cloud computing standards. The process of identifying new interfaces (with corresponding reference implementations) and new use cases will be ongoing.

NIST has developed standards to support federal agencies' information security requirements for many years, beginning in the early 1970s with enactment of the Brooks Act. Through the Federal Information Security Management Act (FISMA), Congress again reaffirmed NIST's leadership role in developing standards for cyber security. FISMA provides for the development and promulgation of Federal Information Processing Standards (FIPS) that are "compulsory and binding" for Federal computer systems. The responsibility for the development of FIPS rests with NIST, and the authority to promulgate mandatory FIPS is given to the Secretary of Commerce. Section 303 of FISMA states that NIST shall:

- have the mission of developing standards, guidelines, and associated methods and techniques for information systems;
- develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems; and
- develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems.

These activities include, for systems other than national security systems, standards and guidelines that must include, at a minimum (1) standards to be used by all agencies to categorize all their information and information systems based on the objectives of providing appropriate levels of information security, according to a range of risk levels; (2) guidelines recommending the types of information and information systems to be included in each category; and (3) minimum information security requirements for information and information systems in each category.

NIST addresses cyber security challenges, which are directly applicable to cloud computing throughout the information and communications infrastructure, through its cross-community engagements. NIST employs collaborative partnerships with our customers and stakeholders in industry, government, academia, and consortia to take advantages of technical and operational insights and to leverage the resources of a global community. NIST is responsible for establishing and updating, on a recurring basis, the federal government's risk management framework, cybersecurity controls, and assessment procedures to determine control effectiveness. NIST engages government and industry to harmonize information security requirements to align with industry business models and best practices.

An example is the release of Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* in August 2009 which was developed by the Joint Task Force Transformation Initiative consisting of members from NIST, the Department of Defense, Office of the Director of National Intelligence, and the Committee on National Security Systems. This unified set of security controls provides a standardized method for expressing security at all levels, from system development and acquisition to operational implementation. This allows for an environment of information sharing and interconnections among these communities and significantly reduces costs, time, and resources needed to secure information systems.

In close collaboration with the Department of Defense, the Committee on National Security Systems and the Intelligence Community, NIST revised its Certification and Accreditation (C&A) guideline, Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* to fundamentally change the focus of the information system authorization process from a static (a point in time) approach to a continuous monitoring approach. This continuous monitoring approach, implemented with automated tools whenever possible, will provide authorizing officials and senior leaders within federal agencies with critical and timely information on the ongoing security state of their information systems, thus allowing them to make more informed, risk-based decisions when authorizing federal information systems for operation.

The current version of Special Publication 800-37 was also updated to allow certification and accreditation efforts to be leveraged among federal agencies. This is an important building block needed to support government adoption of cloud computing.

In 2009 and 2010, NIST, in a technical advisory role, supported the interagency Federal Cloud Computing Advisory Council (CCAC) Security Working Group in the development of a concept for a federal approach to coordinate and apply consistent security authorization requirements for cloud computing systems.

The overall approach is being defined under the governance and implementation auspices of the Federal CIO Council. The NIST role is to provide guidance for a technical approach and process which is consistent with NIST security guidance in the context of FISMA. More specifically, NIST is supporting the definition of a technical process in the context of and to be consistent with Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, referenced earlier.

Cybersecurity is a vital, central mission of our laboratory and is a key concern and risk factor related to cloud computing adoption. In a public cloud computing deployment model the customer generally does not have control or knowledge over the exact location of the provided resources such as storage, processing, memory, network bandwidth, and virtual machines.

NIST recognizes that effective cybersecurity guidance is holistic and must be considered in the context of broad and comprehensive information security guidance for federal agencies as well as the interoperability, portability and security technical standards development efforts described previously. The NIST cloud computing security guidance recognizes the need to consider the security requirements of the foundation technologies which are applied to implement cloud computing and to leverage the existing computer security capabilities and knowledge base.

NIST will continue to conduct the research necessary to enable and to provide cloud computing and cybersecurity specifications, standards, assurance processes, guidance and technical expertise needed for effective and secure U.S. government and critical infrastructure information systems.

NIST is actively engaged with private industry, academia, non-national security federal departments and agencies, the intelligence community, and other elements of the law enforcement and national security communities in coordination and prioritization of cyber security research, standards development, standards conformance demonstration, and cyber security education and outreach activities.

NIST has initiated a strategic Virtualization Laboratory effort to research and evaluate the security of virtualization techniques and the cloud computing systems that employ them. The lab will serve as a resource for the development of ideas to mitigate security vulnerabilities in virtualized and cloud systems, and to gain hands-on experience that will inform NIST cloud and virtualizations guidelines. The lab plans include two research tasks. The first is to conduct research on the integration of advanced access

control mechanisms into virtualized systems. The second task is to conduct research of metrics to evaluate hypervisor security vulnerability and quality. This task will conduct a study of hypervisor architectural principles and will measure the complexity of hypervisor implementations.

NIST has also initiated the Modeling and Analyzing Complex Behaviors in Cloud Computing project. This project seeks to understand and predict behavior in large distributed information systems by using mathematical and statistical techniques applied by scientists to study physical systems. NIST is evaluating various modeling and analysis methods. NIST is conducting its evaluation in the context of communication networks, computational grids and computational clouds. NIST has conducted several studies related to networks and grids. In cloud computing, NIST is initiating a study of the applicability of our modeling and analysis techniques to computational clouds. As a challenge problem, NIST intends to use the model to study various resource allocation algorithms that might be employed to assign virtual machines to clusters and nodes within a cloud.

Thank you for the opportunity to testify today on NIST's role in the development and deployment of cloud computing technology. I would be happy to answer any questions you may have.

Chairman TOWNS. Thank you very much, Ms. Furlani.
Mr. Wilshusen.

STATEMENT OF GREGORY WILSHUSEN

Mr. WILSHUSEN. Chairman Towns, Ranking Member Issa, Chairwoman Watson, and Ranking Member Bilbray, and other members of the committee, thank you for the opportunity to participate in today's hearing on cloud computing.

At Chairwoman Watson's request, GAO has been reviewing the information security implications of cloud computing and Federal efforts to address them. Today we are releasing our report. My statement will summarize the contents of that report. But first, if I may, Mr. Chairman, I would like to recognize two members of my staff, V.J. DeSouza and Season Dietrick, who were instrumental in the preparation of that report.

As has been discussed, cloud computing is a form of shared computing where users have access to scalable, on-demand information technology services and resources. Service providers offer these capabilities using several service and deployment models, including, for example, a private cloud which is operated solely for an organization and a public cloud, which is available to any paying customer.

Cloud computing has both positive and negative information security implications. Potential security benefits include those related to broad network access, possible economies of scale, and use of self-service technologies. Federal agencies frequently cited as potential benefits low cost disaster recovery and data storage, on-demand security controls, consistent application of those controls, and a reduced need to carry data and removable media.

However, the use of cloud computing can also create numerous information security risks. Twenty-two of 24 major agencies reported that they were concerned or very concerned about the potential security risk associated with cloud computing. These risks include: ineffective or noncompliance security practices of the service provider, inability to examine controls of the provider, data leakage to unauthorized users, and loss of data if cloud service is terminated.

These risks generally relate to the dependence on the security practices and assurances of the service provider and the sharing of computing resources. They also may vary depending upon the cloud deployment model used. For example, private clouds may have a lower threat exposure than public clouds, but evaluating this risk requires an examination of the specific controls in place for the cloud's implementation.

Federal agencies have begun efforts to address information security issues for cloud computing, but specific guidance is lacking and often efforts remain complete. Although individual agencies have identified security measures needed when using cloud computing, they have not always developed corresponding guidance. In addition, several Government-wide cloud computing initiatives are underway by organizations such as OMB and GSA.

Nevertheless, much work remains. For example, OMB has not yet finished the cloud computing strategy or defined how information security issues will be addressed in the strategy. GSA has

begun a procurement for expanding cloud computing services, but still needs to develop specific plans for establishing a shared information security assessment and authorization process. Furthermore, NIST has not yet issued cloud-specific security guidance. Both Federal and private sector officials have identified the need for such guidance.

Accordingly, in the report being released today, GAO recommended that OMB, GSA, and NIST take several actions to address these issues. These agencies generally agreed with our recommendations and indicated that actions were planned or underway to implement them.

To summarize, the use of cloud computing offers promise, but also carries risk. Until Federal guidance and processes that specifically address information security are developed, agencies may be hesitant to implement cloud computing programs, and those that have implemented such programs may not have appropriate security controls in place.

This concludes my statement. I would be happy to answer any questions.

[The prepared statement of Mr. Wilshusen follows:]

United States Government Accountability Office

GAO

Testimony

Before the Committee on Oversight and Government Reform and Its Subcommittee on Government Management, Organization, and Procurement, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Thursday, July 1, 2010

INFORMATION SECURITY

Governmentwide Guidance Needed to Assist Agencies in Implementing Cloud Computing

Statement of Gregory C. Wilshusen
Director, Information Security Issues

GAO
Accountability * Integrity * Reliability

GAO-10-855T

GAO
Accountability Integrity Reliability
Highlights

Highlights of GAO-10-855T, a testimony before the Committee on Oversight and Government Reform and its Subcommittee on Government Management, Organization, and Procurement, House of Representatives

Why GAO Did This Study

Cloud computing, an emerging form of computing where users have access to scalable, on-demand capabilities that are provided through Internet-based technologies, reportedly has the potential to provide information technology services more quickly and at a lower cost, but also to introduce information security risks. Accordingly, GAO was asked to testify on the benefits and risks of moving federal information technology into the cloud. This testimony summarizes the contents of a separate report that is being released today which describes (1) the models of cloud computing, (2) the information security implications of using cloud computing services in the federal government, and (3) federal guidance and efforts to address information security when using cloud computing. In preparing that report, GAO collected and analyzed information from industry groups, private-sector organizations, and 24 major federal agencies.

What GAO Recommends

In the report being released today, GAO recommended that the Office of Management and Budget, the General Services Administration, and the Department of Commerce take steps to address cloud computing security, including completion of a strategy, consideration of security in a planned procurement of cloud computing services, and issuance of guidance related to cloud computing security. These agencies generally agreed with GAO's recommendations.

View GAO-10-855T or key components. For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

July 2010

INFORMATION SECURITY

Governmentwide Guidance Needed to Assist Agencies in Implementing Cloud Computing

What GAO Found

Cloud computing has several service and deployment models. The service models include the provision of infrastructure, computing platforms, and software as a service. The deployment models relate to how the cloud service is provided. They include a private cloud, operated solely for an organization; a community cloud, shared by several organizations; a public cloud, available to any paying customer; and a hybrid cloud, a composite of deployment models.

Cloud computing can both increase and decrease the security of information systems in federal agencies. Potential information security benefits include those related to the use of virtualization and automation, broad network access, potential economies of scale, and use of self-service technologies. In addition to benefits, the use of cloud computing can create numerous information security risks for federal agencies. Specifically, 22 of 24 major federal agencies reported that they are either concerned or very concerned about the potential information security risks associated with cloud computing. Risks include dependence on the security practices and assurances of a vendor, and the sharing of computing resources. However, these risks may vary based on the cloud deployment model. Private clouds may have a lower threat exposure than public clouds, but evaluating this risk requires an examination of the specific security controls in place for the cloud's implementation.

Federal agencies have begun efforts to address information security issues for cloud computing, but key guidance is lacking and efforts remain incomplete. Although individual agencies have identified security measures needed when using cloud computing, they have not always developed corresponding guidance. Agencies have also identified challenges in assessing vendor compliance with government information security requirements and clarifying the division of information security responsibilities between the customer and vendor. Furthermore, while several governmentwide cloud computing security initiatives are under way by organizations such as the Office of Management and Budget and the General Services Administration, significant work needs to be completed. For example, the Office of Management and Budget has not yet finished a cloud computing strategy, or defined how information security issues will be addressed in this strategy. The General Services Administration has begun a procurement for expanding cloud computing services, but has not yet developed specific plans for establishing a shared information security assessment and authorization process. In addition, while the National Institute of Standards and Technology has begun efforts to address cloud computing information security, it has not yet issued cloud-specific security guidance. Until specific guidance and processes are developed to guide the agencies in planning for and establishing information security for cloud computing, they may not have effective information security controls in place for cloud computing programs.

Chairman Towns, Chairwoman Watson, and Members of the Committee and Subcommittee:

Thank you for the opportunity to participate in today's hearing on federal guidance and efforts to address information security when using cloud computing. My statement today is based on our report titled *Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing* (GAO-10-513), which provides a fuller discussion of our results and is being released at this hearing.[1]

Cloud computing is an emerging form of computing that relies on Internet-based services and resources to provide computing services to customers. Examples of cloud computing include Web-based e-mail applications and common business applications that are accessed online through a browser, instead of through a local computer. The current administration has highlighted cloud computing as having the potential to provide information technology (IT) services more quickly and at a lower cost than traditional methods.

We have previously reported that cyber threats to federal information systems and cyber-based critical infrastructures are evolving and growing.[2] Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intentions who can intrude and use their access to obtain and manipulate sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. Further, the increasing interconnectivity among information systems, the Internet, and other infrastructure presents increasing opportunities for attacks. For example, in 2009, several media reports described incidents that affected cloud service providers such as Amazon and Google.

Given the potential risks, you requested that we examine the security implications of cloud computing. In response to your request, our report and my statement provide (1) a description of the models of cloud

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

[2]GAO, *Continued Efforts Are Needed to Protect Information Systems From Evolving Threats*, GAO-10-230T (Washington D.C.: Nov. 17, 2009) and *Cyber Threats and Vulnerabilities Place Federal Systems at Risk*, GAO-09-661T (Washington, D.C.: May 5, 2009).

computing, (2) a description of the information security implications of using cloud computing services in the federal government, and (3) an assessment of federal guidance and efforts to address information security when using cloud computing. In conducting the work for our report, we collected and analyzed information from industry groups, private-sector organizations, the National Institute of Standards and Technology (NIST), and 24 major federal agencies.[3] Our work for the report was performed in accordance with generally accepted government auditing standards.

Cloud Computing Is a Form of Shared Computing with Several Service and Deployment Models

Cloud computing is a new form of delivering IT services that takes advantage of several broad evolutionary trends in information technology, including the use of virtualization.[4] According to NIST, cloud computing is a means "for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction." NIST also states that an application should possess five essential characteristics to be considered cloud computing; on-demand self service, broad network access, resource pooling, rapid elasticity, and measured service.

Cloud computing offers three service models: infrastructure as a service, where a vendor offers various infrastructure components; platform as a service, where a vendor offers a ready-to-use platform on which customers can build applications; and software as a service, which provides a self-contained operating environment used to deliver a complete application such as Web-based e-mail.

In addition, four deployment models for providing cloud services have been developed: private, community, public, and hybrid cloud. In a private

[3]The 24 major federal agencies are the Agency for International Development; the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services , Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; the General Services Administration; the National Aeronautics and Space Administration; the National Science Foundation; the Nuclear Regulatory Commission; the Office of Personnel Management; the Small Business Administration; and the Social Security Administration.

[4]Virtualization is a technology that allows multiple software-based virtual machines with different operating systems to run in isolation, side-by-side on the same physical machine. Virtual machines can be stored as files, making it possible to save a virtual machine and move it from one physical server to another.

cloud, the service is set up specifically for one organization, although there may be multiple customers within that organization and the cloud may exist on or off the premises. In a community cloud, the service is set up for related organizations that have similar requirements. A public cloud is available to any paying customer and is owned and operated by the service provider. A hybrid cloud is a composite of the deployment models.

Cloud Computing Has Both Positive and Negative Information Security Implications

The adoption of cloud computing has the potential to provide benefits related to information security. The use of virtualization and automation in cloud computing can expedite the implementation of secure configurations for virtual machine images. Other advantages relate to cloud computing's broad network access and use of Internet-based technologies. For example, several agencies stated that cloud computing provides a reduced need to carry data in removable media because of the ability to access the data through the Internet, regardless of location. Additional advantages relate to the potential economies of scale and distributed nature of cloud computing. In response to our survey, 22 of the 24 major agencies identified low-cost disaster recovery and data storage as a potential benefit. The self-service aspect of cloud computing may also provide benefits. For example, 20 of 24 major agencies identified the ability to apply security controls on demand as a potential benefit.

In addition to benefits, the use of cloud computing can create numerous information security risks for federal agencies. In response to our survey, 22 of 24 major agencies reported that they are either concerned or very concerned about the potential information security risks associated with cloud computing. Several of these risks relate to being dependent on a vendor's security assurances and practices. Specifically, several agencies stated concerns about:

- the possibility that ineffective or non-compliant service provider security controls could lead to vulnerabilities affecting the confidentiality, integrity, and availability of agency information;
- the potential loss of governance and physical control over agency data and information when an agency cedes control to the provider for the performance of certain security controls and practices;
- the insecure or ineffective deletion of agency data by cloud providers once services have been provided and are complete; and

- potentially inadequate background security investigations for service provider employees that could lead to an increased risk of wrongful activities by malicious insiders.

Multitenancy, or the sharing of computing resources by different organizations, can also increase risk. Twenty-three of 24 major agencies identified multitenancy as a potential information security risk because one customer could intentionally or unintentionally gain access to another customer's data, causing a release of sensitive information. Another concern is the increased volume of data transmitted across agency and public networks. This could lead to an increased risk of the data being intercepted in transit and then disclosed.

Although there are numerous potential information security risks related to cloud computing, these risks may vary based on the particular deployment model. For example, NIST states that private clouds may have a lower threat exposure than community clouds, which may have a lower threat exposure than public clouds. Several industry representatives stated that an agency would need to examine the specific security controls of the vendor the agency was evaluating when considering the use of cloud computing.

Federal Agencies Have Begun Efforts to Address Information Security Issues for Cloud Computing, but Specific Guidance Is Lacking and Efforts Remain Incomplete

Federal agencies have begun to address information security for cloud computing; however, they have not developed the corresponding guidance. About half of the 24 major agencies we asked reported using some form of public or private cloud computing for obtaining infrastructure, platform, or software services. These agencies identified measures they are taking or plan to take when using cloud computing. These actions, however, have not always been accompanied by development of related policies or procedures to secure their information and systems.

Most agencies have concerns about ensuring vendor compliance and implementation of government information security requirements. In addition, agencies expressed concerns about limitations on their ability to conduct independent audits and assessments of security controls of cloud computing service providers. Several industry representatives agreed that compliance and oversight issues are a concern and raised the idea of having a single government entity or other independent entity conduct security oversight and audits of cloud computing service providers on behalf of federal agencies. Agencies also stated that having a cloud service provider that had been precertified as being in compliance with

government information security requirements through some type of governmentwide approval process would make it easier for them to consider adopting cloud computing. Other agency concerns related to the division of information security responsibilities between customer and vendor. Until these concerns are addressed, the adoption of cloud computing may be limited.

Several Governmentwide Cloud Computing Information Security Initiatives Have Been Started, but Key Guidance and Efforts Have Not Been Completed

While several governmentwide cloud computing security activities are under way by organizations such as the Office of Management and Budget (OMB) and the General Services Administration (GSA), significant work remains to be completed. For example, OMB stated that it began a federal cloud computing initiative in February 2009; however, it does not yet have an overarching strategy or an implementation plan. According to OMB officials, the initiative includes an online cloud computing storefront managed by GSA and will likely contain several pilot cloud computing projects, each with a lead agency. However, as of March 2010, a date had not been set for the release of the strategy or for any of the pilots. In addition, OMB has not yet defined how information security issues, such as a shared assessment and authorization process, will be addressed in this strategy.

Federal agencies have stated that additional guidance on cloud computing security would be helpful. Addressing information security issues as part of this strategy would provide additional direction to agencies looking to use cloud computing services. Accordingly, we recommended that OMB establish milestones for completing a strategy for implementing the cloud computing initiative and ensure the strategy addresses the information security challenges associated with cloud computing, such as needed agency-specific guidance, controls assessment of cloud computing service providers, division of information security responsibilities between customer and provider, a shared assessment and authorization process, and the possibility for precertification of cloud computing service providers. OMB agreed with our recommendation and noted that it planned to issue a strategy over the next 6 months that covers activities for the next 5 to 10 years based on near term lessons learned. OMB also identified several federal activities planned in the short term to address security issues in cloud computing.

GSA Has Established Program Office and Cloud Computing Storefront, but Has Not Yet Developed Plans for a Shared Assessment and Authorization Process

GSA has established the Cloud Computing Program Management Office that manages several cloud computing activities within GSA and provides administrative support for cloud computing efforts by the Federal Chief Information Officers (CIO) Council. Specifically, the program office manages a storefront, www.apps.gov, established by GSA to provide a central location where federal customers can purchase software as a service cloud computing applications. GSA has also initiated a procurement to expand the storefront by adding infrastructure as a service cloud computing offerings such as storage, virtual machines, and Web hosting.

Establishing both an assessment and authorization process for customers of these services and a clear division of security responsibilities will help ensure that these services, when purchased and effectively implemented, protect sensitive federal information. GSA officials stated that they need to work with vendors after a new procurement has been completed to develop a shared assessment and authorization process, but have not yet developed specific plans to do so. Accordingly, we recommended that GSA ensure that full consideration is given to the information security challenges of cloud computing, including a need for a shared assessment and authorization process as part of their procurement for infrastructure as a service cloud computing technologies. GSA agreed and identified plans for ensuring issues such as a shared assessment and authorization process would be addressed.

Federal CIO Council Has Established Cloud Computing Executive Steering Committee but Has Not Finalized Key Process or Guidance

The Federal CIO Council established the Cloud Computing Executive Steering Committee to promote the use of cloud computing in the federal government. Under this committee, the security subgroup has developed the Federal Risk and Authorization Management Program, which is a governmentwide program to provide joint authorizations and continuous security monitoring services for all federal agencies, with an initial focus on cloud computing.

The subgroup is currently working with its members to define interagency security requirements for cloud systems and services and related information security controls. However, a deadline for completing development and implementation of a shared assessment and authorization process has not been established. We recommended that OMB direct the CIO Council Cloud Computing Executive Steering Committee to develop a plan, including milestones, for completing a governmentwide security assessment and authorization process for cloud services. OMB agreed and identified current activities of the CIO Council which are intended to address the recommendation.

NIST Is Coordinating Activities with CIO Council but Has Not Established Cloud-Specific Guidance

NIST is responsible for establishing information security guidance for federal agencies to support FISMA; however, it has not yet established guidance specific to cloud computing or to information security issues specific to cloud computing, such as portability and interoperability, and virtualization.

The NIST official leading the institute's cloud computing activities stated that existing NIST guidance in SP 800-53 and other publications applies to cloud computing and can be tailored to the information security issues specific to cloud computing. However, both federal and private sector officials have made clear that existing guidance is not sufficient. Accordingly, we recommended that NIST issue cloud computing guidance to federal agencies to more fully address key cloud computing domain areas that are lacking in SP 800-53 areas such as virtualization, and portability and interoperability, and include a process for defining roles and responsibilities of cloud computing service providers and customers. NIST officials agreed and stated that the institute is planning to issue guidance on cloud computing and virtualization this year.

In summary, the adoption of cloud computing has the potential to provide benefits to federal agencies; however, it can also create numerous information security risks. Federal agencies have taken steps to address cloud computing security, but many have not developed corresponding guidance. OMB has initiated a federal cloud computing initiative, but has not yet developed a strategy that addresses the information security issues related to cloud computing, and guidance from NIST to ensure information security is insufficient. While the Federal CIO Council is developing a shared assessment and authorization process, which could help foster adoption of cloud computing, this process remains incomplete, and GSA has yet to develop plans for a shared assessment and authorization process for its procurement of cloud computing infrastructure as a service offerings. Until federal guidance and processes that specifically address information security for cloud computing are developed, agencies may be hesitant to implement cloud computing, and those programs that have been implemented may not have effective information security controls in place.

Chairman Towns, Chairwoman Watson, and Members of the Committee and Subcommittee, this concludes my prepared statement. I would be pleased to respond to any questions.

For questions about this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Individuals making key contributions to this testimony included Season Dietrich, Vijay D'Souza, Nancy Glover, and Shaunyce Wallace.

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 Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to 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 Web site, 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.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Web site: www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Ralph Dawn, Managing Director, dawnr@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 TOWNS. Thank you very much.

Let me just announce to the Members that there are three votes, and what I would suggest is that we break now and then come back 10 minutes after the last vote. The witnesses, of course, need to stay in the area. Thank you very much. It will at least be half an hour or more before we get back.

So we will recess.

[Recess.]

Chairman TOWNS. The meeting will reconvene.

Let me again apologize, but we have to vote around here. And if you don't vote, they put your name in the newspaper.

Let me begin with, I guess, this question probably to you, Mr. Kundra and to Mr. McClure. It seems to me that the shift to cloud computing will move a lot of responsibility that we currently maintain in-house to contractors. What impact will that move have on the Federal IT work force? Will we lose a lot of jobs as a result of this?

Mr. KUNDRA. If I can step back for a second and look at the current environment that we are in. For example, based on the FISMA report of last year, there are over 4,000 systems in the U.S. Government that are maintained by contractors. Just to give you examples of that, with the Navy, their network infrastructure, over 300,000 desktops are maintained and operated by EDS/HP. Our travel system in the U.S. Government, for example, Northrop Grumman actually manages that infrastructure.

So I want to be really careful as we talk about cloud computing in terms of how we treat it versus other IT systems. Like any technology, part of what we are trying to do is make sure that, as we move toward a cloud, that what Federal employees are doing, they are armed in training and that we are focusing on work, as I highlighted on my earlier slide in my opening testimony, that serves the American people. And what I mean by that is making sure that there is appropriate training, a path to actually fundamentally reengineering the functions of those agencies.

But cloud computing is not something that is going to change the way, in terms of the procurement side of it, because what we are already doing is we have already engaged in the last 10, 20, 30 years in a lot of outsource systems, and this is just another area that we are applying security and standards to.

Mr. MCCLURE. Yes, Mr. Chairman, I think it is a good question in terms of the work force impact. As you know, a lot of Federal IT spending is on infrastructure, and as we free up some of the personnel that are actually dedicated to maintenance of legacy systems and infrastructure, you can move them to more high value job categories and into analytical categories for the information.

I will just draw on my own experience with USA.gov. That was heavily dependent upon a staff that was engaged in day-to-day operations and maintenance activities, the updates, the patches, and so forth. By moving it to a cloud environment, we freed up those people to actually focus more of their time on applications for true business needs and high-value security functions.

So that is the fundamental shift that could occur here, is that we are actually enabling an IT work force in the Government to be more focused and more targeted on high-value needs that we have.

Chairman TOWNS. Thank you very much.

Let me say this to you, Mr. Wilshusen. It seems clear to me that there are certain things that should never be placed in the cloud, particularly classified or maybe even sensitive information, because it is simply not worth the risk, I don't think. Do you agree?

Mr. WILSHUSEN. I would say that there are certain applications and information in which it would probably perhaps be imprudent to put in a cloud, but it really depends on what type of cloud is being used, whether it is a private cloud, perhaps, behind an agency's firewalls; and specifically what types of controls and the effectiveness of those controls that are placed over the systems operating in that particular cloud.

It is important to remember that the individual systems that are being used, even in the traditional sense now at many agencies, we have reported over years that many of them are not that secure in and of themselves, and it really gets down to assuring that the security controls over the systems that are processing the information are effective and protecting the information, be it classified information, be it unclassified or sensitive information, to a level that is required.

But I would say that, certainly, what agencies are doing now are kind of taking a go slow approach in terms of limiting the type of information that they are putting in the cloud implementations that they are presently using. Most agencies that we looked at using this kind of low-impact or low-sensitivity information for those clouds which may particularly be in a public cloud.

And even in the private clouds they are still using, for the most part, low-impact information until they work out the issues related to adequately securing that information. Indeed, one of the risks that we have identified with our report is the fact that it may be difficult for agencies to currently assess the security and risk over the cloud implementations that are available.

Chairman TOWNS. Thank you very much. I see my time has expired.

The gentleman from Utah, Mr. Chaffetz.

Mr. CHAFFETZ. Thank you.

Thank you all for being here. It is very encouraging to see the presentations; it makes immense sense, particularly Mr. Kundra. I appreciate that.

How do you get everybody moving in the same direction, though? I mean, you just know the discussion is going to happen. You are going to go over to the Bureau of Indian Affairs and they are going to say, oh, but you don't understand this and, oh, we have all this safety and security, and we have to have our own proprietary system. How do you standardize, how do you push them?

Because I think we would probably all sit down and say we need a unified way to move forward, but the reality is that is why we end up with the thousands of different legacy systems that we have. How do you do that? I don't have a solution to that.

Mr. KUNDRA. Part of the way that we are addressing that challenge is grounded in the budgeting process, so it is part of the fiscal year 2012 budget process. What agencies are doing is they are actually developing plans to consolidate infrastructure, to consolidate data centers, and that activity is vital as we think about where

does it make sense for us to continue to invest in infrastructure versus where are there opportunities to move to the cloud in a safe and secure manner.

Second thing is the program management office that we have stood up at GSA, where that is a center of gravity with the leadership that is being provided from an execution perspective.

Third is making sure, with the Federal CIO Council, that we create the appropriate economic incentives. And what I mean by that is consider what it takes right now for any vendor to actually get certified to sell to the U.S. Government. Well, you have such a high barrier for entry because you have to get certified. If you are dealing with CDC, NIH, or if you are dealing with the FBI, and then you have to go deal with GSA. That is very difficult because the economics or the economies of scale don't work out.

So, from a security perspective, one of the things we are doing in cloud computing is we have launched the FedRAMP program, where we are going to create a certification board made up of members from the Department of Defense, Department of Homeland Security, from GSA, and an agency that actually wants to procure that technology, so that you go through that certification, but you don't just stop there; you move toward a continuous monitoring environment so you are not just generating paperwork reports from a security perspective.

Mr. CHAFFETZ. But is the idea that if you meet that minimum standard that would suffice for, say, some of these that truly do warrant more sophisticated security type applications, that if you meet that standard, that all the rest of the agencies would fall into line? Is that the idea?

Mr. KUNDRA. Absolutely. They will be able to then leverage the work that has been done across the Federal Government. To give you a simple example, the State Department, over the last 6 years, has spent $138 million on these paperwork exercises as far as certification and accreditation is concerned, and that is multiplied across the board with multiple agencies and departments.

What we are trying to do is move away from this environment of just generating paperwork reports and much more toward continuous monitoring, and that is an area that NIST has been spending a lot of energy in terms of how do we get realtime data on the security of the systems, rather than just reports.

Mr. CHAFFETZ. Some of the business models that we see out there that use kind of a version of cloud computing, if you will, are reliant upon those eyeballs and then selling those eyeballs, in essence, in an advertising manner to be able to say, oh, well, we can supplement it. It is free as long as you use it, but we are going to sell some advertising against it.

Is there a standard that you have thought through on how that would work or not work? Because the sensitivity of who is looking at that information, selling of advertising, those types of things may look appetizing to kind of defray the cost, but there are also some security issues on the companies taking that information and then, in essence, packaging it up to an advertiser. Have you thought through how that works or won't work?

Mr. KUNDRA. If we look at the Recovery Board and its move to the cloud when it comes to Recovery.gov, they went through those

issues, and part of what they did was, as they were negotiating the contract. And that is why I want to be careful as we think about the move to the cloud not being something that is brand new, that has never happened. It is essentially contracting.

As I mentioned, we are moving toward contracting systems, whether we are dealing with Lockheed Martin, Raytheon, or a number of other companies. In the same way, Recovery actually said, you know what, with the cloud vendor, the data must in the United States and here are a set of prerequisite solutions. And, frankly, they have to comply with Federal statutes such as FISMA and security guidance that has come out of OMB and NIST.

Mr. CHAFFETZ. Well, Mr. Chairman, I know my time is short, but I am fascinated to continue on in having these further discussions, because my guess is, and it is just a guess, but is that the law is woefully behind in terms of the velocity and the speed in which these types of applications change. It is just the nature of the beast.

We will have to be vigilant on that, but I appreciate the hearing today. Thanks for your input.

Thank you, Mr. Chairman.

Chairman TOWNS. Thank you very much.

I now yield 5 minutes to the gentlewoman from California.

Ms. CHU. Thank you, Mr. Chair.

I would like to ask the panel concerns about the current electronic privacy laws as we head toward this cloud computing. Specifically, commentators have raised concerns about the Electronic Communications Privacy Act and that it hasn't changed in nearly 25 years.

I am also on the Judiciary Committee, and we had a hearing on the fact that information in the clouds in large part is not protected by privacy laws; whereas, information in written communication is protected by the privacy laws. Basically, we have not changed these laws in these 25 years to accommodate this.

So, looking ahead, what steps should Congress take to ensure that the privacy of both individual information and Government records is maintained?

Mr. MCCLURE. I think that is a great question. There are two directives that were issued by the OMB Director last Friday dealing with this issue of protection of personal identification information on third-party sites, which are largely where a lot of SAS cloud applications are being used; and those issues were reinforced by the policy that the protection of personal identifiable information is in place, that agencies have to take steps to ensure that is occurring. And if there is personal identification information collected, that it is specifically explained and posted why it is being collected and what it is being used for.

So I think what we are doing in the policy area is actually bringing up some of the older policies for inspection and looking at ways in which we can modernize them in this environment but still offer security and privacy protections that are fundamental to the data needs of the Government.

Ms. CHU. And are there specific laws that you think need to be changed and updated?

Mr. MCCLURE. I think that the next step will be to open up and look at some of the laws. We are trying to look at the directive and guidance that can come out of the administration, out of the executive branch, because that is normally how agencies implement the basic fundamentals of the laws themselves. So step one, I think, is can we get greater velocity and movement in what these changes need to be, and then I think, longer term, we can open up some of the statutes.

Ms. CHU. Then next let me ask about security concerns. I believe, in testimony this morning, Mr. Bradshaw from Google will argue that the cloud can provide better information security than current legacy systems and, in particular, that the ability of agencies to store information in the cloud, instead of on personal computers, will actually allow for improved security. What do you think about this argument?

Mr. KUNDRA. Well, I think when it comes to security, we need to remain ever-vigilant. Whether that is security in our mobile security or whether that is on systems that are Government-owned and operated or it is in an cloud environment. I don't think there is one answer that fits every single imaginable implementation of these technology solutions.

That is one of the reasons President Obama, after coming into office, quickly issued a directive to his Homeland Security Council and National Security Council to do a bottom-up review of cybersecurity. That is one of the reasons we have focused on investing over $3.6 billion in a comprehensive national cybersecurity initiative and that is one of the other reasons what we have done is looked at our cyber posture and have said, look, we really need to move away from these paperwork exercises and to realtime monitoring of how these systems are implemented.

It used to be that you could literally come in and certify a system, and then come back 3 years later, which was the policy that was actually in place, and figure out whether it was still secure or not. But we have shifted that by guidance that we issued that moves us to more of a realtime monitoring approach where DHS, working with agencies, is going to make sure not only do we have continuous monitoring, but also investments in red teams that would actually look at our own systems to figure out if we have vulnerabilities or not.

The days of just writing a report and hoping things are secure are over. We are confronting attacks on a real-time basis; therefore, we must confront them with realtime monitoring on a continuous basis. And NIST has actually been doing some really good work in the space from a framework perspective.

Ms. FURLANI. Agreed. The risk management framework defines ways to assess risk so that the program officials can actually make those decisions with the facts in front of them.

Ms. CHU. So you are saying basically there would be better oversight, you would be monitoring this. But is there something inherent in the system that would make it more secure? For instance, would the information be fragmented in various locations?

Mr. KUNDRA. Broadly speaking, when you are able to concentrate compute power in one place, you are inherently managing one system, rather than managing hundreds and hundreds of systems and

trying to get firewalls in place, making sure that you are getting realtime traps of what is going on in servers and routers and switches.

So you can make that argument, but in my view there needs to be a more fundamental shift, which is the cloud is not such a special technology, necessarily, that it is exempt from a security perspective, but it is just another implementation of IT and it is a natural evolution of where we have come from.

Congressman Issa very well articulated sort of the historical evolution of where we have ended up in terms of cloud, but there are three big things that have happened. No. 1 is bandwidth, the ability to have access to bandwidth in ways that were not available before. No. 2 is processing power; Moore's Law and the ability to have processing power in ways that were not available before.

And No. 3 is storage, and the cost of storage has gone down exponentially. Therefore, now you are able to provide services in a centralized fashion that you couldn't before. But you still have to take the appropriate security safeguards. That is one of the reasons we have charged NIST with making sure that we are convening the right folks and that agencies have to comply with current statutes and security policy.

Mr. WILSHUSEN. And if I may add, getting to the central question, is it more secure in a cloud versus in agency legacy systems, as I mentioned before, it really gets down to how security is implemented over those systems. Certainly we have reported in the past that agency legacy systems have had significant weaknesses in them.

But there are some very real risks associated with putting information out in the cloud, particularly if they are public clouds. To the extent that agencies will now have to rely on the security of the service providers and have mechanisms in place to assure that those providers are adequately securing the information that they are given and processing. And just because it goes out to the cloud does not necessarily make it more secure, but there are some risks associated with it going out to the cloud.

But there are possibilities where there are certain control elements that can help security over this data, but at the same time it gets back again to making sure there is verifiable implementation of effective security that is over those systems.

Chairman TOWNS. The gentlewoman's time has expired.

I now yield 5 minutes to the ranking member of the committee, the gentleman from California, Congressman Issa.

Mr. ISSA. Thank you, Mr. Chairman.

I am going to pick up right where you left off. I am going to ask a leading question. Let's say I am the labs, the Department of Energy labs, and I have five sites. If those sites have a firewall and access to everybody inside to the Internet, and I take all five sites and I take all the assets that are inside, behind the firewall, and I move them to a private cloud, I move them to one, two, or three sites out on the Internet, and I make a VPN connection with them and I make all traffic to and from, no independent traffic, so it all goes there. And then from those locations, through those firewalls that are maintained, I can also go out and surf the Web.

So I am not taking away any result, but I am simply moving everything to where your communication is simply to one or more locations, and then from there they are centrally located. Isn't it true I haven't changed anything at all? Assuming these are exactly the same assets, just moved, I haven't changed a thing; they are neither any more nor less secure as a result.

Mr. WILSHUSEN. As long as the same set of security controls are implemented over the information.

Mr. ISSA. OK. So, as a baseline, I think you could all agree that, as long as you have an Internet portal, location out of that portal to some other location, if nothing else changes, makes no difference at all; it is neither more secure nor less secure.

Mr. WILSHUSEN. As long as your Internet Web portal is securely configured and secure.

Mr. ISSA. Right. Well, you are only as secure as your firewall to begin with. So now going over and looking at GSA and Mr. Kundra, let's look at it another way. The bureaucracy. Every site, including the Congress, that is Internet access capable out of our firewalls, in other words, they are not closed systems, they are open to the Web, we could take every one of them and we could move them to Northern Canada so that we wouldn't have to worry about cooling year-round.

And as long as we had the bandwidth, we would have changed nothing, isn't that right? Now, we are making the assumption. We are not going to cloud computing, we are just moving our data centers 500 milliseconds of latency time away, but we are moving them. Anyone disagree that we are changing nothing?

[No response.]

Mr. ISSA. OK. So going back to those old systems of where we had a 1200 baud connection to some mainframe and we were going back and forth, the only thing that has really changed from those old systems in that situation is bandwidth; and bandwidth is no longer a limiting factor, right?

Mr. KUNDRA. Yes. But, I mean, there are a lot more as far as cloud is concerned.

Mr. ISSA. OK. Now we want to get to being able to distribute our load, balance our load among more than one, but maybe hundreds or thousands of computing so that we get economies that we could not otherwise get and the ability to have surge without having, as you said, the Government solution that we had with Cash for Clunkers, being you have to buy more PCs all the time. We want to have that in place, right?

So I am going to look at GSA and I am going to say why aren't you here today saying $80 billion, we would like $1 billion to put up resources that would be available to new requirements and to those who wanted to move from where we are to there, where that, in a sense, you would be saying, look, we are not going to worry about your budget, we are going to worry about proving that we can take $1 billion and get what used to be $2 billion, but get it better, faster, and more reliable.

Why are we not talking about a top-down implementation rather than the opening statement that, sadly, I heard where we talked about 500 people going to a big convention and trying to get buy-in? Five hundred people trying to get buy-in is what we were here

a couple weeks ago talking about when we find that agencies, years after the GSA provides better, faster, cheaper solutions for Internet and telephone access, we find that we don't have them because the bureaucracy is slow, because they have their systems, because something as simple as is it safer or less safe?

If the GSA took $1 billion and said we are going to contract a world-class private cloud in which all the vendors have locked doors and separate everything, but we are going to prove that it still is better, cheaper, faster, and provides that, and we are going to make it available to innovative projects or to innovative people that are already wanting to move from owning to simply having, why is it that is not what we are here today talking about? Because, otherwise, I fear that it will be 10 years from now, and even though you will have created the opportunity, the buy-in will be slow in coming.

Mr. MCCLURE. Well, Congressman, I think we are moving pretty aggressively in that area. We already, on our Apps.gov store site, have softwares of service solutions available Government-wide that provide economies of scale. We just closed yesterday an infrastructure as a service blanket purchase agreement offering that should be able to leverage cloud-based infrastructure purchasing Government-wide. So those vehicles, I think, we are rapidly putting in place to allow the economies of scale to actually work.

Mr. ISSA. But each agency is going to have to make those individual decisions, all the things we are hearing that slow the process down.

Mr. MCCLURE. Exactly, except, remember, what we have been talking about this morning also is a Government-wide certification process for the security of these infrastructure offerings, which is quite different from the way we have operated in the past. So an agency could get on our BPA, actually choose one of the vendors, but then each agency would go through its own certification, testing, and control processing.

That is where the process has gotten very inefficient. If we can successfully stand up a FedRAMP process that allows a consensus to be built around the testing and controls being accepted by all parties, or if there is a variation that only the incremental testing is needed, not reinvention of it, we have moved the ball, I think, considerably down the path much further than we have previously.

We also have several pilots. I think one of the other things we have to do—the question earlier was the bureaucracy not accepting this. So we have pilots underway to show proof of concept in these cloud arrangements that I think can also move the needle further down the road by actually showing where these successes are, that security is in place and that cost-savings are being produced. It is, show me, I am from Missouri, and I think that is a valid concern. That is why we are working collaboratively in the E-Gov area to show some of these pilots and their merits.

Mr. ISSA. Thank you.

Mr. Chairman, I might just note that although GSA doesn't control it directly, House Administration does, that you and I are part of a grand experiment where 540 servers in our individual offices are being moved to 540 virtual ones with no cloud capability, simply relocated. So as I went through that painful example of if you

took everything and just moved it somewhere, but didn't get any of the benefits of the cloud, you wouldn't have changed anything, that is what we are doing in Congress.

Chairman TOWNS. Right.

Mr. ISSA. Thank you, Mr. Chairman.

Chairman TOWNS. You are right.

I yield 5 minutes to the gentlewoman from California, Ms. Watson, who has been very involved in this issue.

Ms. WATSON. Thank you so much, Mr. Chairman. I am so glad that we are working in conjunction with the full committee because we have been looking at procurement, and we want to take a deeper look, and I want to continue to restate the purpose for today's hearing: to look at the benefits and the risks of the Federal Government's use of the cloud computing services. So, if you don't mind, I will read my statement, my opening statement.

Chairman TOWNS. Without objection, so ordered.

Ms. WATSON. At its basic level, the term "cloud computing" is a metaphor for Internet-based computing. Some have described it as a new name for an old concept: the delivery of computing services from a remote location, similar to the way electricity and other utilities are provided to most customers. A preponderance of technology experts believe that by 2020 most people will access software applications online and share and retrieve information through the use of remote server networks. This is a dramatic departure from today's environment where we depend on software housed on individual computers.

The use of cloud computing by Federal agencies has significant benefits for collaboration across a broad information infrastructure, as well as for reducing costs associated with long-term information technology investments. It holds out the promise of enabling IT assets to remain on the technological cutting edge over their life cycle at reduced costs.

It is therefore appropriate that President Obama has targeted the Federal Government's IT infrastructure as part of his mandate to cut agency budgets by 5 percent in 2011, particularly when we consider that the Federal Government spends $76 billion annually on IT investments and that the majority of those investments are for software and IT services.

Despite these benefits, we remain concerned with potential or unknown security risks associated with cloud computing across the Federal agency community. For example, Federal customers may become dependent on their cloud computing vendor's effective implementation of security practices or protocols for ensuring the integrity and reliability of agency data and applications.

The cloud computing model also raises privacy issues, as well as the level of control over data, due to issues of portability across different platforms or the fact that vendors may not be willing to divulge proprietary information.

Due to these concerns, in July 2009, I requested that the GAO evaluate the technical and security risks associated with cloud computing across the Federal Government. I am pleased to announce that GAO is releasing the report at the hearing today, and you probably have heard some of them in my absence. Mr. Greg

Wilshusen, who was just reporting when we recessed, was relaying some of the findings.

The GAO report notes that while individual agencies have identified security measures needed when using cloud computing, they have not always developed corresponding guidance, and that OMB and GSA have yet to complete Government-wide cloud computing security initiatives. Overall, I believe the report makes the point that cloud computing has both advantages as well as disadvantages, Mr. Chairman, with respect to cybersecurity and that the administration should move deliberatively and with caution in considering when or when not to use cloud computing platforms.

Concerns involving vendor cybersecurity have not arisen in a vacuum or in an ad hoc manner. Specifically, we know, through reporting done in the Wall Street Journal and other publications, that multiple technology and industrial base companies, including Google, have been compromised by cyberattacks believed to be sourced from the People's Republic of China. It has subsequently been reported that both the Federal Bureau of Investigation and the National Security Agency have examined these episodes to determine their origins and the extent of damages sustained by all parties.

Cyberattacks place personal data, intellectual property, and our national security at grave risk, and require our partners in the Government contractor community to be ever-vigilant in securing those systems and infrastructures used to service both Federal agencies and private citizens alike.

While I understand the aforementioned incidents may not be appropriate for discussion in an open hearing, Mr. Chairman, I believe our vendor panelists need to address the broader issue of how they plan on meeting Federal information security standards for protecting those programs and Federal data that may be hosted through their cloud services.

[The prepared statement of Hon. Diane E. Watson follows:]

Chairwoman Diane E. Watson – Opening Statement
Joint Oversight Hearing on "Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud"
July 1, 2010

Thank you Mr. Chairman for agreeing to hold today's hearing in conjunction with the Subcommittee on Government Management, Organization and Procurement on the benefits and risks of the federal government's use of cloud computing services.

At its most basic level the term "cloud computing" is a metaphor for internet-based computing. Some have described it as a new name for an old concept: the delivery of computing services from a remote location, similar to the way electricity and other utilities are provided to most customers. A preponderance of technology experts believe that by 2020 most people will access software applications online and share and retrieve information through the use of remote server networks. This is a dramatic departure from today's environment where we depend on software housed on individual computers.

The use of cloud computing by federal agencies has significant benefits for collaboration across a broad information infrastructure, as well as for reducing costs associated with long-term information technology investments. It holds out the promise of enabling IT assets to remain on the technological cutting edge over their life cycle at reduced costs. It is therefore appropriate that President Obama has targeted the federal government's IT infrastructure as part of his mandate to cut agency budgets by 5 percent in 2011, particularly when we consider that the federal government spends $76 billion annually on

IT investments and that the majority of those investments are targeted for the purchase of software and services.

Despite these benefits, I remain concerned with potential or unknown security risks associated with cloud computing across the federal agency community. For example, federal customers may become dependent on their cloud computing vendor's effective implementation of security practices or protocols for ensuring the integrity and reliability of agency data and applications. The cloud computing model also raises privacy issues as well as the level of control over data due to issues of portability across different platforms or the fact that vendors may not be willing to divulge proprietary information.

Due to these concerns, in July 2009, I requested that the GAO evaluate the technical and security risks associated with cloud computing across the federal government. I am pleased to announce that GAO is releasing the report at today's hearing and that Mr. Greg Wilshusen will be reporting on GAO's findings.

The GAO report notes that while individual agencies have identified security measures needed when using cloud computing, they have not always developed corresponding guidance, and that OMB and GSA have yet to complete government-wide cloud computing security initiatives. Overall, I believe the report makes the point that cloud computing has both advantages as well as disadvantages with respect to cybersecurity and that the Administration should move deliberatively and with caution in considering when or when not to use cloud computing platforms.

Concerns involving vendor cybersecurity have not arisen in a vacuum or in an ad hoc manner. Specifically, we know through reporting done in *The Wall Street Journal* and other publications that multiple technology and industrial base companies, including Google, have been compromised by cyberattacks believed to be sourced from the People's Republic of China. It has subsequently been reported that both the Federal Bureau of Investigation and the National Security Agency have examined these episodes to determine their origins and the extent of damages sustained by all parties.

Cyberattacks place personal data, intellectual property, and our national security at grave risk, and require our partners in the government contractor community to be ever-vigilant in securing those systems and infrastructures used to service both federal agencies and private citizens alike. While I understand the aforementioned incidents may not be appropriate for discussion in an open hearing, I believe our vendor panelists need to address the broader issue of how they plan on meeting federal information security standards for protecting those programs and federal data that may be hosted through their cloud services. I look forward to hearing their specific plans of actions to do so.

Mr. Chairman, once again I thank you for holding this hearing. I look forward to the testimony of our distinguished panels of witnesses and learning more about this important strategy to achieve efficient and effective IT.

Ms. WATSON. I really needed to be here full-time to hear what the panelists have said, but if I might take a few minutes to raise a question, I would appreciate the time.

Chairman TOWNS. Let me suggest to the gentlelady that what I will do is recognize Mr. Luetkemeyer and then come back to you.

Ms. WATSON. All right. That is fine. Thank you, Mr. Chairman. I yield back.

Chairman TOWNS. I recognize Mr. Luetkemeyer from Missouri.

Mr. LUETKEMEYER. Thank you, Mr. Chairman. I was under the impression that statements like that normally were submitted for the record, but I guess it is proper to read the entire thing.

Chairman TOWNS. If you have a statement, you can read it.

Mr. LUETKEMEYER. I am sorry?

Chairman TOWNS. If you have a statement, you can read it.

Mr. LUETKEMEYER. I think that these gentleman probably have more to do than listen to my statement, so I would be glad to submit it for the record. Thank you, sir.

Mr. Wilshusen, I am just kind of curious. What percentage of the Government's different duties and agencies do you think would be appropriate to put the cloud type of computing in place?

Mr. WILSHUSEN. Well, I don't know if I can really state what percentage of systems should be placed in the cloud; I think it really depends upon what each agency feels would be best for its interest to go to a cloud environment. Certainly, in doing that, there are a number of benefits that come by placing systems and information out into a cloud. I think some of the other panelists have talked about those benefits. But they also have to weigh the risk in doing that. But I really couldn't hazard a guess as to what percentage of systems should be placed in a cloud.

Mr. LUETKEMEYER. Who approves the move to go to the cloud type of computing, is that something that there is a congressional committee that oversees this or is it just your department or various agencies? Who has the authority to make a decision like this, to dump everybody's information to a cloud?

Mr. WILSHUSEN. Oh, I think that would probably be up to the individual agencies, but perhaps Mr. Kundra might be better able to answer that.

Mr. LUETKEMEYER. OK. Mr. Kundra.

Mr. KUNDRA. It is like any other IT system, it would be the Chief Information Officer of the agency and the Chief Information Security Officer to make sure that, before moving any system to the cloud, that, one, they have made sure they have taken into account all the statutory requirements; two, all the policy guidance around privacy and security that have existed for many years.

Mr. LUETKEMEYER. I know that there are a couple of agencies and different groups that already use the cloud type of computing in our Government. Do you know how many? And are there other companies, other States, other countries that have gone to this type of computing that we can look at as models? Just kind of elaborate on that a little bit.

Mr. KUNDRA. Sure. What I would love to do is share with you a report we put together where we have highlighted illustrative case studies, whether that is at a State level, local level, and even within the Federal Government.

But just to give you one example, GSA, as part of the Open Government Directive, when every agency had to engage within 45 days to get input from the American people, what GSA did was it provided a cloud solution, and they went through the appropriate security protocols. Instead of every agency having to go out there and build a proprietary system, they were able to leverage this cloud solutions and agencies, instead, focused actually on the content of how they were going to interact with the American people, how they were going to process that input, rather than standing up yet another set of data centers or servers.

Mr. LUETKEMEYER. In your testimony you indicate that the administration announced three actions this week. The first one was to take under review troubled IT projects across the Federal Government and identify serious problems. Can you identify some of the serious problems and how this cloud computing would impact those? Would that be something that would work with this situation or are they problems that are beyond this type of solution?

Mr. KUNDRA. Well, I think they are larger problems in Federal IT. So as we look at the fiscal year 2012 budget, the President has called for a freeze on non-defense natural security spending and also the 5 percent cut that agencies have to meet, and one of the ways agencies are going to be able to make sure that they are still delivering services effectively is through investments and information technology.

Mr. LUETKEMEYER. Well, what are some of the serious problems? Is the cut you identified a serious problem?

Mr. KUNDRA. No. What we want to make sure is that taxpayer money is being spent well, so some of these serious problems, the example I gave——

Mr. LUETKEMEYER. Identify a serious problem for me. I am just curious as to what the problems were that have been identified.

Mr. KUNDRA. Procurement cycles, for example, that may take 18 months or problems around the Government scoping IT projects with deliverables that take 2, 3, 4 years. And we have seen best practices where, at the local, State level, or even the private sector, where buyers are saying, look, you have to deliver value in 6 months, not 3 years from today.

We have also seen problems in terms of how some of these systems are actually scoped, overly prescribing requirements that will end up in failure as a result of everything being overly specified.

Mr. LUETKEMEYER. OK, so basically the problems you identified there were problems of process and procedure versus something to be solved with the cloud, is that correct?

Mr. KUNDRA. Right. Well, cloud is a technology, by no means a silver bullet that is going to solve all the IT problems we have. It is one approach, it is not the answer to everything that is wrong with Federal IT.

Mr. LUETKEMEYER. All right. Thank you.

Thank you, Mr. Chairman.

Chairman TOWNS. I thank the gentleman from Missouri.

I now yield to the gentlewoman from California 5 minutes.

Ms. WATSON. Thank you so much, Mr. Chairman.

Cost saving estimates for the Federal Government derived from the use of cloud computing very greatly, anywhere from 25 percent

to above 90 percent in savings. The wide range in cost estimates is in part due to the fact that cloud computing is still evolving, and savings are dependent on the type of cloud platform that is deployed.

The required level of security is also an unknown variable. What other valuables should we take into account in measuring potential savings from cloud computing and what cost savings estimate can we reasonably expect? And let's start with Mr. Kundra and then go right down the panelists.

Mr. KUNDRA. Sure. So from a savings perspective it is very much around the problem you are trying to solve. And what I mean by that is when Recovery.gov moved to the cloud, they saved $750,000 on an annual basis, which is very different than what GSA did when they moved USA.gov to the cloud; I believe it was $1.7 million is what GSA saved. But in some cases it may end up costing more because of security requirements that would have to be implemented. So I don't think there is a single number that is going to lead to these savings.

Ms. WATSON. It is a range.

Mr. KUNDRA. Well, even within the range that is why you see such a wide, in terms of degrees of freedom, from 25 to 99 percent, or whatever the number is. For example, with the Open Government Directive, that was a nominal cost to provide a platform for every single agency to engage the American people. We didn't have to go out there and spend millions of dollars and engage in a multiyear contract. So there is also a lot of cost avoidance as a result of leveraging these cloud solutions.

And as we look forward, part of what we are doing is we are making sure we recognize that the power here, when we talk about cloud computing, is it is also greener from a computing perspective, because you don't have to go out there and keep building data center after data center. I mentioned earlier in my testimony how we have gone from over 400 data centers to over 1,100 in a 10-year period; whereas, in the private sector we have seen a move toward consolidation.

So it is greener in terms of making sure that we are leveraging these assets more effectively, and also provides better customer service. Those are the other benefits. The example I used around Cash for Clunkers, where we had challenges around the system not being able to stay online because demand was so high, versus a private sector company that leveraged a cloud solution that kept up with demand without any failure.

Ms. WATSON. We don't want to keep our heads in the clouds. A pun is the worst form of humor.

Mr. McClure.

Mr. MCCLURE. Yes, I think that is absolutely right, what Vivek was saying. I think we have to be careful with numbers on averages being thrown around. I think the examples that we have documented in the Federal Government, if you read the report Vivek was talking about in terms of the dozens of examples of cloud computing, if it has been used for improving software development activities it is one range of cost; if we are actually saving storage cost because it is more efficient in a cloud environment is another type of savings; if we have actually saved software development money

by taking a common tool that is plug-and-play into an environment. So I think the cost savings will be dramatically different depending upon the type of application and type of cloud environment that we are putting these solutions in.

But I would agree that we shouldn't focus totally on cost. Speed, agility, the ability to move quickly into the computing environments are significantly enhanced in these cloud environments, and those are huge payoffs for service delivery to citizens.

Ms. WATSON. Ms. Furlani.

Ms. FURLANI. I think where NIST contributes to this is the standardization or the recommendations of consistency in applying the guidelines and the standards across the agencies so that these cost savings can be realized. Understanding our risk management framework, the release we just put out, an 837 updates and permits the leveraging of the certification and accreditation issues that we have mentioned; the baseline controls that Vivek has referenced, where you can actually continuously monitor security controls are actually deployed appropriately.

So what NIST contributes is this capability of standards and guidelines to provide consistency so agencies can leverage each other's capabilities more effectively and make the cost savings real.

Chairman TOWNS. Would the gentlewoman yield?

Ms. WATSON. Yes.

Chairman TOWNS. Do we really know enough to set standards?

Ms. FURLANI. That is what we are working on, to identify where the standards need to be, and that was the starting point in the workshop where we had many stakeholders come and help us understand. We have guidelines now for how IT systems should be deployed, and that was what I was referencing.

But the applicable standards in the cloud computing environment will be dependent on which model of cloud computing you are actually addressing and which kind you are trying to use for your own particular program and your own mission requirements. So it all comes back to the program official understanding the risks that are being undertaken and having guidance, which we provide, to assess that risk and make the decisions as to which standards are available and which can be monitored.

Mr. WILSHUSEN. And although we did not look at the specific cost savings and issues related to cloud computing in our report, we did discuss the need for OMB to complete a strategy on its implementation of cloud computing and initiatives across the Government, and in our report we talked about the information security issues that need to be addressed in that strategy.

But what also should probably be included in that are performance measures, particularly as they relate to cost savings; the speed, how much faster is it to obtain the resources that my other panelists here have been discussing? So certainly the need to develop performance measures, which data can be collected on, and then one can evaluate just how cost-effective and what cost savings have been acquired through the use of cloud computing.

Ms. WATSON. Mr. Chairman, I know my time is up, but I just want to say that our subcommittee will continue to look at this issue, procurement and is it a cost savings. And what I am hearing today, we have to customize this particular IT, this cloud kind of

IT for the services that you provide. I don't think one method will suit all. It is a work in progress, it is evolving, so we are going to keep tabs on it in the very near future and report back to the full committee. Thank you so much for the extra time.

Chairman TOWNS. I thank the gentlewoman for her work and what she is doing in her subcommittee.

I now yield to the gentleman from California.

Mr. ISSA. I am going to continue. I am a big fan of cloud computing, so don't have anything I say cause you to think that it is anything other than my fear of the bureaucracy that causes me to sound like we are not going to get there as quick as we would like to and I want to look at other things.

Mr. Kundra, if we simply did a move and manage, just assume for a moment that anyone who is eligible to go to the cloud, instead of going to cloud, we just move and manage, meaning, like Congress, we say we are going to take it out of all your offices, where everybody had an individual server. You have enough bandwidth or we will provide you enough bandwidth at a relatively low cost. We are going to centrally manage. We are going to, where appropriate, have multiple servers and multiple raids.

We will make those decisions, but we are providing you with an equivalent amount of processing to whatever you had, but we are going to relocate it. Literally the way they did it in Congress is they picked up your server and took it to another place, and then over time, using VMware or an equivalent, they are going to give you pieces of more powerful servers.

From a purely speed of chipping away at that $80 billion and freeing up dollars for innovation and other uses, isn't that a step that can be done today without any of the concerns that are being talked about, about the fitness of some future vendor? In other words, if you assume that each agency, unless they consent otherwise, doesn't have sharing between agencies and so on, how would you envision that as a, if you can't get what you want, would this be a step?

Mr. KUNDRA. Sure. And that is actually exactly what we are engaged in. One of the things we have done is we have looked at this problem around expenditures in information technology, and approximately $20 billion annually is spent on infrastructure. So if you take the entire $80 billion, break it down to just infrastructure spend on servers, routers, switches, networks.

Mr. ISSA. Air conditioning, backup generators, UPSes.

Mr. KUNDRA. Exactly. So the first step we are taking is to make sure that, one, across the entire Federal Government we have detailed plans as far as data center consolidation is concerned.

So that is an effort that is underway, and part of the 2012 budgeting process, what agencies have to do is make sure they come in to the budget process to say, look, what is your plan? What is your strategy? For example, Department of Homeland Security has committed to move from approximately 24 data centers down to 2. GSA has over eight data centers. And I could cite department by department.

Mr. ISSA. And they are supposed to be the example of best of, right?

Mr. KUNDRA. Well, look, we didn't get here overnight; this is a multi-decade problem. Over the last 50 years that is how the Government has been growing. In my testimony I talked about how companies like IBM have consolidated; whereas the Government continues to grow.

Mr. ISSA. Well, let me ask a question as to that. If that is the case, we here probably are the most parochial group you are going to find. We get reelected based on whether or not people believe we care about them. So it is not uncommon that we would want a data center in our district, particularly if it created good paying jobs.

Chairman TOWNS. I want two. [Laughter.]

Mr. ISSA. I would second that for the chairman.

Now, it happens that Brooklyn may not always be the best place. And I know that the electric costs in San Diego are not the lowest. So what are you, cumulatively or individually, doing to create, if you will, that best of location, best of price cost for some of these data systems, and what are you doing to ensure that GSA actually goes to zero—here me out for a second—zero data centers? Because there is no reason for you to have a unique data center that is only GSA.

You can have a unique room in a larger data center that five other agencies each have a room in. But what would be the cost-effectiveness of having your own eight at your own sites. By the way, you probably would pick sites based on the Congressmen who have the most influence on you, and I am perhaps one of them, while Homeland Security might look to Mr. King and so on other there. What are we doing to ensure that these sitings are both as consolidated as possible and as efficient as possible?

Mr. KUNDRA. And that is part——

Mr. ISSA. And as least interfered by people like us as possible.

Mr. KUNDRA. Well, one, we look forward to working with the Congress as we take on this really, really difficult problem——

Mr. ISSA. I think you are getting those two data centers.

Mr. KUNDRA [continuing]. Because you have 1,100, and what was really interesting was when we went back and looked at the data, some agencies couldn't produce that data right away in terms of where is your data center; how many servers do you have; what is your rack utilization? And what we are finding, unfortunately, is that in some agencies server utilization is actually at 7 percent. And when you think about cloud computing, that is where you have a lot of wasted capacity, because what ends up happening is everybody engineers their solution for what they expect the peak to be. Therefore, they overbuild and it ends up costing a fortune to maintain those systems.

So by this December——

Mr. ISSA. You mean like the stories that we have seen where servers are actually retired, never having been powered up, but they were bought?

Mr. KUNDRA. Right. And that is the type of waste we are taking head on, and that is why, by this December, agencies across the Federal Government have been directed by OMB to come up with road maps and plans on how they are going to consolidate. And part of what we want to make sure is that we are responsible in the consolidation, because what you don't want to do is consolidate

to one place where now everybody knows if you go after that one place, you are going to be able to bring down all of Federal IT.

So we have to figure out how do we, in this environment, where we have over 1,100—and that number may go up, by the way, because the final plans aren't due until this December—how do we make sure that there is enough geodiversity to ensure security, but at the same time that it is not so crazy that you have data centers popping up every year all over the country.

Mr. ISSA. Thank you.

Thank you, Mr. Chairman.

Chairman TOWNS. Thank you very much.

Let me thank all the witnesses for your testimony. You have been very, very helpful and I know the subcommittee will continue to work on this as well. We want to thank you for your time and, of course, the suggestions and recommendations. We look forward to working with you. Thank you very much.

Mr. KUNDRA. Thank you very much.

We would like to call up our second panel.

Mr. Scott Charney is corporate vice president of trustworthy computing at the Microsoft Corp. Welcome. Mr. Daniel Burton is senior vice president of global public policy at Salesforce.com; Mr. Mike Bradshaw is director of Google Federal; Mr. Nick Combs is chief technology officer of EMC Federal; and Gregory Ganger is professor of electrical and computer engineering, as well as director of the Parallel Data Lab at Carnegie Mellon University.

Welcome and thank you all for being here. Let me say to you that we always swear our witnesses in, so if you would stand and raise your right hands.

[Witnesses sworn.]

Chairman TOWNS. You may be seated.

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

Let me start with you, Mr. Charney, and we will just go right down the line. You know you have 5 minutes. You know how it works. After the light comes on caution, then red, and all of that, which will allow us ample time to raise questions. And you can see that we have a lot of questions. So why don't we just start with you, Mr. Charney, and come right down the line?

STATEMENTS OF SCOTT CHARNEY, CORPORATE VICE PRESIDENT, TRUSTWORTHY COMPUTING, MICROSOFT CORP.; DANIEL BURTON, SENIOR VICE PRESIDENT, GLOBAL PUBLIC POLICY, SALESFORCE.COM; MIKE BRADSHAW, DIRECTOR, GOOGLE FEDERAL, GOOGLE INC.; NICK COMBS, CHIEF TECHNOLOGY OFFICER, EMC FEDERAL; AND GREGORY GANGER, PROFESSOR, ELECTRICAL AND COMPUTER ENGINEERING, DIRECTOR, PARALLEL DATA LAB, CARNEGIE MELLON UNIVERSITY

STATEMENT OF SCOTT CHARNEY

Mr. CHARNEY. Thank you, Chairman Towns, Ranking Member Issa, Chairwoman Watson. Thank you for the opportunity to share Microsoft's view on the benefits and risks of cloud computing for the Federal Government.

My name is Scott Charney. I am the corporate vice president for trustworthy computing and environmental sustainability at Microsoft. I also serve as one of the four co-chairs for the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency. Prior to joining Microsoft, I was Chief of the Computer Crime and Intellectual Property Section at the U.S. Department of Justice.

In my testimony today, I want to describe how cloud computing impacts responsibilities for the security, privacy, and reliability of IT systems, and I want to highlight the importance of Electronic Communications Privacy Act reform and identity management issues.

While cloud computing creates new opportunities, it also presents new challenges. More specifically, a Government agency using a cloud service may shift certain security, privacy, and reliability responsibilities to the cloud provider. To ensure this is done properly, Government agencies need to clearly identify their security, privacy, and reliability requirements to the cloud provider, and cloud providers need to be transparent about the steps taken to meet those requirements.

In Microsoft's case, we employ a holistic approach in managing security, privacy, and reliability issues, an approach that is designed to meet or exceed customer requirements. This approach, which encompasses physical personnel and IT security, has three parts: first, we have a risk-based information security program that assesses and prioritizes security and operational threats to the business; second, we maintain and regularly update a detailed set of security controls to mitigate risk; third, we use a compliance framework to ensure that controls are designed appropriately and are operating effectively.

A key part of this process is the Microsoft Security Development Lifecycle [SDL], which helps to improve security and privacy protections in our software and our services. The SDL consists of processes and tools designed to reduce the number and severity of vulnerabilities in software products, manage risk in computing environments, ensure appropriate and agile response when incidents occur, and help protect people and their personal information by imposing mandatory engineering practices related to security and privacy. By building and managing resilient infrastructure with trustworthy people, we can further ensure a high availability in 24/7 support in our service level agreements.

While the cloud is getting ready for the Government, the Government must get ready for the cloud. Agencies continue to struggle to identify, manage, and account for the security of data and systems. Moving to the cloud does not eliminate an agency's responsibility for its data. To adapt to the cloud, an agency must clearly identify and communicate its requirements and expectations to the cloud provider, who, in turn, must indicate how those requirements and expectations will be met.

Progress is being made. The Federal Risk and Authorization Management Program [FedRAMP], is an important initial effort to create efficiencies and define responsibilities. This program enables common assessments of cloud service providers, allowing a cloud provider to certify once and have that certification shared among

the agencies. In addition to increased efficiencies, FedRAMP can ensure better transparency into cloud provider practices.

In addition to managing its own systems, the Government has a policy role to play. In this regard, it must ensure that privacy protections for citizens keep pace with technological changes. Congress enacted the Electronic Communications Privacy Act almost 25 years ago. Dramatic technology advancements, including the shift to cloud computing, require ECPA, as it is known, to be updated and aligned with reasonable privacy expectations. Additionally, industry and Government must create more robust identities for Internet use, particularly as we adapt to the cloud.

There are over 1.8 billion Internet users worldwide. The mechanisms used to identify people and devices on the Internet, even when sensitive data or critical infrastructures are involved, is weak. And as the Government offers more citizen services online and individuals store more sensitive information in the cloud, electronic identifications will become increasingly important. The recently released draft National Strategy for Trusted Identities in Cyberspace represents significant progress in the dialog about how to create trust in online transactions, but much remains to be done.

In closing, clarity and transparency about Government requirements and cloud provider offerings is critically important. The more precise and transparent we are, the greater the trust we will build and the greater the opportunity we create.

Thank you for your important leadership on the issue of cloud computing, and I look forward to working with you on this important topic.

[The prepared statement of Mr. Charney follows:]

Statement of Scott Charney

Corporate Vice President, Trustworthy Computing
Microsoft Corporation

Adapting to the Cloud

Testimony Before the
Committee on Oversight and Government Reform and the
Subcommittee on Government Management, Organization, and Procurement
U.S. House of Representatives

Hearing on "Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud"

July 1, 2010

Chairman Towns, Ranking Member Issa, Chairwoman Watson, Ranking Member Bilbray, Members of the Committee and Subcommittee: Thank you for inviting me here today to discuss the federal government's use of cloud computing.

My name is Scott Charney, and I am the Corporate Vice President for Trustworthy Computing at Microsoft Corporation. I also serve as one of four Co-Chairs of the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency. Prior to joining Microsoft, I was Chief of the Computer Crime and Intellectual Property Section in the Criminal Division of the United States (U.S.) Department of Justice. I was involved in nearly every major hacker prosecution in the U.S. from 1991 to 1999; worked on legislative initiatives, such as the National Information Infrastructure Protection Act that was enacted in 1996; and chaired the G8 Subgroup on High Tech Crime from its inception in 1996 until I left government service in 1999.

I currently lead Microsoft's Trustworthy Computing (TWC) group, which is responsible for ensuring that Microsoft provides a secure, private, and reliable computing experience for every computer user. Among other things, the TWC group oversees the implementation of the Security Development Lifecycle (which also includes privacy standards); investigates vulnerabilities; provides security updates through the Microsoft Security Response Center; and incorporates lessons learned to mitigate future attacks.

Microsoft plays a unique role in the cyber ecosystem by providing the software and services that support hundreds of millions of computer systems worldwide. Windows-based software is the most widely deployed platform in the world, helping consumers, enterprises, and governments to achieve their personal, business, and governance goals. Also, as Steve Ballmer, our Chief Executive Officer, stated, "we're all in" when it comes to the cloud. We already offer a host of consumer and business cloud services, including a wide array of collaboration and communications software.

We operate one of the largest online e-mail systems, with more than 360 million active Hotmail accounts in more than 30 countries/regions around the world. Microsoft's Windows Update Service provides software updates to over 600 million computers globally, and our Malicious Software Removal Tool cleans more than 450 million computers each month on average. We are a global information technology (IT) leader whose scale and experience shapes technology innovations, helps us recognize and respond to ever changing cyber threats, and allows us to describe the unique challenges facing the government as it moves to the cloud.

Cloud computing creates new opportunities for government, enterprises, and citizens, but also presents new security, privacy, and reliability challenges when assigning functional responsibility (*e.g.*, who must maintain controls) and legal accountability (*e.g.*, who is legally accountable if those controls fail). As a general rule, it is important that responsibility and accountability remain aligned; bifurcation creates a moral hazard and a legal risk because a "responsible" party may not bear the consequences for its own actions (or inaction) and the correct behavior will not be incentivized. With the need for alignment in mind, I will, throughout the rest of my testimony, use the word "responsibility" to reflect both responsibility and legal accountability. It must also be remembered that there is another type of accountability:

political accountability. Citizens have certain expectations of governments (much like customers and shareholders have certain expectations of businesses) that may exceed any formally defined legal accountability.

As a cloud provider, Microsoft is responding to security, privacy, and reliability challenges in various ways, including through its software development process, service delivery, operations, and support. In my testimony today, I will (1) characterize the cloud and describe how cloud computing impacts the responsibility of the government and cloud providers; (2) discuss the responsibilities cloud computing providers and government must fulfill individually and together; and (3) examine the importance of trust and identity to cloud computing.

New Computing Models ("The Cloud") Create New Opportunities and Risks

Many people talk about "cloud computing"— what it is, what it does, and why it matters — but it is critically important to have a common understanding of the term before discussing how it changes risk management responsibilities. "Cloud computing" permits all users to leverage Internet-based data storage, processing, and services in new ways, thus complementing the traditional model of running software and storing data on personal devices and servers. There are several key characteristics of the cloud that differ from the traditional client-server model of computing and deliver benefits for customers, including global elasticity, geo-diversity, and co-tenancy.

- Global elasticity means that customers, including governments, enterprises, and consumers, can buy the computing power, storage, and resources they need in a fast and flexible manner without committing to long-term and costly technology investments. Global elasticity provides convenient access to, and creates opportunities for, more efficient delivery of services, and it helps control costs.

- Geo-diversity enables data to be stored in multiple locations, generating efficiency and speed benefits and enhancing reliability.

- Co-tenancy means multiple users share cloud infrastructure, which can create tremendous economies of scale and cost savings.

Service Models and Accountability

The benefits of the cloud can be realized through three different service models described below:

1. Software as a Service (SaaS): The cloud provider makes available to users a single application, such as Hotmail e-mail, or multiple applications, such as Microsoft's Office Suite online.

2. Platform as a Service (PaaS): Users may choose to develop and run their own software applications, while relying on the cloud provider to provide the underlying infrastructure and operating system. Microsoft's Azure is a cloud platform that enables users and developers to write and/or run their own applications.

3. Infrastructure as a Service (IaaS): At its most basic, users rent hardware or virtualized instances of hardware — the infrastructure — to deploy and run their own operating systems and software applications.

Customers need to make informed decisions about adoption of the cloud and its various service models because the model that is embraced will entail different allocations of responsibility between the customer and the cloud provider(s). In the traditional IT model, an organization is responsible for all aspects of its data protection, from its actual use of the data to the protection of that data in its IT environment. A complete data protection program will address the physical security of the data center, the trustworthiness of data center personnel, the configuration and management of hardware and software, and the management of IDs and access controls. Cloud computing changes this. While an organization will still control the use of its data, it will need to set limits on the cloud provider's use of that data. Additionally, it may transfer to the cloud provider the responsibility for certain data center operations. For example, the customer using IaaS may transfer responsibility for data center operations, including the trustworthiness of data center personnel, to the cloud provider.

Once this is understood, it becomes clear that the different cloud service models transfer different amounts of responsibility between the customer and the cloud provider. Figure 1 illustrates these shifts for the different cloud service models.

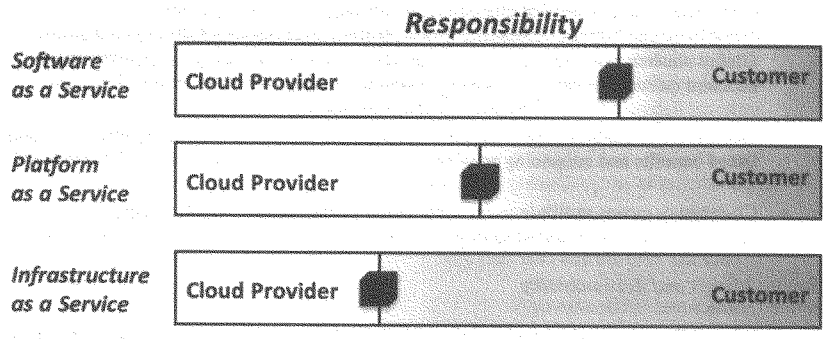


Figure 1: Shifting Responsibility in the Cloud

For example, IaaS customers maintain considerable responsibility for platform, applications, and personnel, but transfer responsibility for the infrastructure (*e.g.*, the physical data center, data center personnel, and hardware) to the cloud provider. At the other end of the spectrum, if customers utilize the entire cloud (from infrastructure to applications), they transfer yet more responsibility to cloud service providers, from physical and personnel security to the secure development and maintenance of applications and the management of identities for access control. Of course, the fact that a customer has transferred these responsibilities to the cloud

provider — and may even have transferred legal liability by contract — is not the end of the matter. For example, citizens ultimately may hold a government accountable if data is lost or stolen, or critical data is not available when needed, notwithstanding any cloud provider agreement. Thus, a government may remain "accountable" to its constituents when an incident occurs, notwithstanding any contractual apportionment of responsibility. That said, as the federal government becomes a customer of cloud services, it must be clear about its requirements — and cloud providers must be responsible for meeting those requirements.

Contracts remain, of course, the primary legal documents for aligning responsibilities, but clearly and comprehensively defining requirements for cloud services is an arduous task. As more functions are transferred to cloud providers, requirements become more critical, more challenging, and more complex. The requirements are more critical because of the scale and scope of functions and data being moved to the cloud; they are harder because this is a relatively new domain where reasonable minds may often differ; and they are more complex because specificity is necessary to ensure a common understanding of expectations between customers and providers. While many enterprises have significant experiences with outsourcing services, the integration and adoption of cloud services is an important evolution in technology adoption and integration. Defining how responsibilities for security, privacy, and reliability are allocated — and creating sufficient transparency about this allocation — represent new challenges. Both customers and cloud providers must understand their respective roles and be able to communicate compliance requirements and controls across the spectrum of services available in the cloud.

Types of Clouds

The three basic service models are generally deployed in four different ways: public clouds, private clouds, community clouds, and hybrid clouds.

- In a public cloud, the general public can access the cloud services through a multi-tenant environment.
- In a private cloud, a single organization makes use of a dedicated cloud infrastructure.
- A community cloud is a private cloud shared by a group of organizations or a community with shared concerns, missions, or interests.
- Finally, a hybrid cloud makes use of two or more cloud types, such as a private cloud and a public cloud, where each cloud remains separate, but is linked in a way that can enable data and applications to flow and communicate between the two.

Which cloud model is most appropriate depends on the nature of the IT activity. For highly sensitive information, dedicated on-premises private clouds can provide more control and security, but at a higher cost and with lower scalability, redundancy, and other benefits. In comparison, public clouds offer the greatest cost savings and likely the greatest elasticity, but at the cost of reduced control and increased risk due to co-tenancy. Hybrid clouds may provide the benefits and risks of both types.

Security, Privacy and Reliability Responsibilities in the Cloud

Regardless of the service model and type of cloud deployment selected, security, privacy, and reliability challenges must be addressed. Cloud providers and governments each have distinct responsibilities and, in some cases, shared responsibilities, as they work to help the Nation realize the benefits of cloud computing services.

Cloud providers

The importance of assuring the confidentiality, integrity, and availability of customer data and operations is not new, but cloud computing does have the effect of shifting the responsibility (in whole or in part) for these areas to cloud service providers. Providers must rise to this new reality and provide commensurate levels of assurance for their customers.

Microsoft addresses this challenge through our holistic approach for managing security, privacy, and reliability that is designed to meet or exceed customer requirements. Our approach includes three cross-cutting functions to manage physical, personnel, and IT security: (1) utilizing a risk-based information security program that assesses and prioritizes security and operational threats to the business; (2) maintaining and updating a detailed set of security controls that mitigate risk; and (3) operating a compliance framework that ensures controls are designed appropriately and are operating effectively.

Any analysis of the cloud must start with the technology that powers it. Microsoft has long recognized the importance of building secure and reliable software, and we devote considerable resources to ensuring the quality of our software, including adherence to the Security Development Lifecycle (SDL). The SDL consists of continuously evolving processes and tools designed to reduce the number and severity of vulnerabilities in software products and ensure appropriate and agile response when necessary. Importantly, in the context of discussing providers' responsibilities in the cloud, it should be noted that the SDL considers and accounts for risks related to the environment in which the application will run (*e.g.*, client computers, on-premises services, or the cloud). Thus, the SDL ensures that Microsoft cloud services are developed using secure development practices.

The SDL is not only about improving code quality; it also helps protect people and their personal information. In cases where data from multiple users is stored on the same system, there are implications for managing the transfer, storage, retrieval, and access of that data in a manner that avoids disclosure of the data to unauthorized parties. Users need to know that they can trust the software and hardware to protect their sensitive information and to isolate them from other co-tenants.

Online service providers can use a variety of technologies and procedures to help protect personal information from unauthorized access, use, or disclosure. Microsoft's software development teams apply the "PD3+C" principles, defined in the SDL, throughout the company's development and operational practices. The PD3+C principles are:

- **Privacy by Design** – Microsoft uses this principle in multiple ways during the development, release, and maintenance of applications to ensure that data collected from customers is used for specified purposes and that the customer is given appropriate notice in order to enable informed decision-making. When data to be collected is classified as highly sensitive, additional security measures — such as encrypting while in transit, at rest, or both — may be taken.

- **Privacy by Default** – Microsoft offerings ask customers for permission before collecting or transferring sensitive data. Once authorized, such data is protected using multiple means, such as access control lists (ACLs) and identity authentication mechanisms.

- **Privacy in Deployment** – Microsoft discloses privacy mechanisms to organizational customers as appropriate to allow them to establish appropriate privacy and security policies for their users.

- **Communications** – Microsoft actively engages the public through publication of privacy policies, white papers, and other documentations pertaining to privacy.[1]

Finally, cloud providers have a responsibility to provide reliable and trusted services. Reliability can be achieved through geo-diversity and redundancy in applications, data, and data centers, resiliency in communications, and high availability of services (as guaranteed in Service Level Agreements (SLAs)). Microsoft has multiple data centers located in the U.S., Europe, and Asia that meet internationally recognized standards and third party evaluations (*e.g.*, ISO 27001:2005 and SAS 70 Type I and Type II).[2] We are able to provide robust, geo-diverse services with more than 9,000 Microsoft hosting providers and more than 40% of all hosting providers worldwide using Microsoft products to support their hosting services. We also provide customers the ability to geo-locate their data, for example, ensuring that data resides only in U.S.-based servers. The integrity of cloud providers — including their personnel — is increasingly important, because the scale and scope of their actions can be exponentially increased in the cloud. Microsoft engineers are required to complete state-of-the-art training on many technology topics, including security and privacy, to help them keep pace with an ever-changing industry. By building and managing resilient infrastructure with trustworthy people, we can ensure high availability and commit to 99.9% uptime and 24x7 support in our SLAs.

Government

As cloud providers continue to evolve their operations to meet the responsibilities cloud customers transfer to them, so too must government evolve its approach to integrating the cloud into its operations. The Information Age has arrived and the cloud is ready for the government,

---

[1] For more information about Microsoft's commitment to privacy, see the Microsoft Trustworthy Computing Privacy page at www.microsoft.com/privacy.

[2] Microsoft's online Information Security Program has been independently certified by British Standards Institute (BSI) Management Systems America as being compliant with ISO/IEC 27001:2005.

but in many respects, the government is not yet ready for cloud computing. For example, according to the Government Accountability Office, federal agencies have serious and widespread information security control deficiencies. In their fiscal year 2009 performance and accountability reports, 21 of 24 major federal agencies noted that inadequate information system controls over their financial systems and information were either a material weakness or a significant deficiency. Furthermore, agencies continue to place federal assets at risk of inadvertent or deliberate misuse, financial information at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption. Agencies' current struggles to identify, manage, or account for security of data and systems are not immediately solved by integrating cloud services. Agencies must still identify and communicate requirements and expectations before transferring the responsibility of these functions to cloud providers. Once this is done, cloud service providers can then enhance agencies' abilities to meet their compliance challenges.

Progress is being made. The Federal Risk and Authorization Management Program (FedRAMP) is an important initial effort to provide joint security authorization for large outsourced systems. This program creates efficiencies for the government by enabling common assessments of cloud service providers, which allows a cloud provider to certify once and have that certification shared among the agencies. The result is a more efficient process than individual agency evaluations. FedRAMP also creates a process for cloud service providers to provide transparency into their operations and empowers agencies to fulfill their responsibilities for systems. Over time, this program could even begin to help reduce the number of federal systems resulting in further savings. In short, FedRAMP is the first government program to help balance responsibility between government agencies and cloud providers.

For security, agencies must approach the cloud thoughtfully, with an unwavering commitment to evaluate threats, assess risks, and define security requirements in order to ensure risks are managed at acceptable levels. Accordingly, agencies must adapt and advance their information security programs and communicate the attendant requirements to their cloud providers so that cloud providers can demonstrate that appropriate security and other operational controls have been implemented.

The government also should require that providers from which it procures cloud computing services meet the government's operational requirements for security, privacy and reliability. As threats continue to evolve, it remains critically important that cloud providers demonstrate secure development practices and transparent response processes for their applications. More broadly, the government should, wherever practicable, ensure that the technologies it procures, acquires, and uses are built and maintained in accordance with industry best practices for secure development. It should also promote (with appropriate incentives) such practices for all application developers. Users — including government users — need to be sure not only that their "boxed" products are secure, but also that their software applications — including those rapidly developed for the cloud — are built and provided on the basis of sound fundamentals.

Despite best efforts to prevent and protect against threats, incidents will inevitably occur. Some of these incidents will require law enforcement investigations, which may be hindered by forensic and jurisdictional issues resulting from cloud architecture and characteristics. Cloud

service providers face a number of challenges with respect to forensics. For example, the complexities of the technology and the distributed nature of the data can reduce both access to and the overall quality of forensics data, making audit and attribution of attacks more challenging. Users' data can be commingled on single pieces of hardware, in virtual machines, or distributed across multiple services in the cloud environment.

For investigations, government may not trust cloud providers to investigate an incident, but at the same time, the cloud provider may not be able to grant the government broad access to conduct an investigation into a multi-tenant environment since that might give the government access to confidential data it is not authorized to see. With respect to jurisdiction for law enforcement investigations, the location(s) of data, particularly when crossing national boundaries, may create significant challenges. These legal challenges can be managed, such as through use of geo-located private clouds, but probably cannot be fully resolved for all users in all cases. In some cases, new technologies, techniques, or standards for data forensics and data deletion may need to evolve for use in public, multi-tenant clouds.

In addition to these security requirements, government must identify appropriate controls to protect the vast amounts of sensitive personally identifiable information (PII) that it maintains and uses. Agreements with cloud providers are just one aspect of taking adequate precautions. A cloud provider can protect data as designated by the agency, but the agency itself must maintain policies and procedures for the identification and handling of data in-house, such as on employees' computers. In other words, privacy protections must be maintained seamlessly from the client to the cloud.

Protecting privacy also requires keeping pace with today's technological realities. Congress enacted the Electronic Communications Privacy Act (ECPA) — the primary federal statute regulating government access to subscriber information, stored communications, and real-time communications — almost 25 years ago, at a time when the vast majority of Americans had never heard of the Internet or e-mail. Electronic communications have evolved dramatically over the past 25 years and have become an essential mode of interaction for most Americans. But the law has not kept up with the changes in technology. When applied to the modern computing world, ECPA is complicated and unclear, and needs to be clarified and updated in order to properly account for consumers' reasonable privacy expectations. Microsoft supports the efforts to modernize ECPA that are being led by the Digital Due Process Coalition, and we encourage the government and Congress likewise to take up responsible reform of ECPA.

As with security and privacy, reliability remains a concern of government. In geo-diverse cloud environments, redundancy can help limit situations where data becomes unavailable; yet at the same time, customers must address connectivity to and reliable performance of cloud services. As these services become more integrated into agency operations and mission critical functions, government officials must ensure that they can maintain connectivity to the cloud by having physically diverse communications paths and alternate methods for accessing data centers. In addition, agencies should consider their reliance on cloud services in their business continuity and disaster recovery planning, and establish the necessary SLAs with their cloud providers to ensure continuity of operations.

If requirements are properly defined, cloud computing could ease the compliance challenges facing government. Unfortunately, the federal enterprise struggles today to meet key compliance goals such as those required by the Federal Information Security Management Act (FISMA). With 23,859 government systems across 25 agencies, key compliance metrics continue to lag. For example, 46% of high impact systems and 45% of medium impact systems in the government have not been certified or accredited. That totals 11,548 uncertified systems. Furthermore, just more than half of all federal systems have had security controls tested or business continuity plans tested.[3] Cloud computing could help ensure government data and systems meet expectations for certification, controls testing, and continuity planning. The cloud also provides a platform by which government could reduce the number of duplicative systems — saving costs, ensuring consistent application of Federal security requirements, and improving services to citizens and compliance.

Shared Responsibilities

Protecting the public good in the cloud requires Congress, the Executive Branch, and industry to work together. Our collaborative efforts should focus on promoting transparency around cloud computing providers' security, privacy, and reliability practices and, in turn, helping to ensure that users can make informed choices. Together, government and cloud providers should also address access and consent in privacy practices, including by requiring notice of privacy policies to cloud computing customers and by promoting the harmonization of global data privacy and data retention laws. Finally, we should collaborate to strengthen criminal penalties against hackers of cloud computing, and define penalties for criminal misuse of legitimate cloud services, to provide more effective deterrence and to enhance prosecutors' abilities to investigate and prosecute malicious actors who place cloud computing customers and the broader ecosystem at risk.

Microsoft is committed to securing the ecosystem and works with government through multiple public private partnerships; we also regularly work with our industry peers to address the most challenging issues facing users. Forums such as the Cloud Security Alliance (CSA) bring together subject matter experts to discuss key cloud risks and challenges and share best practices to resolve them. The CSA serves to create a cohesive set of recommendations and provide education around cloud security issues for cloud providers and consumers both domestically and internationally. Industry participation with organizations such as the National Institute of Standards and Technology (NIST) and the European Network and Information Security Agency (ENISA) helps to define and communicate the security, privacy, and reliability requirements among governments, other cloud users, and cloud providers. Government and industry must continue these international efforts to define and harmonize standards that enable innovation, create opportunity, and power the modern economy.

---

[3] *See* OMB's Fiscal Year 2009 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002, *available online at* http://www.whitehouse.gov/omb/assets/egov_docs/FY09_FISMA.pdf.

These actions will not solve fully the security, privacy, and reliability challenges of integrating cloud computing into the federal enterprise. However, by strengthening the security, privacy, and reliability practices in cloud computing services, and providing greater transparency to users, cloud providers and government will help build confidence in cloud computing services and, in turn, help cloud computing services to reach their potential.

Trust and Identity Imperatives

I have spoken about responsibility with respect to security, privacy, and reliability, but one particular issue is worthy of further note. Today, there are over 1.8 billion Internet users in the world, or more than 26% of the population.[4] Internet users continue to grow at over 19% year over year,[5] yet the mechanisms to provide identity, authentication, and attribution in cyberspace do not yet meet the needs of citizens, enterprises, or governments in traditional computing environments or for the cloud. The lack of trust online stems in part from our inability to manage online identities effectively. The cloud only amplifies the need for more robust identity management to help solve some of the fundamental security and privacy problems inherent in current Internet systems. As people move more and more of their data to the cloud, and share resources across cloud platforms, their credentials are the key to accessing that data. Every day, Microsoft authenticates more than one billion Windows Live ID authentications and processes two to four billion Exchange Hosted Services e-mails. Cloud providers will need to develop technologies that allow us to better manage identities both within their own systems and in settings where identities must be federated across separate networks.

Cyber attacks are facilitated by the anonymity and lack of traceability of the Internet; malicious actors in cyberspace must be convinced that either the cost of their actions is not worth the return on investment or that there is a real chance of attribution and punishment. Mandating robust authentication for some Internet uses — such as accessing critical infrastructures — while ensuring anonymity at other times (*e.g.*, when citizens want to access public information) can help strike the right balance between security and privacy. Modern identity systems increasingly permit users to provide elements of their identity without having to provide more information than is required for a given transaction. Additionally, in appropriate cases, hardware, software and data should be authenticated as well. For example, if someone wants to visit a website with content that is inappropriate for children, that person should be able to present reliable proof of age without having to reveal his or her entire identity. Granular attributes of identity that can be proven or asserted are called "identity claims."

While the industry and academia are advancing many technological capabilities for strong and robust identity and identity claims, a supporting ecosystem is also required. We must have mechanisms (and associated policies) for the issuance of digital credentials that provide stronger verification and are based upon in-person proofing. We must have interoperable identity systems so those who provide robust credentials and those who wish to consume them can do so easily,

---

[4] http://www.internetworldstats.com/stats.htm
[5] http://www.internetworldstats.com/pr/edi038.htm

thus enabling better trust decisions. The need for interoperability also demands standards and formats for managing and exchanging identity information.

The draft *National Strategy for Trusted Identities in Cyberspace*,[6] recently released by the White House, represents significant progress to help improve the ability to identify and authenticate the organizations, individuals, and underlying infrastructure involved in an online transaction. Government and industry must continue to work together on this initiative, as well as on advancing standards and formats on both a national as well as a global basis to enable a robust identity ecosystem.

Conclusion

Integrating cloud services into the federal enterprise fundamentally advances government in the Information Age. The characteristics of the cloud can enable a new agility and responsiveness in government to meet the needs of its citizens, but only if government and cloud providers work together in this transformation to embrace the new responsibilities of the cloud.

As part of this transformation, agencies' business models will change and they will transfer responsibilities for security, privacy, and reliability, in varying degrees, to cloud providers. Evaluating and apportioning the risks resulting from this transfer depends largely upon the type of cloud computing service model(s) selected. The adoption of cloud computing in the government is not about the success or failure of any one agency, but about the federal enterprise transitioning functions in a thoughtful and healthy way. The success of this transition depends on two factors: (1) the ability to adapt and advance information security programs and to communicate requirements to agencies' cloud providers; and (2) the ability of cloud providers to meet customers' requirements with sufficient transparency to ensure that requirements for security, privacy, and reliability are met appropriately.

Government is not alone in the adoption and integration of cloud services. Enterprises of all sizes and consumers are dramatically increasing their dependence upon cloud services. As such, it is incumbent upon the government to work with industry to address our shared responsibilities. Addressing these new fundamentals will foster innovative uses of the cloud, cultivate confidence, and advance information technologies for the new economy. The alignment and understanding of responsibility in the cloud requires greater transparency from both cloud providers and cloud customers (including enterprises and governments). The more precise and transparent we are, the greater the trust we will build, and the greater opportunity we create.

---

[6] http://www.dhs.gov/xlibrary/assets/ns_tic.pdf

Chairman TOWNS. Thank you very much, Mr. Charney.

Mr. Burton.

STATEMENT OF DANIEL BURTON

Mr. BURTON. Thank you, Chairman Towns, Chairwoman Watson, Ranking Member Issa, members of the committee. Thank you for holding this hearing and inviting me to share my views.

As the senior vice president for global public policy at Salesforce.com, I am deeply involved in discussions with Government about cloud computing, and I applaud the efforts of this committee and the subcommittee to shed light on this effort.

Salesforce.com is a leading enterprise cloud computing company whose applications allow organizations to input, store, process, and access data about their customers over the Internet. In addition, we provide a cloud collaboration tool called Chatter and a cloud technology platform called Force.com. Several U.S. Federal agencies already use Salesforce, including the Army, HHS, NASA, GSA, the State Department, the Census Bureau, and many others.

In my remarks, I will make reference to the Salesforce enterprise cloud computing model, not the consumer cloud computing model popularized by companies like Amazon and eBay.

Descriptions of cloud computing are like the parable of the blind men and the elephant. One blind man grabbed its trunk and said it resembled a giant snake; another its legs and said it was a tree; a third its tusks and said it was an enormous walrus, and so on. This parable will sound familiar to anyone who follows cloud computing. Some companies state that since it involves third-party data centers, they are cloud providers; others say that since it uses subscription payments, they are cloud providers; still others say that since it is accessed over IT networks, they are cloud providers.

While each of these descriptions is true as far as it goes, by themselves these discreet services do not constitute cloud computing. Nor can the companies that provide these discreet services be called cloud computing providers any more than an elephant can be called a snake, a tree, or a walrus.

True cloud computing consists of a combination of third-party data centers, subscription payments, Internet access, and something known as multi-tenant architecture, which NIST notes in its definition.

A good analogy for multi-tenancy is a skyscraper. Just like a skyscraper allows many occupants to run their businesses discreetly in the same building, multi-tenant cloud computing allows many users to run their applications discreetly on the same computing platform. Although users share the underlying infrastructure, they can only view the data and applications that pertain to them. In this way, multi-tenant cloud computing is like online banking; it lets a number of people use their accounts simultaneously, while keeping their information secure and private.

The great benefit of multi-tenancy is that it can satisfy the needs of numerous organizations on a single computing stack. Salesforce, for example, processes the data and applications for its 77,000 customers on just a few thousand serves. A single tenant computing model, which is sometimes referred to as a private cloud, could re-

quire several hundred thousand servers to manage a customer base this size.

For Government, multi-tenant cloud computing offers cost savings, flexibility, fast deployment, and lower risk of project failure. Traditional Government IT systems require up-front investments in hardware and software, and can take years to implement. As a result, they are often out of date and over-budget by the time they are deployed. Multi-tenant cloud computing eliminates large up-front costs and lets Government agencies start with a few users and scale rapidly so there is much less chance of waste and failure.

I understand that cost data ownership, security, and interoperability are of particular interest to this committee. Most studies conclude that cloud computing offers important cost savings. A recent Brookings study concluding that the cost savings for Government average between 25 and 50 percent. Salesforce cast studies support this conclusion.

As for ownership of data, Salesforce claims no rights to the information its customers submit to our cloud services. We use and process this information only as our customers instruct us to or to fulfill contractual and legal obligations. If a customer decides it no longer wants to use our cloud services, we make their information available to them in a format that allows them to move it elsewhere.

The Salesforce security management system is based on internationally accepted security standards like ISO27001. Perhaps the most compelling evidence of our security is the fact that over 77,000 organizations around the world, including very large institutions in highly regulated sectors like financial services, health care, and government, trust their information on cloud applications to Salesforce.

When it comes to interoperability, the proof is in performance. Over 50 percent of the transactions we process are handled automatically. In other words, about 150 million times per day our computers seamlessly operate with outside computers without human involvement.

I appreciate the committee's efforts to advance the Government's ability to take advantage of this important technology and look forward to your questions.

[The prepared statement of Mr. Burton follows:]

Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud

Testimony of Daniel F. Burton, Jr.

Senior Vice President, Global Public Policy

Salesforce.com

Before

The U.S. House of Representatives

Committee on Oversight and Government Reform
and
Subcommittee on Government Management, Organization, and Procurement

July 1, 2010

Chairman Towns and Chairwoman Watson, Ranking Member Issa and Ranking Member Bilbray, Members of the Committee, thank you for holding this hearing on cloud computing and for inviting me to share my views with you. Cloud computing is a revolutionary and disruptive new technology that is having a profound impact on how we use, manage and build computing applications. As the Senior Vice President for Global Public Policy at Salesforce.com, I am deeply involved in government discussions about cloud computing, and I applaud the efforts of this Committee and the Administration to enable federal agencies to take advantage it.

About Salesforce.com

Salesforce.com is a leading enterprise cloud computing company that provides cloud solutions to organizations of all sizes in all industries globally. Our main service offerings are applications that allow organizations to input, store, process, and access data to manage their sales and customer services. In addition, we provide a platform (Force.com) that enables customers and developers to build and sell new cloud applications, as well as a collaboration tool (Chatter).

Salesforce.com delivers its services over the Internet through commercially available Web connections and browser software. Instead of building and maintaining costly IT infrastructure, our customers simply log on to the Salesforce.com Website and access their cloud services using a unique username and password. Over 77,000 organizations globally, including governments and businesses in highly regulated industries like financial services, healthcare, insurance and communications trust Salesforce.com with their data. Our U.S. federal government customers include the Bureau of Census, the Department of Army, the Department of Energy, the Department of Health and Human Services, the Department of Homeland Security, the Department of Navy, the Department of State, the Department of Transportation, the Environmental Protection Agency, the General Services Administration and NASA, among others.

In my remarks today, I will discuss the core characteristics of cloud computing. I will also address issues related to cost, data ownership, security and interoperability because I understand that they are of particular interest to the Committee. In doing so, I will make reference the Salesforce.com enterprise cloud computing model, not the consumer cloud computing model that companies like Amazon and eBay offer.

How do you know cloud computing when you see it?

Descriptions of cloud computing are like the parable of the blind men and the elephant. Six blind men were asked to touch an elephant and describe it. One blind man grasped the elephant's trunk and announced that it resembled a giant snake; another felt the legs and said it was more like a tree; a third touched the tusks and insisted that it was similar to an enormous walrus; and so on. While each was correct in his own narrow description, each missed the larger picture.

This parable will sound familiar to anyone who has followed the discussion about cloud computing. Some focus on the fact that cloud computing involves third-party data centers and insist that because they hold their customer's data in remote data centers they are cloud computing providers; others emphasize the pay-as-you-go feature and conclude that because they charge their customers in increments over time they are cloud providers; others stress that it is accessed over IT networks and claim that because they provide applications over networks they are cloud providers.

While each of these descriptions is true as far as it goes, by themselves they do not constitute cloud computing. Nor are the companies that provide these discrete functions cloud computing providers any more than an elephant is a snake, a tree, or a walrus.

Cloud computing consists of a combination of these three features, plus something known as "multi-tenant" architecture.

- Third-party data centers – With cloud computing the actual computing takes place in a third-party data center, not on an individual's computer or within a company's own IT facilities. As a result, the user does not have to install or maintain a local copy of the software, invest in IT infrastructure, or maintain data centers.

- Internet Access – Users access cloud software over the public Internet with a browser. This means that they can retrieve their data and applications anywhere they have Internet access without dedicated networks or proprietary communication lines. It also means they can access information from multiple devices, like lap-top computers and smart-phones.

- Pay-as-you-go – Enterprise cloud customers do not purchase cloud applications, but subscribe to them, usually on a per-seat or a per-usage basis for a period of time.

Multi-tenancy

As important these three features are, unless they are combined with a multi-tenant architecture, they do not constitute true cloud computing

NIST alludes to the essential requirement of multi-tenancy in its definition of cloud computing, which reads as follows:

> *Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*

The definitive reference to multi-tenancy comes when NIST defines resource pooling:

> *The provider's computing resources are pooled to serve multiple consumers* ***using a multi-tenant model,*** [emphasis added] *with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.*

At the September 2009 Gov 2.0 Summit in Washington, DC Casey Coleman (CIO of GSA and Chair of the Federal Cloud Computing Executive Steering Committee) summed up the essential role of multi-tenancy when she stated that "Cloud computing by its very nature is multi-tenant."

A good analogy for multi-tenancy is the skyscraper. A skyscraper enables large numbers of different tenants to conduct their operations in the same building. The tenants do not have to lay the foundation, construct the building or maintain the underlying infrastructure. Instead, they simply lease office space and customize it to meet their needs, knowing that their business activities will be kept private from the other building occupants. The landlord is responsible for improvements to the building, and each time he upgrades the infrastructure all of the tenants benefit. If a tenant's needs change or if it becomes dissatisfied with the building services, he can terminate his lease and move.

Just like a skyscraper allows many different occupants to run their businesses discretely within a single building, a multi-tenant cloud computing platform allows many different users to run their computer applications discretely on the same computing platform. Because the users' data and applications are separated logically within the hardware and software, they can view only the data and cloud services that pertain to them. In this respect, multi-tenant cloud architecture is like online banking – it allows a number of consumers to use their individual accounts at the same time while keeping their banking information private through the logical (not physical) separation of data.

In order to appreciate the power of multi-tenant cloud computing, it is useful to compare it to traditional, single-tenant computing applications. Multi-tenant applications can satisfy the needs of numerous organizations with the hardware resources and staff needed to manage one large computing stack. By contrast, single-tenant applications require a dedicated set of resources for each organization. It is largely for this reason that the Application Service Provider (ASP) single-tenant computing model of the late 1990s failed. In the ASP model, the setup, maintenance and upgrades of computer applications were outsourced to a third-party service provider, just like they are with cloud computing. The difference was that the ASP had to maintain a separate infrastructure stack for each customer. As more and more customers were added, the sheer scale, cost and complexity of maintaining the aggregate computing infrastructure became unsustainable.

With multi-tenant cloud computing, the software applications are provided as a service to multiple customers on a single, large infrastructure stack. The configurations of each user are stored as metadata that describes the base functionality of their application and corresponds to their data and customizations. This metadata is then interpreted by the platform's runtime engine. In a robust multi-tenant, metadata cloud architecture there is a clear separation of the compiled runtime engine (kernel) and the application data. As a result, the kernel can be upgraded without disrupting customer's applications or data, thus

allowing for continuous improvement in performance, reliability, security and scale. In short, multi-tenant computing yields massive cost, speed, scale and innovation advantages that single-tenant computing cannot match.

With its multi-tenant architecture, Salesforce.com is able to run approximately 230,000 applications for its more than 77,000 customers on just a few thousand servers. No other computing model delivers that kind of efficiency. A single-tenant computing model (sometimes referred to as a "private cloud") would require a minimum of 2 servers per application (one database server and one application server), plus additional servers for redundancy and disaster recovery. Consequently, a single-tenant computing model could require several hundred thousand servers to manage the computing needs of the customer base that Salesforce.com manages with just a few thousand servers.

The key advantages of the Salesforce.com multi-tenant enterprise cloud computing solutions include the following:

- *Secure, scalable and reliable delivery platform* – The delivery platform for our service has been designed to provide our customers with high levels of performance, reliability and security. We have built, and continue to invest in, a comprehensive security infrastructure, including firewalls, intrusion detection systems and encryption for transmissions over the Internet, which we monitor and test on a regular basis.
- *Rapid deployment* – Our service can be deployed rapidly since our customers do not have to spend time procuring, installing or maintaining the servers, storage, networking equipment, security products, or other infrastructure hardware and software necessary to ensure a scalable and reliable service.
- *Ease of integration* – Our platform is designed to enable IT professional to integrate our service with existing applications quickly and seamlessly. Our Force.com platform provides a set of application programming interfaces (APIs) that enable customers and independent developers both to integrate our service with existing third-party, customer and legacy applications, and to write their own application services that integrate with our service.
- *Rapid development of applications using the Force.com platform* – Our customers and third party developers can develop applications rapidly because of the ease of use and the benefits of a multi-tenant platform.
- *Lower total cost of ownership* – We enable customers to achieve significant upfront savings relative to their traditional enterprise software model. Customers benefit from the predictability of their future costs since they pay for the service on a per subscriber basis for the term of the subscription contract. All upgrades are included in our service, so customers are not burdened or disrupted by the periodic need to perform system upgrades. Because we implement all upgrades on our servers, new features and functionality automatically become part of our service on the release date and therefore benefit all of our customers immediately.
- *Increasing innovation* – By providing infrastructure and development environments on demand, we provide developers the opportunity to create new and innovative applications without having to invest in hardware and distribution. A developer with an idea for a new application can log onto our platform, develop,

host and support their system on Force.com, and make the application accessible for a fee to our customers.

- *High level of user adoption* – We have designed our service to be intuitive and easy to use. Since our service contains many tools and features recognizable to users of popular websites such as those of Amazon, eBay and Google, it has a more familiar user interface than typical enterprise customer relationship management (CRM) applications. As a result, our users do not require substantial training on how to use and befit from our service.

For the U.S. government, these advantages translate into cost savings, flexibility, fast deployment and lower risk of project failure. Traditional government IT systems require significant up-front investments in hardware and software. Moreover, they can often take years to write, customize and install. As a result, they frequently fail to deliver the required functionality and are out-of-date by the time they are deployed, leading to newspaper articles about unsuccessful government IT projects with massive cost over-runs. Because cloud computing eliminates large up-front capital investments, lets government agencies start with a few users to see if the application meets their requirements and enables them to scale rapidly if it does, there is much less chance of waste and failure.

Like any new technology, cloud computing raises several issues that must be addressed if it is to achieve its promise. Among these are cost, data ownership, vendor lock-in, security and interoperability. I will discuss each of these below. In doing so, I will refer to the experience of Salesforce.com as an enterprise cloud computing provider and our customer case studies.

Cost

Because cloud computing services can be tailored to the specific needs of individual customers, it can be difficult to calculate precise cost comparisons between cloud solutions and traditional on-premise solutions. Nonetheless, most studies conclude that cloud computing offers substantial cost savings over on-premise computing. Moreover, there is broad consensus that cloud computing is far less risky than traditional on-premise computing – there are no massive up-front costs because users do not have to purchase software licenses or invest in expensive IT infrastructure. There is also general agreement that the on-going cost of cloud computing is much more predictable than traditional on-premise computing. Users of the cloud typically pay as they go, and pay only for what they use.

One of the best studies of the cost savings of cloud computing to the U.S. government is by Darrell West, Saving Money Through Cloud Computing (Brookings Institute, May 2010). This report concludes that there are significant cost savings associated with cloud computing.

> *Depending on the scope and timing of the migration, reliance on public versus private clouds, the need for privacy and security, the number of file servers before*

> *and after migration, the extent of labor savings, and file server storage utilization rates, savings generally average between 25 and 50 percent. Combined with cross-platform accessibility, scalability, and reliability, there is a strong argument for the federal government to place a greater emphasis on cloud solutions. Clouds bring convenience, efficiency, and connectability that are vital to government agencies.*

Because of these cost savings, Dr. West concludes that the amount of federal IT spending devoted to cloud computing will grow rapidly.

Salesforce.com case studies of government cloud implementations support these conclusions. For example, the U.S. State Department's Nonproliferation and Disarmament Fund (NDF) used Salesforce.com to create a cloud application to give program managers around the world ready access to up-to-date budget information. A 2009 Nucleus Research report estimated that the NDF cloud application cost one-quarter as much as it would have if it had been developed in-house. Furthermore, the report concluded that the return on investment was 216%, the payback time was 8 months, and the average annual benefit was $1,625,066.

NJ TRANSIT, which uses Salesforce.com to track and respond to service issues, offers a similar success story. Because of the communication and issue-tracking capabilities the cloud application enabled, NJ TRANSIT has been able to increase the number of inquiries it handles by 600% and reduce its response time by 35% without adding any additional staff.

These U.S. public sector examples are backed-up by case studies from the private sector and from other governments. For example, the Salesforce.com cloud-computing model saved Qualcomm an estimated $100,000 in hardware costs and allowed it to reduce support staff by 60%. Similarly, the Japan Post Network avoided $10 million hardware and software costs by deploying a Salesforce.com cloud solution and experienced a return in investment of 511% over three years. All of these case studies can be found on the Salesforce.com Website at www.salesforce.com.

Data Ownership, Compliance and Vendor Lock-in

As an enterprise cloud computing company, Salesforce.com manages massive amounts of information -- about 300 million transactions each business day. We use and process the information our customers enter into our system only as they instruct us to, or in order to fulfill our contractual and legal obligations. We claim no ownership rights to the information our customers submit to our cloud computing services. We disclose information submitted by our customers only if required to do so by law, and we provide affected customers prior notice of any such compelled disclosure to the extent permitted by law.

Salesforce.com also maintains strict confidentiality obligations and does not access customer data except under narrowly-defined circumstances. Like any organization that

stores and processes data, we face a patchwork of U.S. state, federal, and international privacy requirements. Customer data may also be subject to these requirements.

Some critics have raised concerns that cloud computing will lead to vendor lock-in. It is unclear, however, that customers will be locked-into their cloud computing applications any more than they are to their traditional on-premise computing applications. At Salesforce.com, for example, if a customer decides that they no longer want to use our cloud services, we make their respective information available to them in a format that allows them to download it and take it elsewhere.

Security

Security concerns are often cited as one of the main reasons to avoid cloud computing. Critics of cloud security emphasize that cloud computing is a new technology that lacks appropriate security standards and adequate controls. They also voice reservations about multi-tenant architecture and often point to private clouds as the best way to address the security issues associated with cloud computing. Others, however, believe that enterprise cloud computing is more secure than traditional client-server computing. They note that enterprise cloud computing allows for uniform high performance for all users, continuous improvements in the security of the underlying platform, features that can be tuned to match the sensitivity of the data being stored, a locked-down management network that is easier to secure than a distributed corporate network, and robust back-up systems.

In assessing the security of cloud computing platforms, it is important to look beyond generalizations to the specific security practices of individual cloud providers. Broad assertions about cloud security are like saying that trucks are safer than cars. Such a statement may appear to be true in the abstract, but it does not take into account the make, model and performance of the vehicles, where they will be driven, or who the driver is. Similarly, declarations like "private clouds are more secure than public clouds" are not very meaningful unless the security features of individual private and public cloud providers are carefully evaluated.

Salesforce.com views security as part of a trust equation that includes privacy, performance and reliability. Because trust also requires transparency, we have established a public trust site (https://trust.salesforce.com) that provides the Salesforce.com community with real-time information on system performance and security, including the following:

- Live and historical data on system performance
- Up-to-the minute information on planned maintenance
- Phishing, malicious software, and social engineering threats
- Best security practices for your organization
- Information on how we safeguard your data

The Salesforce.com security management system is based on an internationally accepted security framework that encompasses physical security, host security, logical network security, transmission level security, database security and operational security.

Salesforce.com is ISO27001 certified, SAS 70 Type II audited and SysTrust certified. We are a signatory to the US-EU Safe Harbor and have been certified by TRUSTe. We are also certified with the Japan Privacy Seal (JIPDEC).

Perhaps the best evidence of our security, however, is the fact that over 77,000 organizations around the world trust their information to the Salesforce.com enterprise cloud. Included among these customers are organizations that place a high premium on security, including financial services institutions, Fortune 500 companies, healthcare firms, technology companies, and governments.

We are encouraged by the actions the Obama Administration has taken to align the federal government security certifications with the cloud computing model and to streamline the security audit process. Programs such as FedRamp and Apps.gov are positive steps, and we look forward to working with federal agencies on these and other initiatives designed to facilitate the government's ability to use cloud computing.

Interoperability

Interoperability is also frequently raised as an issue for anyone considering cloud computing. No matter how powerful an individual company's cloud services are, they will not be effective unless they interoperate with outside software programs. For this reason, interoperability is a core feature of the Salesforce.com enterprise cloud. Perhaps the best indication of the extent to which Salesforce.com interoperates with other software programs is the fact that over 50% of the transactions we process are handled through our application programming interface (API). In everyday terms, this means that about 150 million times each day our computers are talking with other computers outside our system – or "interoperating" – without the intervention of individuals.

Salesforce.com provides interoperability at several different levels. We offer application mash-ups with other software programs, such as Google and Hoovers; native enterprise resource planning (ERP) connectors with SAP and Oracle; and native desktop connectors with Lotus Notes and Microsoft Outlook. We maintain an integration partner ecosystem that includes companies like Deloitte, Accenture and Acumen, and offer developer toolkits for .Net and Java. In April 2010, we announced a partnership with VMWare that will allow the 6 million enterprise Java developers to write cloud computing applications on the Force.com platform in the Java programming language. Our cloud services also interoperate with other major cloud companies, like Google and Amazon, and can be used on desktop, laptop and notebook computers, as well as on mobile devices like the iPhone and the Blackberry.

In addition, Salesforce.com hosts AppExchange, which is like an iTunes for enterprise cloud software applications. AppExchange is an online directory that provides customers a way to browse, test-drive, share and install application developed on our Force.com platform. Partners and developers can offer their applications on the AppExchange directory. This directory gives our users a way to find and install applications to expand

their use of the Force.com platform to areas that are complementary to or extend beyond customer relationship management solutions.

Conclusion

Cloud computing is a powerful technology that promises tremendous benefits for consumers, companies, non-profits, and governments. It has already been successfully implemented in organizations of all sizes around the world. According to Gartner, the cloud computing market was worth approximately $46 billion in 2009 and will increase to $150 billion by 2013. Gartner predicts that next year 25% of new software deployments will be based on software-as-a-service cloud computing applications. According to a recent Goldman Sachs technology software report, the shift toward cloud computing is "unstoppable." The remarkable growth of cloud computing is not limited to consumer and business applications. Numerous federal, provincial, and local governments in North America, Europe, and Asia have also implemented cloud computing solutions. Led by federal CIO Vivek Kundra, the U.S. federal government is emerging as a leader in public sector efforts to take advantage of cloud computing.
I appreciate the Committee's interest in this issue and your efforts to advance the federal government's ability to take advantage of this important new technology.

Chairman TOWNS. Thank you very much, Mr. Burton.

Let me just say to the committee members that we have three votes, and we will hear from Mr. Bradshaw and then I will recess the committee, and we will return 10 minutes after the last vote.

Mr. Bradshaw.

STATEMENT OF MIKE BRADSHAW

Mr. BRADSHAW. Thank you, Mr. Chairman, Chairwoman Watson, Ranking Member Issa, and members of the committee. I lead the Google team that provides cloud computing services to the Federal Government, and I am pleased to be here.

Federal IT is at a crossroads. Down one path, the adoption of cloud computing, we see more competition and innovation; down another path, which keeps IT tethered to the traditional desktop computing model, we have more of the status quo, meaning fewer choices and less competition. If there is one thing I want to leave you with today, it is this: the cloud is secure, the cloud saves taxpayer money, and the cloud can make Government more efficient. We believe Federal IT procurement policy should encourage competition and choice.

As you have heard today, there are three basic types of IT infrastructure: cloud, there is legacy, and a hybrid model that tethers the cloud to legacy systems.

Google offers cloud solutions that are used by 2 million businesses. A growing number of State and local governments, from Los Angeles to Orlando, use the cloud, as do Federal agencies, including the Departments of Defense, Energy, and Interior, as well as NASA, the SEC, and the GSA.

I would like to focus on three benefits from Federal adoption of the cloud: one, enhanced security; two, savings for taxpayers; and, three, more competition and innovation.

First, the cloud offers security advantages over legacy and tether cloud alternatives. Under legacy computing models, we store critical data on our computers and servers either at work or at home. This is the equivalent of keeping cash under our mattress. Storing data securely in a multi-tenant cloud is like keeping cash in a bank. Cloud providers are security professionals, and they can offer better security than customers do on their own.

There have been several examples where Government laptops and hard drives were lost or stolen, compromising the sensitive personal information of hundreds of thousands of individuals. In fact, GAO confirmed in 2009 that recent data losses occurring at Federal agencies have been the result of physical thefts or improper safeguarding of systems.

An important security benefit of full cloud model is that you can control security updates much more consistently and easily. Research shows most organizations take between 25 to 60 days to deploy security patches, and some CIOS admit it can take up to 6 months. In the cloud, everyone gets security updates as soon as they are available, not weeks or months later. Attacks come frequently, and cloud computing allows us to react quickly.

Hackers do not care about the labels assigned to cloud computing, whether the cloud is public or private or otherwise. Hackers will exploit security vulnerabilities where they find them. That is

why security must be judged based on an examination of specific security controls in place by a given cloud computing implementation.

At Google, we protect data by shredding and splitting it across numerous servers and data centers, making an attack much harder because no user's data resides on a single disk or server. The data is replicated and spread across different locations. So if a hurricane or an earthquake strikes one place, the application keeps running elsewhere. This is important for backup and disaster recovery. It was a key consideration for the city of Los Angeles because of their location in an earthquake zone. Backup and recovery solutions are built into Google's cloud architecture, and it comes at no extra cost.

Second, the cloud can save taxpayer dollars. This April, Brookings found that the Government agencies that switched to some form of cloud computing saw up to 50 percent savings. Last year, Forrester calculated that Google's cloud-based email service was one-third the cost of legacy email. To put that in context, the Federal Government spends $76 billion per year on IT, with $20 billion of that devoted to hardware, software, and file servers.

Other cost savings come from improving productivity, enabling more Federal employees to telework, and reducing energy consumption.

Third, introducing more choices into the Federal marketplace will intensify competition, which in turn will drive innovation up and prices down. The Federal Government is embracing cloud computing, and we support the administration's effort to drive the adoption of the cloud, including FedRAMP. We strongly support the effort to accelerate the process.

Naturally, legacy providers would benefit if they didn't have to compete with the cloud, so it is not surprising that some may try to slow this transition by fomenting fear of cloud security. This overlooks the security problems we have seen in legacy IT systems and it fails to recognize how these problems can be solved by the cloud.

Ms. WATSON [presiding]. We are out of time now, so we are going to recess and we will reconvene 10 minutes after the last vote. Thank you so much.

Mr. BRADSHAW. Thank you.

[The prepared statement of Mr. Bradshaw follows:]

Google™

Testimony of Mike Bradshaw, Director, Google Federal, Google Inc.
before the House Committee on Oversight and Government Reform and the
Subcommittee on Government Management, Organization, and Procurement
Hearing on "Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud"
July 1, 2010

Chairman Towns, Chairwoman Watson, Ranking Members Issa and Bilbray, and members of the Committee.

Thank you for the opportunity to discuss with you the benefits of migrating more federal agencies to cloud computing. I lead the Google team that provides cloud computing services to the federal government.

Cloud computing is a relatively new term for some, but the cloud is being used today by significant numbers of consumers, businesses, and – increasingly – the public sector. In fact, more than two million businesses use our cloud service, Google Apps. In the cloud, everyday processes and information that are typically run and stored on local computers – email, documents, calendars – can be accessed securely anytime, anywhere, and with any device through an Internet connection. The cloud enables government agencies to replace in-house information technology – which is costly and complex to own, maintain, and secure – with externally provided computing power that offers better and secure performance at dramatically reduced costs.

Google's cloud service allows users to store data or run programs on our geographically distributed, well-secured data centers. Businesses increasingly are choosing to use Google's data centers the same way they now use their desktop computers or on-premise file servers, and in the process are saving money, becoming more efficient, and improving their security. For example, more than 50,000 companies, including 15 percent of the Fortune 500, rely on Google's cloud security service to filter billions of emails against malicious attacks.

In my testimony this morning I would like to make three basic points.

- First, government agencies are finding that the cloud can provide better information security than they have today. Agencies face significant challenges with lost or stolen laptops that contain sensitive data. The cloud enhances security by enabling data to be stored centrally with continuous and automated network analysis and protection. When vulnerabilities are detected they can be managed more rapidly and uniformly. Cloud security is able to respond to attacks more rapidly by reducing the time it takes to install patches on thousands of individual desktops or hundreds of uniquely configured on-premise servers.

- Second, the cloud offers cost savings, efficiency, improved collaboration, and scalability.

By using multi-tenant cloud infrastructure, the costs of computing are spread out over many users instead of just the few users at a particular agency. Government data centers today are typically underutilized, which means they often waste money and energy.

- Finally, although the federal government is starting to adopt cloud computing, more could be done to broaden and accelerate the government's adoption of the cloud. Already, a path to cloud adoption exists, and federal government initiatives like Apps.gov and the Federal Risk and Authorization Management Pilot Program (FedRAMP) are making – or soon will make – progress towards accelerating cloud adoption. We support these efforts and thank the committee for the opportunity to explain the aspects of the government transition to cloud that are working as well as those that can be made even better.

We are excited about the cloud, and we are proud of our achievements in this space. But it is important to note that many companies are offering cloud services. Salesforce.com and Microsoft are just two of the many companies driving innovation and competition in cloud computing. Though most of my testimony will focus on Google products – which are the products I'm most familiar with – there are many cloud solutions out there. And, though we think we offer the best ones, we welcome and encourage the competition and innovation that we see every day in this space.

Cloud Computing Enhances Security

One of the key benefits that cloud computing can provide to the federal government is improved security compared to the status quo model of desktop-centric and on-premise computing.

How we use banks is analogous to cloud computing. Under traditional computing models, we store our critical data on our computers either at home or at work. This is the equivalent of keeping cash under your mattress. Storing data with a cloud computing service provider is like keeping cash in a bank. These companies are security professionals and they typically provide much more consistent security than their customers can on their own.

In today's model of traditional desktop computing there is significant government data stored on portable devices like laptops and USB thumb drives, which can – and often do – get lost or stolen. There are dozens of examples of government computers having been lost or stolen. In 2007, a Transportation Security Administration external hard drive that contained the names, bank records, Social Security numbers, and payroll information of up to 100,000 TSA employees went missing. An Army National Guard laptop that contained the personal information of 131,000 soldiers reportedly was stolen in 2007. A Department of Veterans Affairs portable hard drive that contained sensitive VA-related information on approximately 535,000 individuals was also stolen in 2007. As these examples demonstrate, government agencies have struggled with security under the traditional desktop computing model.

A 2009 Government Accountability Office report on existing government security deficiencies confirmed that many of the data losses occurring at federal agencies over the past few years have

been the result of physical thefts or improper safeguarding of systems, including laptops and other portable devices.

> *At least nine agencies also lacked effective controls to restrict physical access to information assets. We have previously reported that many of the data losses occurring at federal agencies over the past few years were a result of physical thefts or improper safeguarding of systems, including laptops and other portable devices.*
>
> *In addition, agencies did not always configure network devices and services to prevent unauthorized access and ensure system integrity, patch key servers and workstations in a timely manner, or segregate incompatible duties to different individuals or groups so that one individual does not control all aspects of a process or transaction.* (GAO Report GAO-09-701T, at page 6).

Cloud computing can protect against these security vulnerabilities. Moving data across portable devices becomes unnecessary, as cloud computing enables data to be accessed securely from anywhere with an Internet connection.

The most important component of feeling comfortable with one's data in the cloud is trusting a cloud services provider and the practices and policies they have in place. Most people probably do not realize that they have been doing this for years with web-based e-mail or common services like online banking. With Google products, users can set fine-grained access controls for documents, calendars, and other types of information commonly stored in the cloud.

Another important security benefit in the cloud is that agencies and other organizations can control security updates much more consistently and easily. Our research shows most organizations take between 25 and 60 days to deploy security patches, and some corporate chief information officers admit it can take up to six months. Google's cloud service allows everyone to get security updates as soon as they are available, not weeks or months later.

At Google data centers, data is stored on custom-built machines maintained by proprietary software that continually monitors systems. If a threat is found, the system can respond automatically. This structure provides scalability and helps make patching and upgrades more efficient. We can detect security threats across the web early and prepare appropriate defenses, sometimes even before anti-virus companies know about them.

Security is at the core of Google's design and development process; it is built into the DNA of our products. Google is a company that came of age in the Internet era and consistently defends against and adjusts to Internet security threats. We use a combination of people, process, and technology to help secure our systems.

Google employs a dedicated, full-time security team with some of the world's foremost experts in information, application, and network security. The security team can collectively anticipate and fix security issues more quickly and effectively than most single companies or individuals.
This team is responsible for maintaining the company's networks, developing security review processes, and building customized security infrastructure. It also has a key role in developing,

documenting, and implementing Google's security policies and standards. Also, Google's security professionals are empowered by the design of our cloud – we are able to update all of our servers at once.

Google uses an access model designed to only grant as-needed access to customer data. Data centers themselves are equipped with security technologies like thermal imaging cameras, electronic card access systems, 24/7 guard coverage, video analytics, and access logs, among others. Data is obfuscated and split across numerous servers and data centers, making an attack much more difficult because no single user's data resides on a single disk or server.

The data in Google's cloud is stored in geographically distributed data centers. The data is replicated several times so that it will still be available if we are confronted with a power outage in one part of the country. If, for example, a hurricane or earthquake strikes one data center, the application keeps running in the other data centers, and the data stays safe. This has important implications for backup and disaster recovery from a continuity of government perspective. For example, the City of Los Angeles noted that for them, because of their location in an earthquake zone, Google Apps could provide more affordable and efficient backup and recovery solutions than they could otherwise have procured.

Cost Savings, Efficiency, and Other Benefits

Beyond enhanced security, the shift to cloud computing brings demonstrable benefits for saving the government money and increasing the efficiency and functionality of government services. In January 2009, Forrester Research, an independent technology research company, calculated that Google's cloud-based email service, Google Apps Gmail, costs businesses only $8.47 per user per month, versus $25.18 for traditional on-premise email. In case after case, real world examples show that cloud computing costs far less than the traditional desktop model.

For example, in 2009 the City of Orlando was facing aging infrastructure and budget cuts that led it to reconsider managing an in-house email system and running its own servers. In just two months, Orlando was able to switch its 3,000 employees over to a cloud computing service that cut the annual cost per employee from $133 to $50. Now, Orlando employees, from city planners to police officers, will use a web-based email system similar to Google's popular Gmail, but with more storage (25 Gigabytes) and more customized features.

Federal agencies also can reap these significant cost savings. Booz Allen Hamilton, a strategy and technology consulting firm, reported in October 2009 that federal agencies could save 85 percent of their yearly IT infrastructure budgets by moving operations to external cloud providers. In April of this year, the Brookings Institution found that government agencies that switched to some form of cloud computing saw up to 50 percent savings. To put that in context, the federal government is currently spending $76 billion per year on IT, with $20 billion of that devoted to hardware, software, and file servers. That's billions of dollars of taxpayer money.

Cost savings from switching to the cloud are especially relevant given the current under-utilization

of government IT resources. The Office of Management and Budget emphasizes that while government data centers increased in number from 400 to 1,100 in a decade, server utilization at those data centers is on average a mere seven percent of full capacity. The cloud will be instrumental in reducing this kind of waste across the federal government's IT infrastructure.

In addition to being more cost efficient, the cloud is also more energy efficient. The City of Los Angeles, which contracted with Google to provide cloud-based email in October 2009, estimates that it will save $750,000 over the next five years simply from the reduction in energy costs.

For its part, the federal government, with over 1,200 of its own data centers, could significantly lower spending and energy consumption by moving some applications to the cloud. The Environmental Protection Agency estimated in 2007 that consolidated, energy-efficient servers and storage systems could cut electricity use by 55 percent. By 2011, the agency estimates that the cut in electricity use could save up to 74 billion kilowatt hours of electricity, $5.1 billion, and 47 million metric tons of carbon dioxide emissions.

Another way the federal government can help to reduce energy consumption is by promoting telework to reduce federal worker commute times and the energy consumed in that commute. As the series of snowstorms that blanketed the Washington, DC region this February showed, teleworking can prevent the government from shutting down completely in an emergency. Teleworking and the cloud can be important components of federal agencies' Continuity of Operations Plans. The cloud can allow teleworkers to easily and securely access their data and work from wherever they happen to be. During the February 2010 snowstorms, the Office of Personnel Management and GSA used cloud computing to share the load with other computer networks in order to keep OPM's Status Alert website running.

The cloud also brings increased functionality. Federal employees can collaborate more easily and effectively because information and applications run in a shared, secure space online, making it easy for people to work together on documents. Two or more people can, for example, edit a web-based document together in real-time while they are hundreds or thousands of miles away from each other – rather than sending it back and forth as an attachment and going through the laborious process of incorporating edits on top of edits. Running applications online means that they can be accessed more easily and securely from any device – a netbook, a smartphone, or any desktop computer where a user happens to be located.

The Federal Government Risks Falling Behind the Private Sector

Today the private sector is using cloud computing to allow employees to access their information and run software applications from anywhere they might be, anytime they need it, from virtually any device that's connected to the Internet. With cloud, it is easier to communicate and work together on documents, calendars, and other collaborative projects. A 2010 report by Gartner, a leading IT research and advisory firm, confirms an acceleration of adoption of cloud computing with the scale of deployments growing. More than 3,000 businesses sign up for Google Apps every day. Businesses are able to save money by spending less on building and managing their own, often

under-utilized, IT systems. The same benefits are available for the federal government, with the cost savings ultimately going to taxpayers.

Every day hundreds of millions of consumers use the cloud when they use email services like Microsoft's Hotmail, Yahoo! Mail, or Gmail, which are being run and stored on the Internet rather than locally on a specific computer. Similarly, consumers are using the cloud when they use online banking to look up bank records, balance check books, manage funds, or pay bills. A June 2010 Pew Research Center study projects that within ten years most Internet users will be doing the majority of their computing in the cloud instead of with software that runs and stores programs on a specific computer.

Businesses large and small are rapidly embracing cloud computing. Companies like Amazon.com, Salesforce.com, and Google are providing cloud platforms to allow business customers to improve efficiency and collaboration, lower operating costs, and secure data in ways that are simply not possible using the traditional, desktop-focused IT model.

Though the federal government is adopting at a slower rate compared to industry, we are beginning to see government cloud initiatives and pilot programs. The public sector is already adopting cloud at all levels of government to better serve citizens, reduce costs, lower energy consumption and make more effective use of taxpayer dollars overall. Federal entities currently using the cloud include the Department of Energy, Department of Defense, Department of the Interior, the National Aeronautics and Space Administration, the Social Security Administration, the Security and Exchange Commission, and the General Services Administration.

The DOE cloud computing migration is a good example of progress that is already being made. In 2009, DOE's Lawrence Berkeley National Labs (LBL) began exploring how to use cloud computing and LBL has already moved over 2,300 email accounts to Google Apps and will transition 5,000 accounts later this summer. This cloud deployment uses an identity management system to improve security. Also, the LBL cloud is empowering DOE scientific research teams to foster collaboration and community documentation through the use of Google Docs and other tools.

Simply put, cloud computing is already here and being used every day by individuals, business, and government. But we believe that the federal government could move more quickly, and by doing so it could reap benefits similar to those enjoyed by the private sector. The opportunity to switch to the cloud means that the approximately $80 billion per year market for federal government IT will see more innovation and competition – along with cost and energy savings, which are critical in today's environment.

Conclusion

We would like to thank Chairman Towns, Chairwoman Watson, Ranking Members Issa and Bilbray, and the members of the Committee for holding this hearing on the use of cloud computing by the federal government. The cloud can help agencies at all levels increase productivity, cut costs, keep pace with technology innovation, and improve security. We look forward to working with you and

other government officials to continue to make cloud computing more efficient, cost-effective, and secure.

[Recess.]

Chairman TOWNS [presiding]. Mr. Combs.

STATEMENT OF NICK COMBS

Mr. COMBS. Chairman Towns, Ranking Member Issa, thank you for the opportunity to address this important session.

Prior to my current role as CTO of EMC Federal, I served more than 25 years in Federal Government, primarily in the Army, DOD, and the intelligence community, so I echo the remarks of Mr. Issa about concerns with security.

During my career in Government and public sector, I have personally experienced many of the IT challenges facing Federal agencies today. Cloud computing is the buzz word of the day in IT, but the characteristics the cloud brings are what is important for Federal organizations. IT environments must be flexible, on-demand, efficient, and resilient.

Organizations must change, and the IT infrastructures that support them must be able to keep pace. At no other time has it been more important to change our IT landscape, as organizations are experiencing unprecedented levels of information growth and are under constant pressure to deal with the costs associated with maintaining our legacy IT environments.

Many Federal organizations have already begun to build the bridge to the cloud by adopting some form of virtualization. In fact, virtualization has become the foundation of the cloud and, in my view, is a great enabler of cloud services across the various deployment models.

Cloud computing is virtualization taken to its most logical extreme, creating the ultimate in flexibility and efficiency, and revolutionizing the way we compute, network, store, and manage information. Cloud computing has the potential to make the biggest impact in IT since the development of the microprocessor, but it is not going to happen overnight. This will be a journey, but we will realize benefits at many points along the way. In the end, we will be able to provide organizations with much greater flexibility to ensure we can meet the demanding needs of our Federal Government.

Many challenges and questions are yet to be fully answered, including acquisition, availability, performance, scalability, solution maturity, vendor lock-in, and, of top concern, security. I have addressed many of these in my written statements; however, due to time constraints, I will focus on security. We have an opportunity to get it right with cloud computing by engineering security into the solution, not bolting it on, as has been in the past.

Admittedly, with cloud computing sophisticated automation, provisioning and virtualization technologies, there is significant security implications. These risks require that we look at security in a whole new way. While perimeter and point security products will still be used by organizations, companies such as EMC and VMware are embedding security controls and security management in the virtual layer, creating an environment in the virtual world that is safer than the physical world today. Industry must continue to develop and deliver technology components that support centralized, consistent management of security across the technology stack.

The level of transparency that cloud computing vendors provide is critical when utilizing private sector partners. While there is a lot of talk about service level agreements helping to satisfy Federal security needs, SLAs alone are inadequate. The Government must take a trust, but verify approach and cloud vendors should be required to provide the tools and capabilities to allow customers visibility into those clouds to ensure the SLAs are being met.

Fundamentally, security must be risk-based and driven by a flexible policy that is aligned to the business or mission need. The need for common framework to ensure that security policies are consistently applied across the infrastructure is critical to successful risk management. That is one of the principle reasons that EMC supports updating the Federal Information Security and Management Act [FISMA], important legislation that will update the law to enable more operational risk management.

Technologies exist today to deliver private cloud environments inside Federal organizations to dramatically improve IT efficiency and still provide the security required to protect sensitive information within the Government enterprise. Multi-tenant federated clouds can be deployed where similar security requirements exist. However, placing information on a public cloud today should be limited to public facing information only, and then only if the providers can prove the level of auditing and protection procedures are implemented to deal with breaches of sensitive information.

Ultimately, cloud computing offers great potential for reducing cost and increasing efficiency and transparency throughout the Federal Government, and Federal departments and agencies should be encouraged to embrace that potential.

I again thank the committee for allowing EMC and me to contribute to this important effort. I look forward to taking your questions.

[The prepared statement of Mr. Combs follows:]

WRITTEN TESTIMONY OF
NICKLOUS COMBS
CHIEF TECHNOLOGY OFFICER, EMC FEDERAL
ON "CLOUD COMPUTING: BENEFITS AND RISKS MOVING FEDERAL IT INTO THE CLOUD"

BEFORE

THE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
AND
THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT

JULY 1, 2010

Chairman Towns, Ranking Member Issa, Chairwoman Watson, Ranking Member Bilbray, and Members of the Committee, thank you for the opportunity to address the opportunities and risks associated with moving federal IT into the cloud.

My name is Nick Combs and I am the Chief Technology Officer for EMC Corporation's Federal Division. EMC is a global leader in cloud computing infrastructure and services. We enable the full realization of the inherent power of information by creating complete information environments that are reliable, efficient, and secure. With EMC, users and organizations can bring the power of information to life...information that illuminates what is possible and that moves the world forward. Prior to joining EMC, I served for more than 25 years in the Federal Government as a senior leader in the Army, Senior IT leader in the Defense Intelligence Agency and as an IT Director and CIO with the Director of National Intelligence. During my career in government and the IT industry, I personally experienced many of the IT the challenges facing federal agencies today, particularly as agencies transition to cloud services. In both the public and private sectors, I have worked with different types of cloud computing models, each of which had its own risk management, interoperability, and data portability requirements.

First, let me comment on the term "cloud computing" and its definition. Today, the term is one of the most common yet most misunderstood references to information technology

and services. There are a number of definitions for cloud computing. For purposes of my testimony today, I will adopt the definition of The National Institute of Standards and Technology (NIST), which defines cloud computing as: "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1]

Given this understanding of cloud computing, I will address the various approaches to implementing the underlying infrastructure that facilitates cloud based solutions.

Confusion in the marketplace generally arises from discussion of different approaches to cloud deployment, that is to say discussions of Private, Community, Public, or Hybrid Clouds. Again, NIST has provided definitions of these delivery models that help provide more clarity:

- **Private Cloud** is infrastructure deployed and operated exclusively for an organization or enterprise. It may be managed by the organization or by a third party, either on or off premise.
- **Community Cloud** is infrastructure shared by multiple organizations with similar missions, requirements, security concerns, etc. It also may be managed by the organizations or by a third party on or off premise.
- **Public cloud** is infrastructure made available to the general public. It is owned and operated by an organization selling cloud services.
- **Hybrid cloud** is infrastructure consisting of two or more clouds (private, community, or public) that remain unique entities but that are tied together by standardized or proprietary technology that enables data and application portability.[2]

[1]: "The NIST Definition of Cloud Computing" by Peter Mell and Tim Grance, Version 15, 10/7/2009.
[2] "The NIST Definition of Cloud Computing" by Peter Mell and Tim Grance, Version 15, 10/7/2009.

The organizations represented at today's hearing collectively deploy all of these types of cloud computing models. EMC, for example, deploys solutions and services via private, community and public clouds. As an enterprise, EMC has used its solutions, as well as virtualization technology from VMware – the foundation of cloud infrastructure – as our IT organization leverages private clouds internally, reducing our IT costs and use of power resources. EMC has also been enabling customers to further their virtual datacenters and embrace cloud computing through the solutions and services it offers.

For example, through a public cloud, EMC's Mozy online backup and data recovery service provides peace of mind to over a million consumers and tens of thousands of individuals and businesses. EMC also teamed with Cisco and VMware to start the Virtual Computing Environment coalition, representing an unprecedented level of collaboration in development, services, and partner enablement that reduces risk in emerging cloud infrastructures in both the public and private sector. Just last month EMC announced the formation of a new Technical Advisory Board to shape the strategic vision of private clouds and beyond. This Board, comprised of recognized industry experts from business and academia, will focus on long-term technology strategy, industry trends, and advanced development opportunities and initiatives. Members were selected for their expertise and thought leadership in such key areas as server, networking, storage, virtualization, cloud computing, data structures, security, application middleware, and technical computing.

The Benefits of Cloud Computing

Cloud computing provides the characteristics that every IT organization needs by enabling IT infrastructures to be flexible, on-demand, efficient, and resilient. Organizations have been building IT systems the same way for the last 40 years and it is time for a change. However, we can no longer afford to have these legacy and stove-piped, monolithic systems in which each requirement has its own IT system. Organizations have attempted to utilize Service Oriented Architectures (SOA) to bring these disparate IT systems together, but have struggled due to the lack of interoperability

standards in designing IT systems. Cloud computing, based on open systems architectures and aligned to evolving cloud standards, can provide the foundation for future interoperable systems.

These new environments can dramatically reduce the largest costs associated with IT systems, particularly those related to operations and maintenance. According to the analyst firm IDC, more than 70 percent of organizations' IT budgets are dedicated to just keeping the lights on and only 30 percent of budgets are available to bring new capabilities to the organization. The Federal Government has spent billions of dollars for computers to create and process information, internal networks to move that information around, and hardware to store it. And don't forget about the application software for those internal processes and accounting. We are at a point where government agencies are spending a majority of IT budgets just to maintain our current systems and infrastructure. During my service in the federal government, I saw some government organizations with operating and management costs as high as 85 percent of their overall IT budget. Cloud Computing offers the means through which to address this imbalance.

Through the cloud, organizations can centrally manage their IT systems and provide uniform policy implementation. They will reduce their operating and management costs, thus freeing up resources to address other needs. For example, money previously devoted to simply maintaining the infrastructure could be used to increase the infrastructure's security posture. Cloud computing brings a level of automation to IT that dramatically reduces costs by sharing resources and frees up more resources to deliver the capabilities that organizations need.

Federal Strategy for Cloud Computing

The transition to cloud computing will not occur overnight; rather it requires a journey to realize all the benefits the cloud has to offer. The federal government has many unique environments, but these organizations can benefit greatly from the successes that commercial organizations have already achieved through the adoption of cloud

computing. The economies of scale, flexibility, and efficiencies of these cloud infrastructures will not only save us significant amounts of capital and maintenance costs, but enable us to apply and use information across our enterprises as never before.

One can only imagine all the ways in which information technology could be applied in the government if federal IT professionals were freed from the task of managing today's complicated and antiquated infrastructures. OMB Director Orszag made a similar point last month when he highlighted the fact that government organizations are unable to match the productivity and innovation of the private sector because of archaic and complicated computing infrastructure.[3] Cloud computing provides a mechanism to address this technology gap, allowing the federal government to unleash new innovations and improve productivity.

Many federal organizations have already begun to build a bridge to the cloud by adopting some form of virtualization. In fact, virtualization has become the foundation of the cloud and in my view, is the great enabler of cloud services across the various deployment models. Cloud computing is virtualization taken to its most logical extreme, creating the ultimate in flexibility and efficiency, and revolutionizing the way we compute, network, store, and manage information. Virtualization capabilities are also evolving outside the server realm. In fact, EMC recently announced breakthrough capabilities that enable virtual storage over distance. The industry's first distributed storage federation will provide unprecedented business agility by eliminating the current boundaries of physical storage. This is a key enabler to future cloud architectures.

Cloud Security and Risk Management

Information security is by far the biggest concern of federal CIOs considering implementing cloud infrastructure and services. According to an April 2010 Lockheed Martin Cyber Security Alliance survey of U.S. federal government, defense, and intelligence agency decision makers, respondents were most concerned by data security,

[3] Remarks by Peter Orszag, Center for American Progress, June 8, 2010, Washington, DC.

privacy and integrity in the cloud.[4] In addition, 46 percent of respondents to the Ponemon Institute's November 2009 "Cyber Security Mega Trends" survey of IT leaders in the U.S. federal government indicated that cloud computing increases security risk within their organization.[5] The biggest security concern noted by Ponemon survey respondents (30 percent) was the inability to protect sensitive or confidential information and the second most significant concern (20 percent) was to restrict or limit the use of computing resources or applications.

Admittedly, with cloud computing come sophisticated automation, provisioning and virtualization technologies that have significant security implications, so we must look at security in a whole new way. In March of 2010, RSA the Security Division of EMC, unveiled a shared vision with Intel Corporation and VMware for building a more secure and transparent infrastructure for business-critical cloud services. While perimeter and point security products will still be used by organizations, companies such as EMC and VMware are embedding controls and security management in the virtual layer, creating an environment in the virtual world that is far safer than what exists in the physical. Industry must continue to develop and deliver technology components that support centralized, consistent management of security across the technology stack. Security must be dynamic and intelligent. The static, reactive environment developed in the past simply will not work.

With virtualization and cloud computing, applications have become completely disassociated from the IT infrastructure on which they run. It provides the flexibility to have the same application run in the datacenter next door on one day, in a centralized datacenter hundreds of miles away the following day, and in a service provider datacenter another day. For that reason, security cannot solely rely on the controls of the IT infrastructure such as the network perimeter. Security must evolve to become much more centered on the users and on the information they are accessing. For that reason,

---

[4] "Awareness, Trust and Security to Shape Cloud Adoption," a survey commissioned by the Lockheed Martin Cyber Security Alliance and conducted by Market Connnections, Inc., April 2010

[5] "Cyber Security Mega Trends: Study of IT leaders in the U.S. federal government", Independently conducted by Ponemon Institute LLC; Publication Date: November 18, 2009.

emerging technology practices, such as adaptive authentication and data loss prevention, are both widely used in the commercial world. However, they are only beginning to be adopted in federal government organizations. Such practices must be more broadly deployed. This environment must be transparent to the enterprise and to the user. Security cannot be an after thought; it must be embedded in the fabric. It must be built into the products and infrastructure by the vendor community.

For a decade, fraudsters have been crafting malware to steal users' passwords and perform fraudulent actions on their online bank accounts. Cloud computing can increase the risk of exposing corporate assets to fraudsters and cybercriminals. The automaker's next design is worth more on the black market than online bank accounts. The same malware used to steal online banking password is also being used to steal corporate passwords. In the age of cloud computing, solely relying on passwords to protect access to cloud applications is not sufficient. Additional best practices like risk based authentication must be employed and we think that that approach will fit well within the Trusted Identity strategy that is currently being developed by the Obama Administration.

When implemented correctly, cloud environments can be much more secure than today's IT environments, which are often protected by inadequate perimeter security practices. The level of transparency cloud vendors provide is a critical aspect when choosing a cloud partner. While there is a lot of talk about Service Level Agreements (SLA) helping to satisfy federal government information security needs, this alone is inadequate. The federal government must take a trust-but-verify approach. Cloud vendors should be required to provide the tools and capabilities to allow customers visibility into their cloud environments to ensure compliance with those SLAs. SLAs should be clearly defined and monitored by government customers to ensure maximum service value is received for budget dollars spent. For instance, SLAs in areas of performance, availability, backup and recovery, archive, continuance of operation, and disaster recovery must be clearly stated, measured, and monitored by the government agencies. Additionally government risk and compliance capabilities need to be deployed and dash boards

provided to the customer to ensure that our information is protected and our policies are being followed.

Security must be risk-based and driven by flexible policy that is aligned to the business or mission need. The need for a common framework to ensure that security policies are consistently applied across the infrastructure is critical to the success. That is one of the principle reasons that EMC supports updating the Federal Information Security and Management Act or FISMA, important legislation that will update the law to enable more operational risk management, which is essential in both today's environment and the evolving cloud computing infrastructure.

Technologies and effective best practices exist today to deliver private cloud environments inside federal organizations to gain dramatic improvements in IT efficiency, while also providing the security required to protect sensitive information within the government enterprise. Multi-tenant federated clouds can be deployed where similar security requirements exist. However, placing information on a public cloud today should be limited to public facing information only and then only if the providers can provide the level of auditing and protection procedures needed to deal with breaches of sensitive information.

Conclusion

I again thank the Committee for allowing EMC and I to contribute to this very important effort. IT is on the verge of dramatic change; cloud computing has the potential to have the most significant impact on IT since the development of the microprocessor. We have to remain focused to ensure we get it right. This will be a journey and we will realize benefits at many points along the way and it will provide organizations with much greater flexibility to meet the demanding needs of our federal government. Admittedly, security is a top concern, but the technology and best practices exist to address that risk. A critical part of the solution lies in engineering security into the cloud, not bolting it on as an afterthought. Ultimately, cloud computing offers great potential for federal

information technology, and federal departments and agencies should be encouraged to embrace that potential.

Chairman TOWNS. Thank you very much for your testimony, Mr. Combs.

Mr. Ganger.

STATEMENT OF GREGORY GANGER

Mr. GANGER. Thank you for this opportunity to testify along with the others. I am a professor of electrical and computer engineering at Carnegie Mellon University, where I am also the director of a research center focused on issues like cloud computing, and have been for over a decade. I hope that my independent voice from an elite educational institution can help with clarifying the issues being explored today.

You have heard from a number of folks already today, and obviously, from the questions, investigated the issues yourselves as well; and I will attempt to avoid being needlessly redundant. But I will underscore a few important points and raise a few new ones.

As we have heard and as you have read, cloud computing is a buzz word for using others' computers together with yet others in order to achieve efficiency, instead of doing everything yourself. It is a natural evolution as a part of a service-based economy. In fact, as Mr. Issa noted, it is a bit of a return to the past in some ways. I won't get into the details of it now, but there is actually a good reason why it has gone back and forth a little bit as engineering technology and economies of scale have changed.

One aspect of the definition of cloud computing that I want to make sure doesn't get lost is the differentiation between a private cloud and a public cloud, which has to do with who shares the cloud. A private cloud is something that an organization does itself and might be shared amongst the sub-organizations of that organization. So in the Federal Government imagine all the agencies sharing a cloud. As contrasted with a public cloud that might be offered to many organizations to share, as is usually thought of when one hears the term cloud computing because of the Internet analogy of everybody being able to access the Internet.

But the private cloud is something that we don't want to lose sight of because it is going to play a part of the approach that gets taken with the breadth of Federal IT functions. In fact, this is another thing that was brought up earlier, this notion of moving to a centralized management site. That is one step toward a private cloud approach.

And there are some private cloud initiatives that are going on in the Government right now. For example, the NBC of the Directorate of the Interior has some cloud computing functions and there is also an activity called Nebula that NASA is doing for scientific activities.

The benefits of cloud computing, when done well, can be huge. We have heard a number of examples. I liked the example, in particular, of IBM going from 235 data centers to 12. In my written testimony I talk about several others, including HP going from 85 data centers to 6 over the course of the last 4 years and reporting from that 60 percent reductions in their data center costs across the board, while at the same time increasing the amount of computing and storage that they are doing. So the savings are real and they are large.

As with most things, your mileage may vary, and this was brought up multiple of you already, and just how much you save is going to depend, for example, on how efficient the function that you are moving was already. And the efficiency of existing implementations of functions varies widely, so naturally the savings you are going to get is going to vary as well.

But one big benefit that I haven't heard talked about as much that you don't want to lose sight of as well is the speed of deploying a new application. In the traditional model, where you have to procure, buy, deploy, set up a set of computers before you can even start to develop the application that you are trying to deliver, and that process may take many months, 18 months was the example that Mr. Kundra used, comparing that to the notion of renting some computing utility and getting started right away is a sea change in terms of how quickly you can move in a new direction.

There are risks. It is natural to address them with questions, which is why I started with the benefits. Security is a very natural one. It is very important, in talking about security, to not start from the mentality that doing it yourself means that it will be done perfectly. There are too many examples where that is not the case, and, in fact, having a collection of security experts try to do the job for a larger collection of people, rather than having each of those people do it themselves, makes a lot of sense.

You get more ability to move forward quickly when you have the experts doing it for people rather than everybody doing it themselves. It doesn't mean that everything is going to want to migrate to a central place, but it is going to mean that a lot of things are going to make sense to that kind of centralization.

Lock-in fears mean that standardization is going to be critical. Resistance to change is going to mean that change management and new training is going to be critical, as well as centralized knowledge sharing portals and information sharing. And IT culture changes are going to mean that the IT staff are going to have to be retrained to new roles as well. They are not going to go away; you are still going to need expert IT staff to manage the interaction between any given agency, for example, and the cloud computing provider, but their roles are going to change, they are going to move closer to the applications folks.

But the potential is great; it needs to be embraced. I am thrilled to see that is happening, and thank you for letting me be here and I am happy to answer any questions that you have.

[The prepared statement of Mr. Ganger follows:]

Written Testimony of
Gregory R. Ganger
Professor of Electrical & Computer Engineering and Computer Science,
Carnegie Mellon University

United States House of Representatives
Committee on Oversight and Government Reform
Subcommittee on Government Management, Organization, and Procurement
Hearing on
Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud
July 1, 2010

I thank you for the opportunity to testify about the benefits and risks of using cloud computing for federal IT functions.

About me: My name is Gregory (Greg) R. Ganger. I am a Professor of Electrical & Computer Engineering and Computer Science at Carnegie Mellon University (CMU). For the last ten years, I have also served as Director of CMU's Parallel Data Lab (PDL). The PDL is a world-renowned research center focused on storage and large-scale infrastructures, such as cloud computing and more traditional data centers, regularly working with and annually supported by most of the major developers of technology in these areas. Current industry sponsors include Google, Microsoft, Yahoo!, VMware, HP, IBM, Intel, Oracle, Facebook, APC (of Schneider Electric), EMC, Hitachi, LSI, NEC, NetApp, Seagate, and Symantec.

I have been conducting research on large-scale computing and storage infrastructures (e.g., cloud computing) and their operation/administration for over a decade. Among the cloud computing projects I lead are CMU's Data Center Observatory (DCO) and the CMU portion of OpenCirrus. The DCO was conceived as a consolidated data center and private cloud for research computing/storage needs, but heavily instrumented and forward-looking to enable research into efficiency, and it is being realized with active collaboration from several of the PDL sponsor companies. OpenCirrus (https://opencirrus.org/) is an open cloud computing testbed currently consisting of ten sites worldwide, each of which provides public cloud computing resources via open interfaces and open source software.

Testimony roadmap: I have been asked to testify about the use of cloud computing for federal IT needs, including potential benefits, risks, challenges, and consequences. My

written testimony is organized as follows. First, I provide a brief review of cloud computing generally, highlighting a few forms that it can take, including the highly relevant concept of a so-called "private" (or "internal") cloud. Second, I discuss the large potential benefits of using cloud computing for federal IT functions, which are similar (in many cases) to those for large corporate organizations. I highlight the benefits first because, while I suspect that most questions will focus on the risks and challenges, overall thinking about the concept of using cloud computing resources for federal IT functions should not lose sight of the large potential benefits of this young, maturing technology. Third, I discuss various risks, challenges, and consequences. Some of these (e.g., resistance to change) will require continuing education and strong guidance, possibly including explicit incentives. Some of these (e.g., lock-in and management complexity) will require patient and incremental approach to moving federal IT into the cloud, as advancement in both technology creation and standards bodies address unresolved issues. A few (e.g., security) may require certain IT functions to never migrate fully to a public cloud. None, however, preclude rapid partial migration of federal IT function into the cloud and expanded migration over time.

It is important to keep in mind, while considering pros and cons of moving federal IT into clouds, that it is far from an all-or-nothing decision. For some federal IT functions, it will be the right choice, and for others it may not be. The choice need not be the same for all IT functions, and movement can happen independently for each, allowing incremental movements that each yield benefits.

A. Cloud computing basics

Very broadly, "cloud computing" involves using someone else's computers (and possibly software setups), shared with yet other groups, for some task instead of using your own. There are many technical issues involved, which have delayed the realization of this long-sought notion of computing services as utilities, but the basic concept of outsourcing work is natural in today's service-based economy.

The "cloud" aspect refers to the fact that the computers used are on the network, somewhere, but that the cloud computing customer need not be aware of where they are or

details of how the outsourced work is completed – it is referred to as "in the cloud", because large networks (e.g., the Internet) are often illustrated as clouds in technical diagrams.

The term "cloud computing" has been applied to a broad class of IT outsourcing activities, leading to broad definitions. For example, NIST's definition[1] is more technical than my very brief description above, but it closes with "and is composed of five essential characteristics, three delivery models, and four deployment models." Just the cross-product of the three delivery and four deployment models yields twelve configurations that fit the definition. I will not detail the full breadth here, but I will highlight a couple configuration options in an attempt to help clarify cloud computing and important issues involved.

Raw resources vs. software services: The delivery model axis relates to the form of computing service purchased from a cloud computing provider. One option, called "Infrastructure as a Service (IaaS)" by NIST, is to rent raw computing resources, such as computer time or storage capacity. Which programs a customer runs in their rented computer time,[2] or what data is stored in rented storage capacity, is entirely up to the customer (who must, therefore, configure and maintain the programs themselves). Setting aside technical details, the IaaS concept should be familiar to anyone who has rented a car, exercised in a fitness center, or stayed at a hotel. The other two options, called "Software as a Service (SaaS)" and "Platform as a Service (PaaS)" by NIST, provide complete applications (e.g., email) and/or building blocks (e.g., database systems) for use by customers (and perhaps provided by customers to third parties). Setting aside technical details, these concepts are akin to outsourcing of food services, patent litigation services, or accounting services.

---

[1] The full NIST definition is two pages long, but the primary paragraph states "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential **characteristics,** three **service models**, and four **deployment models**." Most of the remainder details the five, three, and four. The latest version (v15) can be found at http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc .

[2] Rented raw computer time in most cloud offerings is used to execute software encapsulated in a so-called "virtual machine", which appears to the customer as a physical machine. Indeed, all cloud resources are "virtualized" in the sense that details of how they are provided are hidden from customers and may not match the appearance given to the customer – such virtualization enables improved efficiency and is fine for customers, so long as the behavior promised to the customer is realized.

Public cloud vs. private cloud: The deployment model axis focuses on who shares the cloud. One option, termed a "public cloud" by NIST, is made available to the general public by a provider selling cloud computing services. This is the option usually in mind when people first think about cloud computing, since it matches the general accessibility of the Internet. But, it is not the only option. Another option, termed a "private cloud" by NIST, is operated solely by one organization and shared by its various sub-parts. For particularly large organizations, such as the federal government or a large Internet service company (e.g., Google or Microsoft), many of the benefits of cloud computing can be realized with a private cloud model – for such organizations, the economies of scale and aggregation are sufficiently present without sharing externally, because of their many sizable sub-organizations.[3] Of course, an organization can use more than one cloud, including of different types, and can also used both cloud and non-cloud (i.e., their own) computer resources.

B. Potential benefits of moving federal IT functions into the cloud.

Cloud computing has the potential to provide large efficiency improvements for federal IT functions. As with outsourcing in non-IT domains, such as rental cars and food services, the efficiency arises from having multiple customers (organizations) share the provider's offering instead of each providing for itself. Efficiency improvements come from multiple fundamental sources, including: (1) increased utilization of resources, since sharing allows the portions unused by one customer to be sold to (used by) another, while each customer pays for just what they use; (2) economies of scale, since operational costs usually do not scale down linearly with resource size – for example, one cannot use a part of a car, and cooking for two takes nearly as long as cooking for five; (3) increased specialization, since experts working for the provider can focus on the one offering rather than being "jacks of all trades"; (4) low entry cost (in terms of time, effort, and dollars) for new customers, since the resource is already set up by the provider and ready for use. These benefits can all be present for cloud computing, with large potential reductions in IT costs (both capital and personnel), energy demands (due to the need for fewer total computers), and time to establish new IT functions.

[3] As one example, the National Business Center (NBC) of the Department of the Interior now provides some private cloud capabilities (http://cloud.nbc.gov/).

Although concision precludes full analysis here, two examples can help illustrate potential infrastructure efficiency benefits of even just one or two of these sources:

- Although an imperfect example, because of artifacts of CMU's smaller size and relative resource-poorness, our experiences making a case for using cloud computing for research computing at CMU provide some insight. In surveying the separate infrastructures used by research groups on campus, we found average utilizations around 25% -- that is, ¾ of the work potential of the computers went unused, over time, even in a University research environment that struggles to find funds to purchase equipment.[4] A private IaaS cloud computing approach with 75% utilization would reduce the number of servers needed by 66% or allow three times the work to be completed during heavily active times, which has induced us to aggressively pursue deployment of such a private cloud at CMU. Such numbers are normal, even laudable for the traditional "every group for themselves" approach, not a sign of misbehavior. Indeed, a GSA presentation[5] indicated "Average Server Utilization" values of 7-15%, offering even more room for improvement.

- HP's recent data center consolidation effort provides a second example. In 2006, HP identified their "many separate data centers" deployment (85 data centers across 29 countries) as a significant source of inefficiency. They noted plans to consolidate into six large data centers, estimating $1B/year savings in IT expenses and significant energy savings as a result.[6] Recently, HP's CIO Randy Mott shared some outcomes of this successful consolidation effort, including 60% reduction in overall data center costs.[7] Despite ever-growing demands for computing, HP reduced their number of server computers by 40%, which would combine with their improved cooling approaches to yield significant energy savings.

The savings in these examples do not even account for the much improved IT staff efficiency (#3 above) or the faster pace of deployed IT improvements (a consequence of #3). With consolidated infrastructures, IT staff specializing in particular aspects can focus on those aspects – because of the large scale, such specialization does not lead to excessively sized IT staffs. Since the particular aspects (e.g., network management or storage management) are handled by the provider, none of the customers need to employ staff focused on those aspects – one set of staff handles them for all, eliminating redundancy across customers and allowing customer IT staff's to focus on the customer's missions instead. Also, because specialized

[4] But, during active times, they tend to be overburdened.
[5] "GSA Presentation on the Federal Cloud Computing Initiative" by Michael Goodrich (Project Manager, FedRAMP and Apps.gov, General Services Administration) on Software & Information Industry Association panel. See slide 22. Available at http://www.siia.net/blog/index.php/2010/06/gsa-presentation-on-the-federal-cloud-computing-initiative/
[6] http://news.cnet.com/HP-plans-data-center-consolidation/2110-1011_3-6073187.html
[7] http://www.enterprisenetworkingplanet.com/news/article.php/3878966

staff have fewer aspects to manage, they can focus more attention on improving their specific aspects, leading to more rapid adoption of new technologies and best practices from which all customers immediately benefit.

In addition to significantly increasing efficiency across a set of current customer IT functions, cloud computing can greatly improve the situation for new IT functions (#4 above). Traditionally, a lengthy start-up process is often involved with establishing a new IT function, including procuring new computers (and sometimes building machine room space to power and cool them), installing and configuring the computers, and only then finally starting to set up the IT function in question. With cloud computing, one can rent pre-setup computer resources as soon as one has budget to do so, leading to much quicker progress on new directions. Moreover, one does not have the danger of incorrectly guessing how many computers are needed (which can lead to waste or delays), since the cloud provider allows rapid incremental scale-up (charging only for what is used) as long as the customer is willing to pay for what they use. Among other things, therefore, cloud computing could significantly accelerate deployment of e-government applications.

Overall, the potential benefits from cloud computing are huge, both for global efficiency (total equipment and energy used) and for each customer (dollars and mission focus).

C. Risks, challenges, and consequences

Cloud computing is very different from the traditional approach of each organization (e.g., agency) creating and maintaining their own computing resources, from top to bottom. Naturally, there are many challenges to be faced in making the significant transition to outsourcing aspects to external providers, particularly given the relative youth and rapid evolution of cloud computing. Of course, there are security concerns when an external provider is made part of an agency function. There are also "lock-in" concerns caused by lack of standardization and (in some cases) the difficulty of moving large data sets. Another significant source of challenges is the massive IT culture change inherent in a transition to cloud computing, which will require overcoming resistance to change and retooling IT staff skill sets.

Security concerns: Security is an issue for all networked computer activities. It is natural to imagine that security might be weakened by involving an external provider, particularly when confidential data are involved. But, it is not necessarily the case in all, or even most, circumstances. As in the real world, computer security is about risk management, not absolutes – most of us feel relatively secure in our homes, for example, despite glass windows on the ground floor.

Having federal agencies maintaining infrastructure does not guarantee their security, both because humans are imperfect and because no perfect computer security technologies exist. Public cloud providers are capable of employing the same best practices and technology as government agencies and potentially upgrading more rapidly to new advances (because of #3 above). The question is whether or not they can be trusted to do so. To establish that trust, there will need to be certification of the degree of trust that can be placed in a given provider, using established (e.g., FISMA) and perhaps new mechanisms – standardized approaches to doing this is an area of necessary, and ongoing, effort in technology working groups. Movement of IT functions to providers must be limited to those pairings with acceptable risk. Certain functions, and certain data, will perhaps never be appropriate for public clouds – highly classified intelligence activities, for example. But, for many federal computing activities, security needs are likely to be consistent with those of corporate customers of public clouds.

It is worth noting that private clouds, maintained by the government, can be used for IT functions that may require security efforts beyond those that public cloud providers are willing to employ (e.g., because they go beyond what corporate customers require).

Lock-in concerns: Currently, cloud computing offerings are diverse – one can choose among several to which to migrate a function, and then go thru the effort to migrate, but often there is no easy way to switch from one provider to another. Today, such a switch can involve time-consuming extraction of one's data, reprogramming of one's application to fit the new provider's interfaces, and uploading of one's data to the new provider. Each step can be onerous.

One big part of the problem is standardization or, rather, lack thereof. Although various working groups are now focused on standardization, it is still early in the process.

Indeed, cloud computing is sufficiently new that there is some danger in standardizing so quickly, with such a short window of experience from which to draw. Nonetheless, standardization is an important part of promoting compatibility and competition among cloud computing providers.

A technical issue, for IT functions that involve very large data sets, is the time required to upload or download the data. For example, at commonly available wide-area networking (WAN) rates, transferring multi-terabyte datasets to or form a public cloud could require multiple weeks, which would make the concept of migrating a high hurdle. This is a challenge that federal customers share with corporate customers, and technical solutions will undoubtedly be developed.

Resistance to change: Some of the trickier challenges faced when efficiency-seeking leaders push their IT staff to move some functions to a cloud are non-technical, relating to human nature. Some (not all!) IT staff resist changes to currently working practices that they control and understand. I suspect that, where it exists, this resistance will be stronger in consistently-funded government IT settings, where business-style pressures and incentives (e.g., bonuses) for innovative steps leading to tangible savings are not present. Simply demanding an IT change rarely yields desired outcomes, as unhappy IT staff can become inefficient in a variety of ways. A mixture of push (e.g., requests and insistent education) and pull (e.g., incentives) may be needed to effect rapid and positive adoption.

Perhaps the most common form for such resistance to take is aggressive arguing against the change in question, on technical grounds and by overstating the effort required to enact the change. The awkward aspects of such arguments are usually twofold: the IT staff raising them generally know more than anyone else in the organization about the technical issues in question, and the arguments raised generally are at least partially correct. A mixture of education (for the IT staff and their managers) and a technical mindshare (for both to utilize) may be needed to separate the legitimate concerns from those based primarily on a desire to avoid change.

The technical mindshare should also provide for sharing of effort on issues like certification/accreditation (e.g., for security issues discussed above), verifying continued good practices, negotiating Terms of Service (ToS), and procurement (e.g., multiple bids obtained

and okayed periodically). Forcing every agency to independently deal with such issues truly could become a significant barrier, but a shared clearinghouse is a natural way to eliminate redundant effort for common needs. Note that none of my discussion is meant to imply that actions, including those that I mention, are not already being pursued in the context of the Federal Cloud Computing Initiative; indeed, some are (e.g., see apps.gov).

IT culture changes: A consequence of moving to cloud computing is major change for IT staff. Note that even full transition to cloud computing would not mean elimination of all IT staff – not by a long shot. Expert IT personnel will be needed to assist with planning, to provision, and to manage IT functions outsourced to the cloud. But, the expertise that they will need is going to be different. Rather than expertise in managing the aspects now outsourced (e.g., physical computers, networks, and building-block applications), for example, IT staff and managers will need new expertise in working with cloud-based activities, projecting usage costs rather than capital costs, and there may be reduced separation between application engineers and IT staff. Continued education for IT personnel, and perhaps a new breed of staff, will be an important part of such transition.

Not only will new IT expertise be needed to manage functions outsourced to the cloud, but a hybrid IT model is most likely for quite some time – some functions will be moved to one or more clouds, while others remain "in house". Thus, the IT staff will need to manage a set of functions spread across multiple environments, using new integrated management tools. Creation of such tools can be expected, as particular cloud interfaces become very popular and/or standardized.

D. Concluding remarks

Cloud computing is an exciting realization of a long-sought concept: computing as a utility. Pursuing judicious use for federal IT functions is important, given the large potential benefits. Patience, perseverance, incremental adoption, and continued investment in research, education, and standardization related to cloud computing will be needed in realizing that potential. Some specific recommendations for consideration that follow from my observations include:

- First, cloud computing is a big change, and realizing its large potential will require significant formal technical and change management training for IT staff and managers. This need may warrant expansion or adaptation of programs like "scholarship for service" as well as targeted executive education initiatives.
- Second, standardization is important to address lock-in concerns, but continued experimentation (including research, testbeds, and case studies) and innovation are also crucial given the relative youth of cloud computing and the presence of unresolved technical questions (e.g., in security, data transfer, and management). The natural tension between these two needs may warrant focused programs for each in order to avoid lack of progress on either.
- Third, information and effort sharing across federal agencies considering cloud computing will be an important aspect of overcoming resistance to change. Explicit support should exist for shared technical mindshare, provider tracking/clearing, and case study reporting.

It is my hope that my testimony has helped to clarify some of the major technical matters and logistics associated with the idea of using cloud computing for federal IT. For non-technical practitioners, I recognize that digesting the concepts and evaluating the merits of cloud computing is no easy feat. Yet, I understand how important it is for members of the Committee to have trust and confidence in the IT directions taken by federal agencies, given the expense and mission importance of IT. As leaders in the realm of technology and innovation, please know that we at Carnegie Mellon University stand ready to assist you in dealing with technical questions as they relate to your efforts to craft sound public policy and oversee federal IT activities. We applaud your diligence in reviewing this specific matter.

Again, thank you for the opportunity to testify. I will be happy to answer any questions the Committee might have.

Chairman TOWNS. Thank you very much.

Let me thank all of you for your testimony.

I guess I just want to ask all of you this question, and you can sort of answer it as briefly as you possibly can. What do you see as the greatest benefit and the greatest risk to the Federal Government in terms of cloud computing? If you just go right down the line and sort of be as brief as possible.

Mr. CHARNEY. I see a couple of huge benefits. One, of course, we have talked about, which is cost savings. But the other huge benefit, I think, is that the aggregation of data will allow, in appropriate circumstances, much deeper analysis of data. When you think about how we are going to do health care in the future, for example, the ability to analyze a lot of data and see trends and other things could be hugely valuable to the Government.

In terms of risk, it really does come back to the things we have talked about: security, privacy, and reliability. We are going to be dependent on this cloud, and if you can't access this cloud, or if cyber criminals go after the cloud because the aggregation of data presents a rich target, or people don't have faith that the data in the cloud is both protected and not improvidently used by the cloud provider, we will lack trust.

Mr. BURTON. Yes, I think the benefits of cloud computing are enormous, and that is why it is really taking off in the private sector; and to look at those benefits: cost advantages, speed advantages, scale advantages, ease of use advantages, customization advantages, and, not to be overlooked, tremendous innovation advantages, because once people are on a cloud platform, you can easily develop new applications, you can deploy them instantly, you can share them with other agencies.

If you look at risk, usually at the top of the risk list is what this committee has focused on, and that is concerns about security and privacy.

Mr. BRADSHAW. I think there are great advantages to cloud computing. Innovation, innovation of features and functionality, but, more important, innovations around security, our ability to react much more quickly now to security threats. There are great cost savings as well for the taxpayer.

As far as risk, I do think we, right now, are in the risk of trying to label cloud computing a certain way so that we don't understand the security issues in it. We label it and dismiss it based on labels versus really what the security requirements are for the environment.

Mr. COMBS. Thank you, Mr. Chairman. I agree with all the comments that have previously been stated, but the greatest benefit, I think, is speed to delivery of capabilities, like Mr. Ganger brought up. Today, it takes far too long to implement new capabilities in organizations. With cloud computing we can rapidly implement capabilities and, therefore, keep up with the changing needs of the Government.

As far as the greatest risk, I have to go back to my intelligence community days, that is the loss of the information. In the intelligence community, in the Department of Defense realms, that loss of information can mean the loss of lives. In the commercial world,

that loss of information can be the loss of intellectual property and lots of money.

So those are the greatest benefits and the greatest risks as I see them. Thank you.

Mr. GANGER. I would say that the greatest benefit, as most have noted, is efficiency, efficiency both in terms of cost and in terms of the ability to roll out a new application, a new e-Government approach in each of the individual applications that one wants to get started, both of those forms of efficiency.

In terms of the greatest risk, I guess I am going to depart from a lot of people here and say that I would worry that the greatest risk is entrenchment and the difficulty that one has in making a transition from a comfort level that one has with the way they do things currently to something very different.

And given how widespread the IT functions of the Federal Government are already, we heard about 1,100 data centers, getting all those people around the idea of looking at cloud computing and seriously considering not doing it all themselves, it is a tough sell to do that with people, to get them to really seriously consider doing that. The security aspect is one of the concerns that will get raised, and there are legitimate security concerns, but the technical security concerns, to me, seem smaller than the entrenchment concerns that will be rallied around, for example, the security word.

Chairman TOWNS. Thank you very much.

I now yield 5 minutes to the ranking member from California.

Mr. ISSA. Thank you, Mr. Chairman.

Mr. Ganger, I am going to followup with you as the honest broker. Eleven hundred data centers. In your opinion, is there any reason that this committee shouldn't drive the bureaucracy toward, let's say, 200 data centers and force people who have 8, like GSA, to have 8 that are co-located within those 200 centers? And wouldn't that represent billions of dollars in savings and a consolidation toward a private cloud—which is the second question, since you are writing—which is aren't we big enough at $80 billion worth of total IT services, tens of billions of dollars worth of specific software support and $20 billion worth of infrastructure support, aren't we big enough to own our own cloud?

I don't want to quote, but I will, the Rolling Stones, 1967, when they said "Get off of my cloud," but why would we get onto somebody else's cloud to begin with? Why wouldn't we say we are big enough to go alone or to be co-located with other locations, but have complete segregation so that security is designed in from the door on?

Mr. GANGER. OK, so I will try to take them in the order that you gave them.

Mr. ISSA. No, no, take them in the order best for you.

Mr. GANGER. OK. So do you drive data center reductions? I don't have a lot of insight into what the 1,100 are doing. It would shock me to hear that an analysis of the 1,100 doesn't lead to being able to do 200, for example.

Mr. ISSA. Earlier testimony, it took a long time to find out how many they had and where they were in some cases.

Mr. GANGER. Which means, by the way, that it is going to take longer to do the consolidation than one might hope, right, because

there is going to have to be a lot of learning about what functions those different data centers are doing in order to make a consolidation actually work.

Mr. ISSA. But just shared bandwidth efficiency, facilities advantages, all of that would be in the hundreds of millions of dollars, enough to pay for the consolidation in a short period of time.

Mr. GANGER. Yes, absolutely, I agree. Huge advantages to be had there. And I would be really surprised to learn that type of consolidation couldn't be done and that those advantages couldn't be realized. The corporate world has done it and we have seen two examples of very large corporations that have gone from two and three digit numbers of data centers to single and 12 was the second example numbers of data centers.

In terms of is the Government big enough to do a private cloud, there is no question the Government is big enough to do a private cloud. The question that you would have to ask yourself isn't whether you are big enough to do it, it is whether you have the expertise to do it for all of the different types of cloud technologies that you might need to do it for.

Mr. ISSA. OK. I am going to move to the cloud folks for a moment.

Mr. Burton, you offer a public cloud solution that is already purchased by agencies of the Government, and they buy a product as a COTS product, basically. So that can proliferate with vendors offering them, and the only problem, of course, is certifying that the data they put on to your cloud is in fact safe, secure, and so on, right? Would you say that there are things like Mr. Combs might mention, the NSA or the CIA, that never really should be customers of yours, at least not with the same computer and the same location that are dealing in the clandestine world?

Mr. BURTON. Yes, I think without a doubt not only in the Federal Government, in the private sector there are certain data sets that are so secret, so sensitive that they will never go on to a multi-tenant cloud structure.

Mr. ISSA. There is a company in Atlanta called Coca-Cola. I suspect that is at least one formula you will never host.

Mr. Charney, in light of that, won't there always be some private computing facility-based, like some of our labs activities, where even the hard drives have to be removed between uses? So, in a sense, isn't this committee looking at the migration of public, private, and legacy, with an inevitability that one size doesn't fit all?

Mr. CHARNEY. I agree with that completely. I mean, there will be cases where organizations, Government agencies want to run an on-premises system and control it very tightly, like some of the intelligence communities. There will be places where the Government is a community of interest and can share a cloud, and there may be places for public information that a public cloud service is not a big concern because it is information you want to share anyway. The key is customer choice and mapping the cloud model to the risk model.

Mr. ISSA. Mr. Bradshaw, I understand that you are a super salesman, among other things. You would like to sell as much of your product as you can, I am sure. But wouldn't you also agree that there is a segment that could be moved sooner, rather than

later, to public cloud, a segment that needs to have that transition, and then a segment that will never, in the foreseeable future, make that transition?

Mr. BRADSHAW. I absolutely agree with that. We have aimed our initial offering at the sensitive, but unclassified, level to meet that or exceed it. But we do agree there are some things that we would not recommend you move to the public cloud.

Mr. ISSA. And I will close with one thing on behalf of the chairman and myself, both. Isn't one of the challenges to a truly transparent cloud, when it is pointed toward the public, that portion of cloud computing, the fact that all of our various Government agencies have failed to have standards that are interoperable and easily searchable so that you can know that a name or a particular cell in a data base will in fact correspond not just, but including Web sites?

Mr. BRADSHAW. I do believe it is very difficult to put standards in place that meet the requirements of all the individual agencies and individual bureaus within the agencies, and take advantage of information technology at the same time. That is a big challenge. But I do think we can use the current regulations that are in place, get a great understanding of how things compare, and then all of us, we have security experts in our company, let's take advantage of those and work with you to continuously update these through continuous monitoring and things like that.

Mr. ISSA. Thank you.

Anyone else before the chairman reclaims my time?

[No response.]

Mr. ISSA. Thank you all.

Chairman TOWNS. Thank you very much.

I now yield 5 minutes to the gentlewoman from California.

Ms. WATSON. Thank you.

As I mentioned in my opening statement, in light of the recently reported cyberattacks involving China and other nation states, I would like to hear some specifics from each one of our vendors about how we would protect our particular systems, and I would like specifics on how your companies plan to demonstrate compliance with the requirements on a regular basis. And I would just like you to go down the line.

And then I am going to ask, since we are not going to have time within this session to hold additional hearings in our subcommittee, how you would provide this information and would you give us kind of a summary in writing to our committee? And then we will submit that to your committee.

So just tell us in your own words about what you, as an individual vendor, would do to protect the security.

Mr. CHARNEY. I think there are really two parts to the question. First, in terms of how we protect security, the real key is having a documented information security program that looks at the assets you want to protect, what the threats to those assets are, and then you build and test a set of controls to protect those assets.

But the China question is a little bit difficult in the sense that one of the changes we have seen over the last 20 years is a major change in the threat model. When I was at the Justice Department prosecuting cyber crimes in 1991 and 1992, at the beginning of my

career there, a lot of the hackers were young students exploring networks.

Now we have what we call the advanced persistent threat; we see more and more nation state activity on the Internet, we see more organized crime activity on the Internet, we see a black market for vulnerabilities. A regular documented information security program that might be adequate for most commercial purposes may not be completely adequate for an advanced persistent threat.

This is why, for example, as I said earlier, I don't think the intelligence community should be parking its information on even public or shared tenant clouds. The advanced persistent threat is going to require a much more careful analysis and different cybersecurity strategies. I have, in fact, written a paper on this very point and would be happy to share it with the committee.

Mr. BURTON. Thank you for that question, Chairwoman Watson. Security is something that our smallest customers take very, very seriously; whether you are a corner pizza store maintaining your customer data or a multinational bank or health care company or an agency of the Federal Government.

Ms. WATSON. Let me be more specific. How do we have assurance that our Federal information within our systems can be protected? And I know this is not the place where you can give direct answers.

Mr. BURTON. I will respond to that.

Ms. WATSON. Good.

Mr. BURTON. Each of our customers can come in and do security reviews with Salesforce, and they do not go on to our platform until they are satisfied with our security. We comply with major international security standards, ISO27001, SAT Type 2 Systrust. All of those are available. We feel that without trust no one is going to use Salesforce.

So we have site. Anyone can look at it, this committee can look at it, Trust.Salesforce.com, and if you look at that site you can see what the performances of our system every single day. I looked at it this morning. We processed 315 million transactions yesterday, each one in about 300 milliseconds on that site. You can see the types of security attacks we are facing; you can see all of our credentials.

If you want to lock down your security, it provides you who to talk to, how to get at that. So we feel that not only security standards, but transparency is critical to the whole cloud model, and that is why we have this trust site that is available for anyone to look at.

And I think just the one question, to come back really, I think, to a comment Mr. Issa raised, is, yes, there, are some data sets that are so sensitive, so secret that they should be kept outside of a cloud environment.

But I think if you look at the vast majority of the data that the U.S. Federal Government processes and stores, it falls into a lower level of security, and I think that is perfectly adequate for a strong vendor with good security to manage on a multi-tenant platform in a cloud.

Mr. BRADSHAW. Thank you. Google has made a commitment at the executive level of the corporation to meet Federal security requirements. We have completed and submitted to the Government

our FISMA certification package and we are waiting to hear. We do meet the security and privacy requirements that are laid out in the Federal statute under FISMA and we make those findings available upon request.

I think what we also do, we are so focused on security. We all know this is a growing threat for everybody. We look at two areas, one is reducing the threat environment. So we are very focused on bringing down things that had been exploited in the past, trying to limit that, limit the doors that have made these threats possible; and then looking at moving some appropriate data to an environment where we can take our security professionals and we can take just multiple layers of security and protect that data for you.

Ms. WATSON. You are so out there, that is why I mentioned Google, because I say to myself would you Google that, please, quickly. We know the problems that all of you are facing, so I just want to get some ideas how you are addressing them.

Mr. Combs.

Mr. COMBS. Thank you, ma'am. Today's security architectures are nothing more than a broken safety net of point security solution products. We have to move from point security products to an information-centric approach to managing our data. It is all about two things: it is about identities.

Those systems and processes that either need to have access or be restricted access to our resources, and the information. That information must be either available or restricted however an organization's policies defines. That gets into your second part, which is Government risk and compliance.

What we are doing at EMC is we have acquired technologies and we are further developing them to allow portlets for organizations to look inside our cloud offerings and to ensure that we are providing the Government the risk and compliance capabilities that matches their requirements.

Ms. WATSON. What I am going to advise my staff to do is send letters to all of you, and you can respond to the questions that we have in your letters. So you will get something and we will try to do it as soon as possible.

Thank you so very much, and thank you, Mr. Chairman, for the time.

Chairman TOWNS. Thank you very much.

I now yield to the gentleman from Utah, Mr. Chaffetz.

Mr. CHAFFETZ. I like the enthusiasm, Mr. Chairman. I appreciate that.

Thank you all for being here, I appreciate it. Full disclosure: I think I have been a consumer of all of your products and services, with the exception of the parallel data lab. I can't think of something, although you probably have something I have consumed along the way, all with great success. You are obviously market leaders and we appreciate your perspective here, and we won't do it justice in the 5-minutes, so if there is additional information you want to share with us, please know that we would love to have you followup on that.

Mr. Bradshaw, starting with you if I could, in your written testimony you say, "The most important component of feeling comfortable with one's data in the cloud is trusting a cloud services

provider and the practices and policies they have in place." Ronald Reagan famously said once, trust but verify.

How does that work in a government-type model? Because the second part of my questions is how does Google, which is so unique in all the world, how does your business model fit with government types of services, where you have relied a lot on getting a lot of eyeballs and then converting those into advertising dollars? How does that work in a business model with the Federal Government or State government?

But going back to this, OK, it is great to say, hey, trust us, that is the most important thing, but how do we gain a comfort level that information is secure?

Mr. BRADSHAW. I agree with you on that. First of all, I am in a group called Enterprise, which is a separate group from the consumer group you are very familiar with. We actually look at the consumer products and determine how we can change them so they fit into a government or into a commercial environment. So the products are slightly different and they are modified for that reason.

As far as trust, we understand this is the biggest thing for you on security and privacy, so we try to be as transparent as possible. I think sometimes we make sure we put something out in a blog as soon as we find it so that you will understand what kind of problem we have. I think the benefit of that to you, and to me as well, is that the technology allows us to very quickly react to some of these attacks that we have seen, look at the situation, and then correct it, and immediately make that fix available to a lot of people. So, again, this is where the innovation just really plays to this increasing threat model we are all seeing.

Mr. CHAFFETZ. And that is where I think one of the interesting questions going forward, is how do those cloud-oriented companies, and in their business model, how do they make that work. We will have to explore that further.

The GAO, in their report, reported that 23 out of 24 agencies identified multi-tenancy as a potential information security risk. Do you find that? Is that baseless or is that something you would concur with?

Mr. BRADSHAW. I don't concur with this. I think we have many examples where we have multi-tenant application solutions that we use and we are very comfortable with, such as an ATM, you know, a banking system where multiple people are in the same system. We are very comfortable with that. I think the Government has several examples where they have solutions they have been using for years where they are multi-tenant.

So I think you can gain so many benefits from this environment, again, because we are putting the data in one location and we are putting multiple layers around it.

Mr. CHAFFETZ. Mr. Charney, how would you address that, the GAO concern?

Mr. CHARNEY. I think multi-tenancy can be fine, but I think it also raises different threat models, and the ATM analogy is not quite right; and the reason for that is I can go up to an ATM machine and put in my card and take out money, and it may be true that my account is stored with other accounts, but the ATM is not

a platform on which I can load software. There has been some research done where academics have basically hosted in the cloud applications designed to attack the rest of the cloud, and with multi-tenancy in that environment, virtualization becomes key to separating the data.

So it doesn't mean multi-tenancy is dangerous; what it means is it presents a different threat model and you need to make sure you are mitigating those threats.

Mr. CHAFFETZ. So what are those technologies that ought to be highlighted in terms of differentiating?

Mr. CHARNEY. I think there are a few things. The key thing, of course, is that you have secured development of the virtualization technology; that the people who are developing that technology are trained in security and that they use good development practices and security to make sure that the containers that are built through virtualization are in fact robust.

Mr. CHAFFETZ. Do we possibly have enough personnel in order to achieve that? I mean, it is hard enough to hire as it is in some of these specialized fields.

Mr. CHARNEY. Many years ago, when Microsoft adopted the Security Development Lifecycle, we took the view that, basically, keeping it to ourselves for competitive advantage was the wrong approach. We decided that what we needed to do was share our best practices.

And what we did was we published books on threat modeling, unsecured code development, and on the Security Development Lifecycle itself; and we published some of the tools we use in Visual Studio, which is our product for developers, and we have also made tools publicly available, like our threat modeling tool. We believe that there are not enough well-trained security experts on the planet today, and it is something the Government can help address as well.

Mr. CHAFFETZ. Mr. Chairman, thank you.

I can spend hours with each of you, but thank you for your time, and appreciate any followup. Thank you.

Ms. WATSON [presiding]. I would like now to yield 5 minutes to our distinguished member, Mr. Bilbray.

Mr. BILBRAY. Thank you, Madam Chair.

I want to followup on my colleague's comments about this exposure, I guess it was 23 out of 24. That really kind of makes us focus on the task at hand when we have that kind of exposure, and I again would like to followup by asking why you think we have these risks but, more importantly, what can we do to address these risks and try to avoid impact by them? Basically, how do we armor the system and protect the system?

Mr. CHARNEY. I think in part there is a lot of concern because the technology is new and evolving. Therefore, we are not familiar with the risks and, undoubtedly, what will sometimes occur is we will learn new things along the way. I think there is a natural and healthy tendency to say I need to protect my data, and I may put it in this new environment that has these new threat models that I don't fully understand.

The way to address that is through transparency; that is, that the cloud providers need to be transparent about how they run

their operations and manage their information security program, and governments need to be clear about what their requirements are so that both parties to the transaction get greater comfort level with both what they are trying to protect, what they think is needed to protect it, and whether those controls are in place.

Mr. BILBRAY. Before we go on, let me just say, Madam Chair, it is kind of just reminding me of when I got here in 1995 and the leadership was changing after 40 years, that there were a lot of members of the previous majority that actually were terrified at the concept of having Internet between offices and among offices because they were worried about security. Literally, that was the fear at that time.

Of course, at the same time we were still delivering buckets of ice, 95 years after the invention of refrigeration, but that fear was there even among Members of Congress as late as 1995, and I am sure it has been much more recent than that.

Mr. Burton, you had a comment.

Mr. BURTON. Yes. I would very much like to comment on that question. Multi-tenant cloud computing is a mature technology. Salesforce has been doing this since its founding 10 years ago, and you have major banks, major health care companies running mission-critical applications on this platform today. Gardner says 25 percent of all new software sales are going to be softwares of service cloud computing next year.

So I think while there are issues to consider, it is a mistake to say this is new, this is unproven, this is untested, don't go there. This has been tried and proven successfully in the marketplace.

I think the key question about multi-tenancy, the key question about security is know your vendor. Does the cloud provider let you do deep security reviews? Does it have international security standards? Does it have transparency and trust so that you can go in and see what is going on? And I think as government agencies start exploring this, they will find that, in fact, there are some cloud providers that provide that today. There are lots of others who don't. There are lots of issues.

We are going to be discussing this for some time, but I don't want this committee to leave with the impression that somehow multi-tenant cloud computing is not tested, it is new, it is not to be trusted, because I think the marketplace has already ruled on that and the marketplace is moving in a major way toward this new platform.

Mr. BRADSHAW. I also would like to point out I think something like FISMA provides a great way of evaluating the current systems we have against this new technology right now, so we can take a look at what we are facing with the current environment and put it right next to what we get, what benefits we get from it. FISMA has independent audits in there, we have that third-party audit, so it gives you a great way of looking and comparing this system to what is available to you right now.

Mr. COMBS. Why do we have these risks? There is no doubt that our adversaries can penetrate our networks and gain access to the resources that we have.

Chairwoman Watson, you brought the Chinese up in your opening statement. It is absolutely proven time and time again that we

cannot stop our adversaries from getting into systems that are available on the open Internet.

This is why I say that moving information into the public cloud should be limited to the information that is public-facing information. The internal information, the engineering, the intellectual property, the sensitive information that exists in our Government needs to be protected behind appropriate security measures to prevent us from getting into big trouble.

Ms. WATSON. Thank you.

Mr. Issa, you will have the last comment and question, and then after that we will be adjourning; we have two votes or three votes, as I understand, at 2.

Mr. ISSA. And I will be brief.

Mr. Combs, in a compartmented world, the term compartmented exists for a reason. Would you briefly, in light of a multi-tenant environment, if, hypothetically, all of Government was all in the cloud and, because of government-to-government requirements, interlaced, what would happen to the historic compartmenting that we rely on in the intelligence world today?

Mr. COMBS. Mr. Issa, there are ways to bring cloud computing into those environments. The consolidated data centers that are going on within the Directorate of National Intelligence today, these are similar security requirements across the intelligence community.

We can develop and deploy private cloud environments in a multi-tenant environment that will allow the security controls to be protected in that environment. Across NASA, NASA is going through a 110 data center consolidation right now. Much of their engineering processes today are similar, yet they have 110 separate data centers.

Mr. ISSA. I think you have answered the question. I want to be brief for the Chairlady.

Mr. Bradshaw, responsible disclosure, when companies discover flaws in each other's software, does your company have a stated policy for how that is to be done?

Mr. BRADSHAW. We do make security and privacy statements. We definitely try to be as transparent as we possibly can.

Mr. ISSA. No, that wasn't the question, sir. All of the software companies that interact get access to various portions of each other's source code and interface with it for purposes of porting software, going back and forth through data bases and so forth.

Does Google have a responsible disclosure policy as to discoveries of opportunistic or whatever security failures? How do you inform Sun or somebody else that you found something that would be a vulnerability to the outside world if it were discovered? You have teams of software producers, as does Microsoft, as does Salesforce. What is your stated policy or do you have a stated policy if a software engineer discovers a vulnerability in somebody else's software?

Mr. BRADSHAW. I can't personally state the policy, but I will be glad to get that back to you.

Mr. ISSA. If you would respond to that for the record. Actually, if all of your companies would. It is an area of deep concern to me, mostly because I understand the Chinese are out there trying to

penetrate us. I find it interesting that sometimes the penetrations end up in blogs and they really come from software engineers employed by competitors.

And as long as we are buying from all of the companies, the one thing we don't want is a vulnerability created at our expense in a competitive environment. So if each of you would respond to the extent it is appropriate to your company.

Ms. WATSON. Let me ask that each of you will respond in writing. We have all framed the question, if that is all right with you.

Mr. ISSA. That would be great.

Ms. WATSON. Because that is a vote.

Mr. ISSA. OK, and I have one closing one only for the record, and it is for Google. The Presidential Records Act requires that we capture all emails of the President and their entire Office of the President. Could you respond for the record of how you are capturing Gemails that are being used in and around the White House by White House personnel?

Mr. BRADSHAW. I am in a group, again, that sells a product to the Federal Government, but it is not the Gmail system, the personal Gmail system. In our group, in our organization, we have a tool that allows you to do e-discovery as well as archiving for our mail product.

Mr. ISSA. And I was talking about specific examples of what is going on relative to use of the public Gmail. So if you could respond for the record. Thank you.

Ms. WATSON. All right, thank you so much for your questions, Mr. Issa.

I want to thank the witnesses for your testimony, the time that you have spent here. We are sorry for the interruptions, but this is the Congress and we do have to go to vote.

Thank you, audience, for hanging in here with us. The meeting is now adjourned and we will put our comments and questions in writing to you. Thank you.

[Whereupon, at 2:07 p.m., the committee and subcommittee was adjourned.]

[The prepared statement of Hon. Gerald E. Connolly and additional information submitted for the hearing record follow:]

Opening Statement of Congressman Gerald E. Connolly

"Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud"

July 1, 2010

Thank you, Chairman Towns and Chairwoman Watson for holding this important hearing. Cloud computing offers the federal government several potential benefits: savings related to economies of scale, avoided capital investment obligations, and reduced service disruptions due to superior resiliency of the cloud compared to a single server or data center. In addition, moving to the cloud offers an opportunity to enhance federal information security and information management in-house expertise, if contracts are structured correctly. We know that our security management systems have failed, based on extensive hearings held by Ms. Watson's subcommittee. Her legislation, entitled the FISMA Amendments Act, will certainly improve our information security, but cloud data storage and processing offers another opportunity to shift away from failed information security systems.

The means by which federal agencies shift to cloud computing is critically important. If we simply outsource data storage and processing to private firms, we may achieve economies of scale but will remain dependent on private firms for both security and technological expertise. Instead, we should structure contracts so that federal security managers have a role in monitoring and enhancing cybersecurity. This will strengthen our in-house capacity and allow us to reassure Americans that we aren't simply accepting private companies' assurances that they will secure our systems. We must trust and verify those assertions.

Fortunately, it is realistic to make major improvements to our cybersecurity by shifting to a cloud. Currently, the federal government possesses a hodgepodge of servers and data centers. If our security systems could be compared to a fortress, then the numerous data centers, patches, updates, and points of access are like building dozens of doors and gates in the walls of the fortress. By comparison, consolidating data management and storage to the cloud reduces the vulnerable points that could be used by hackers. Conversely, those fewer access points must be robust against attack, necessitating a strong partnership between agencies and the private sector to provide information security.

We know that the status quo is unacceptable, and have already taken steps to improve information security. We should take the next step, using private sector expertise to enhance both security and in-house capacity to protect sensitive information of the government and our constituents.

Supplemental Written Testimony of
Gregory R. Ganger
Professor of Electrical & Computer Engineering and Computer Science,
Carnegie Mellon University

United States House of Representatives
Committee on Oversight and Government Reform
Subcommittee on Government Management, Organization, and Procurement
Hearing on
Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud
July 1, 2010

I thank you for the opportunity to testify about the benefits and risks of using cloud computing for federal IT functions. I hope that the information that I and the other panelists were able to share helps in your deliberations on cloud computing and its role in federal IT.

Under time pressures, there were a number of topics for which a small amount of follow-up comment may be helpful. To provide deeper answers to some of the questions posed during the hearing, I would like to provide this brief follow-up.

Greatest benefit and greatest risk: Chairperson Towns posed the always-tough challenge of identifying the one greatest benefit and one greatest risk. Like most, I identified "efficiency improvement" as the greatest benefit, encapsulating both reduced application deployment time/effort and reduced overall IT costs in that response.

Departing from most, though, I indicated that the greatest risk is not that using cloud computing will be bad in some major way (e.g., security), given judicious decisions regarding its use, but that human factors can make the transition go badly. If not well managed, a push for change can cause expenses and delays that far exceed the potential benefits.

I used the word "entrenchment" to summarize the sources of this risk. During the hearing, Mr. Issa mentioned his concerns about one type of those sources: bureaucracy, which can eliminate many potential efficiency benefits and make transition take much longer than necessary. In addition, IT staff and managers who are not "on board" with a major change to their existing work culture can severely dampen the benefits by working against the change in various passive and active manners – resistance to change is human nature. Worse, these

sources can feed one another, in a vicious cycle that wastes many resources without realizing benefits.

Substantial change is difficult, and increasingly so for large organizations with deeply entrenched status quo and many largely-independent sub-organizations. The federal government is, of course, known for both. Navigating this change and realizing its potential benefits will require your strong leadership, including extensive change management, information and success story sharing, mechanisms for reducing duplicated ramp-up efforts, and incentives for doing the right thing. My original written testimony discussed these issues in more depth. Carefully distinguishing between real concerns in need of policy guidance, of which there will be some, and artificial concerns raised by those seeking to avoid change will also be crucial.

Should there be a federal private cloud: Mr. Issa wisely noted that the aggregate size of federal IT is such that the efficiency benefits arising from economies of scale and multi-tenancy could be achieved with a private cloud. Indeed, I agree with that thinking.

Mr. Issa also posed the natural companion question to that insight: should we (the federal government) do our own? In my opinion, the answer is "yes, but it should be one of several options used for federal IT functions". That is, there should be federal private clouds used for some IT functions, while others use public cloud resources and still others do not use cloud computing at all. IT functions, and their associated requirements, are diverse. Which solutions can work for any given IT function, and the trade-offs between them, argue for ensuring that all viable options are available for consideration – otherwise, we may end up paying (much) more than is necessary, suffering longer application development times, etc.

Mr. Issa's questions do highlight another key point: a private federal cloud can help ease the transition of federal IT functions to cloud computing. By allowing "not entirely done by agency X" to be tackled without the "not entirely done by federal IT staff" worries (e.g., security concerns), some will be more willing to act sooner. This is a concept worth pursuing, including with continued pursuit of current federal private cloud efforts (e.g., the NBC cloud at http://cloud.nbc.com/). For IaaS-type clouds, in particular, this could be done while regularly benchmarking efficiency against corporate offerings.

At the same time, I think that it is important to not have the entire cloud computing agenda focus on private cloud efforts. There are some mature cloud providers that offer public cloud computing services that would require huge investments in time and money to replicate. It may make sense to do so, in certain cases, but the more efficient alternative (in time and money) will often be to purchase public cloud resources.

Security and the public cloud: Multiple members raised important questions regarding security, and the discussion on that topic will certainly continue. I wanted to comment on a couple of aspects of the security discussions during the hearing.

First, there appeared to be universal agreement that certain data would not be appropriate for public clouds, with the clearest example being highly-classified data critical to national security. At the other end of the spectrum, there is much data that is in fact intended to be available to the public. Much of the data in between can be used with public cloud computing, given careful matching of security needs to vendor practices.

Second, there appeared to be more open-ended mystery to what security consequences exist with use of a public cloud than is warranted. I see two primary changes that affect security and one that could affect privacy:

- the first change that can affect security is that the provider of a public cloud is not a federal agency. Therefore, it is possible that the provider will not implement the expected security mechanisms. But, this concern must be considered in the context of two facts: corporate providers have access to, and most generally utilize, the same security technologies and best practices as federal IT staff; also, indications (including those offered during testimony at the hearing) are that much federal IT is no more secure than corporate environments. The focus regarding this concern should be on mechanisms for accreditation and verification of provider security practices and comparison of those to requirements for any given federal IT function.
- the second change that can affect security is multi-tenancy, and particularly sharing of the cloud with non-federal tenants. This change introduces a greater (theoretical) possibility that other tenants could steal federal IT data, manipulate application execution, or deduce aspects of them. This is largely a technical concern, which can

be addressed by well-implemented virtualization technologies for isolating the data and activities of tenants, despite resource sharing.

- the primary potential privacy issue, particularly with SaaS and PaaS cloud computing, is logging of user accesses (e.g., as is done for targeted avertising). Some of the larger cloud providers have built businesses around advertising revenue, and they have extensive built-in log collection and processing architectures. Use of such clouds may require careful consideration of citizen privacy as it relates to citizen access to federal websites and e-government functionalities.

Each of these issues does merit discussion, and any of them may prevent movement of some federal IT functions to some types of public cloud. But, continuation of the Committee's process of carefully understanding these issues before creating policy regarding them will be important. For many federal IT functions, these issues should not be showstoppers for judicious use of public cloud computing.

Concluding remark

Again, thank you for the opportunity to testify. I will be happy to answer any follow-up questions the Committee might have.

Google Inc.
1101 New York Avenue, N.W.
Second Floor
Washington, DC 20005

Main 202 346.1100
Fax 202 346.1101
www.google.com

July 21, 2010

The Honorable Darrell Issa
Ranking Member, Committee on Oversight and Government Reform
United States House of Representatives
2347 Rayburn House Office Building
Washington, DC 20515

Ranking Member Issa:

Thank you for your July 9, 2010 letter inquiring about Google's policies for retaining electronic records, complying with subpoenas from law enforcement agencies, and federal records statutes. I appreciate the opportunity to respond.

1. Identify and describe Google, Inc.'s policy for retaining electronic records, such as emails transmitted through the public Gmail system.

At Google, we seek to consolidate for users the information pertinent to our retention and usage policies in our Privacy Center, which can be accessed at www.google.com/privacy.html. Among the information posted in the Privacy Center is the Google Privacy Policy as well as specific privacy policies for Gmail and the other services that we offer. I have enclosed as attachments to this letter printouts from the Privacy Center homepage, the general Google Privacy Policy, and the Gmail Privacy Policy.

2. How long are emails retained or retrievable after a user deletes an email from their public Gmail account?

It is our policy that when a user deletes an email it may take up to 60 days for the email to be deleted from our active servers and the email may remain in our offline backup systems. For those users who may use additional Gmail features, such as Chat, which connects to the Google Talk network, or Google Buzz, the retention time for communications made through those applications may vary depending on individual user preference. Users can find any of our application-specific policies in the Privacy Center referenced above and clearly linked to at the bottom of each application's landing page.

3. Identify and describe Google, Inc.'s procedures for complying with subpoenas from law enforcement agencies.

We have a team specifically trained to evaluate and respond to law enforcement requests for user data when they are received. The documents enclosed as attachments in response to Question 1 also describe under the heading "Information Sharing" that, as part of our policy of protecting user data, we limit disclosure of user information to situations where:

> We have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or

enforceable governmental request, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against harm to the rights, property or safety of Google, its users or the public as required or permitted by law.

Once we receive a request, we first check to make sure it meets both the letter and spirit of the law before complying. We notify affected users about requests for user data that may affect them if doing so does not jeopardize an ongoing investigation and is allowed by law. If we believe a request is overly broad we will seek to narrow it.

4. Has the White House or any federal agency contacted Google about retention of emails sent by personnel covered by the PRA or Federal Records Act?

We understand your concern about the government's compliance with the Presidential Records Act and the Federal Records Act and appreciate the importance of those statutes in preserving a historical record of the federal government's actions. We have a policy of not disclosing, even to another agency or branch of the government, whether we have received governmental requests about particular users. This is to ensure that we protect the privacy of our users, do not jeopardize ongoing investigations, and comply with any applicable legal limitations on disclosure.

We trust that this letter is responsive to your concerns. Again, thank you for these additional questions and for the chance to testify on how cloud computing will improve security and efficiency for the federal government while saving money for the taxpayer.

Sincerely,

Mike Bradshaw
Director, Google Federal
Google Inc.

Encl.
cc: The Honorable Edolphus Towns, Chairman, Committee on Oversight and Government Reform

Printed on 100% post consumer waste recycled paper

Google Privacy Center

Privacy Center

- Privacy Policy
- FAQ
- Blog posts
- Principles
- Videos

Privacy Tools

- Dashboard
- Ads Preferences Manager
- Analytics Opt-out

Terms of Service

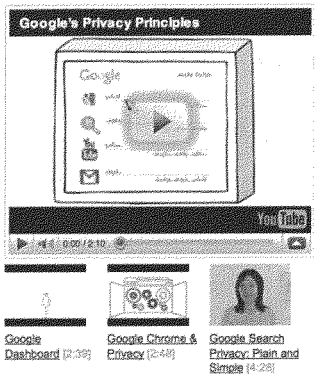
Transparency and Choice

At Google, we are keenly aware of the trust you place in us and our responsibility to protect your privacy. As part of this responsibility, we let you know what information we collect when you use our products and services, why we collect it and how we use it to improve your experience.

We have 5 privacy principles that describe how we approach privacy and user information across all of our products:

1. Use information to provide our users with valuable products and services.
2. Develop products that reflect strong privacy standards and practices.
3. Make the collection of personal information transparent.
4. Give users meaningful choices to protect their privacy.
5. Be a responsible steward of the information we hold.

This Privacy Center was created to provide you with easy-to-understand information about our products and policies to help you make more informed choices about which products you use, how to use them, and what information you provide to us.



Privacy policies

Google's Privacy Policy describes how we treat personal information when you use Google's products and services.

The following statements explain specific privacy practices with respect to certain products and services:

3D Warehouse	Desktop	Location Service in Firefox	Sites
Advertising	Docs	Maps	Store
App Engine	Firefox Extensions	Mobile	Talk
Apps	Gears	Moderator	Tasks
Blogger	Gmail	O3D	Toolbar
Books	GOOG-411	Orkut	Trader
Buzz	Google Web Toolkit	Personalized Search	Translator Toolkit
Calendar	Groups	Picasa	Voice
Checkout	Health	Postini	Web Accelerator
Chrome	iGoogle	PowerMeter	YouTube
Chrome Frame	Knol	Safe Browsing	
Comparison ads			

©2010 Google - About Google - Feedback

Google

Privacy Center

Privacy Policy

Last modified: March 11, 2009 (view archived versions)

At Google we recognize that privacy is important. This Privacy Policy applies to all of the products, services and websites offered by Google Inc. or its subsidiaries or affiliated companies except DoubleClick (DoubleClick Privacy Policy) and Postini (Postini Privacy Policy); collectively, Google's "services." In addition, where more detailed information is needed to explain our privacy practices, we post supplementary privacy notices to describe how particular services process personal information. These notices can be found in the Google Privacy Center.

Google adheres to the US Safe Harbor Privacy Principles of Notice, Choice, Onward Transfer, Security, Data Integrity, Access and Enforcement, and is registered with the U.S. Department of Commerce's Safe Harbor Program.

If you have any questions about this Privacy Policy, please feel free to contact us through our website or write to us at

Privacy Matters
c/o Google Inc.
1600 Amphitheatre Parkway
Mountain View, California, 94043
USA

Information we collect and how we use it

We offer a number of services that do not require you to register for an account or provide any personal information to us, such as Google Search. In order to provide our full range of services, we may collect the following types of information:

- **Information you provide** – When you sign up for a Google Account or other Google

service or promotion that requires registration, we ask you for personal information (such as your name, email address and an account password). For certain services, such as our advertising programs, we also request credit card or other payment account information which we maintain in encrypted form on secure servers. We may combine the information you submit under your account with information from other Google services or third parties in order to provide you with a better experience and to improve the quality of our services. For certain services, we may give you the opportunity to opt out of combining such information.

- **Cookies** – When you visit Google, we send one or more cookies – a small file containing a string of characters – to your computer or other device that uniquely identifies your browser. We use cookies to improve the quality of our service, including for storing user preferences, improving search results and ad selection, and tracking user trends, such as how people search. Google also uses cookies in its advertising services to help advertisers and publishers serve and manage ads across the web. We may set one or more cookies in your browser when you visit a website, including Google sites that use our advertising cookies, and view or click on an ad supported by Google's advertising services.
- **Log information** – When you access Google services, our servers automatically record information that your browser sends whenever you visit a website. These server logs may include information such as your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.
- **User communications** – When you send email or other communications to Google, we may retain those communications in order to process your inquiries, respond to your requests and improve our services.
- **Affiliated Google Services on other sites** – We offer some of our services on or through other web sites. Personal information that you provide to those sites may be sent to Google in order to deliver the service. We process such information under this Privacy Policy. The affiliated sites through which our services are offered may have different privacy practices and we encourage you to read their privacy policies.
- **Gadgets** – Google may make available third party applications through its services. The information collected by Google when you enable a gadget or other application is processed under this Privacy Policy. Information collected by the application or gadget provider is governed by their privacy policies.
- **Location data** – Google offers location-enabled services, such as Google Maps for mobile. If you use those services, Google may receive information about your actual

location (such as GPS signals sent by a mobile device) or information that can be used to approximate a location (such as a cell ID).

- **Links** – Google may present links in a format that enables us to keep track of whether these links have been followed. We use this information to improve the quality of our search technology, customized content and advertising. Read more information about links and redirected URLs.
- **Other sites** – This Privacy Policy applies to Google services only. We do not exercise control over the sites displayed as search results, sites that include Google applications, products or services, or links from within our various services. These other sites may place their own cookies or other files on your computer, collect data or solicit personal information from you.

Google only processes personal information for the purposes described in this Privacy Policy and/or the supplementary privacy notices for specific services. In addition to the above, such purposes include:

- Providing our services, including the display of customized content and advertising;
- Auditing, research and analysis in order to maintain, protect and improve our services;
- Ensuring the technical functioning of our network;
- Protecting the rights or property of Google or our users; and
- Developing new services.

You can find more information about how we process personal information by referring to the supplementary privacy notices for particular services.

Google processes personal information on our servers in the United States of America and in other countries. In some cases, we process personal information on a server outside your own country. We may process personal information to provide our own services. In some cases, we may process personal information on behalf of and according to the instructions of a third party, such as our advertising partners.

Choices for personal information

When you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use.

If we propose to use personal information for any purposes other than those described in

this Privacy Policy and/or in the specific service privacy notices, we will offer you an effective way to opt out of the use of personal information for those other purposes. We will not collect or use sensitive information for purposes other than those described in this Privacy Policy and/or in the supplementary service privacy notices, unless we have obtained your prior consent.

Most browsers are initially set up to accept cookies, but you can reset your browser to refuse all cookies or to indicate when a cookie is being sent. However, some Google features and services may not function properly if your cookies are disabled.

Google uses the DoubleClick advertising cookie on AdSense partner sites and certain Google services to help advertisers and publishers serve and manage ads across the web. You can view, edit, and manage your ads preferences associated with this cookie by accessing the Ads Preferences Manager. In addition, you may choose to opt out of the DoubleClick cookie at any time by using DoubleClick's opt-out cookie.

You can decline to submit personal information to any of our services, in which case Google may not be able to provide those services to you.

Information sharing

Google only shares personal information with other companies or individuals outside of Google in the following limited circumstances:

- We have your consent. We require opt-in consent for the sharing of any sensitive personal information.
- We provide such information to our subsidiaries, affiliated companies or other trusted businesses or persons for the purpose of processing personal information on our behalf. We require that these parties agree to process such information based on our instructions and in compliance with this Privacy Policy and any other appropriate confidentiality and security measures.
- We have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against harm to the rights, property or safety of Google, its users or the public as required or permitted by law.

If Google becomes involved in a merger, acquisition, or any form of sale of some or all of its assets, we will ensure the confidentiality of any personal information involved in such transactions and provide notice before personal information is transferred and becomes subject to a different privacy policy.

We may share with third parties certain pieces of aggregated, non-personal information, such as the number of users who searched for a particular term, for example, or how many users clicked on a particular advertisement. Such information does not identify you individually.

Please contact us at the address below for any additional questions about the management or use of personal data.

Information security

We take appropriate security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of data. These include internal reviews of our data collection, storage and processing practices and security measures, as well as physical security measures to guard against unauthorized access to systems where we store personal data.

We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to operate, develop or improve our services. These individuals are bound by confidentiality obligations and may be subject to discipline, including termination and criminal prosecution, if they fail to meet these obligations.

Data integrity

Google processes personal information only for the purposes for which it was collected and in accordance with this Privacy Policy or any applicable service-specific privacy notice. We review our data collection, storage and processing practices to ensure that we only collect, store and process the personal information needed to provide or improve our services or as otherwise permitted under this Policy. We take reasonable steps to ensure that the personal information we process is accurate, complete, and current, but we depend on our users to update or correct their personal information whenever necessary.

Accessing and updating personal information

When you use Google services, we make good faith efforts to provide you with access to your personal information and either to correct this data if it is inaccurate or to delete such data at your request if it is not otherwise required to be retained by law or for legitimate business purposes. We ask individual users to identify themselves and the information requested to be accessed, corrected or removed before processing such requests, and we may decline to process requests that are unreasonably repetitive or systematic, require disproportionate technical effort, jeopardize the privacy of others, or would be extremely impractical (for instance, requests concerning information residing on backup tapes), or for which access is not otherwise required. In any case where we provide information access and correction, we perform this service free of charge, except if doing so would require a disproportionate effort. Some of our services have different procedures to access, correct or delete users' personal information. We provide the details for these procedures in the specific privacy notices or FAQs for these services.

Enforcement

Google regularly reviews its compliance with this Privacy Policy. Please feel free to direct any questions or concerns regarding this Privacy Policy or Google's treatment of personal information by contacting us through this web site or by writing to us at

Privacy Matters
c/o Google Inc.
1600 Amphitheatre Parkway
Mountain View, California, 94043
USA

When we receive formal written complaints at this address, it is Google's policy to contact the complaining user regarding his or her concerns. We will cooperate with the appropriate regulatory authorities, including local data protection authorities, to resolve any complaints regarding the transfer of personal data that cannot be resolved between Google and an individual.

Changes to this Privacy Policy

Please note that this Privacy Policy may change from time to time. We will not reduce your rights under this Privacy Policy without your explicit consent, and we expect most such changes will be minor. Regardless, we will post any Privacy Policy changes on this page

and, if the changes are significant, we will provide a more prominent notice (including, for certain services, email notification of Privacy Policy changes). Each version of this Privacy Policy will be identified at the top of the page by its effective date, and we will also keep prior versions of this Privacy Policy in an archive for your review.

If you have any additional questions or concerns about this Privacy Policy, please feel free to contact us any time through this web site or at

Privacy Matters
c/o Google Inc.
1600 Amphitheatre Parkway
Mountain View, California, 94043
USA
©2010 Google - About Google - Feedback

Gmail by Google

Gmail: Google's approach to email

Gmail Privacy Notice

February 9, 2010

The Google Privacy Policy describes how we treat personal information when you use Google's products and services, including information provided when you use Gmail. In addition, the following describes our privacy practices that are specific to Gmail.

Personal information

- You need a Google Account to access Gmail. Google asks for some personal information when you create a Google Account, including your alternate contact information and a password, which is used to protect your account from unauthorized access. A Google Account allows you to access many of our services that require registration.
- Gmail stores, processes and maintains your messages, contact lists and other data related to your account in order to provide the service to you.
- When you use Gmail, Google's servers automatically record certain information about your use of Gmail. Similar to other web services, Google records information such as account activity (including storage usage, number of log-ins), data displayed or clicked on (including UI elements, ads, links); and other log information (including browser type, IP-address, date and time of access, cookie ID, and referrer URL).

Uses

- Google maintains and processes your Gmail account and its contents to provide the Gmail service to you and to improve our services. The Gmail service includes relevant advertising and related links based on the IP address, content of messages and other information related to your use of Gmail.
- Google's computers process the information in your messages for various purposes, including formatting and displaying the information to you, delivering advertisements and related links, preventing unsolicited bulk email (spam), backing up your messages, and other purposes relating to offering you Gmail.
- Google may send you information related to your Gmail account or other Google services.

Information sharing and onward transfer

- When you send email, Google includes information such as your email address and the email itself as part of that email.
- We provide advertisers only aggregated non-personal information such as the number of times one of their ads was clicked. We do not sell, rent or otherwise

share your personal information with any third parties except in the limited circumstances described in the Google Privacy Policy, such as when we believe we are required to do so by law.

Your choices

- You may change your Gmail account settings through the Gmail "settings" section.
- You may organize or delete your messages through your Gmail account or terminate your account through the Google Account section of Gmail settings. Such deletions or terminations will take immediate effect in your account view. Residual copies of deleted messages and accounts may take up to 60 days to be deleted from our active servers and may remain in our offline backup systems.
- You may choose to use additional Gmail features, such as chat, which connects to the Google Talk network, or Google Buzz. The Google Talk service has its own privacy notice available here, and Google Buzz here.

More information

Google adheres to the US Safe Harbor privacy principles. For more information about the Safe Harbor framework or our registration, see the Department of Commerce's web site.

Further information about Gmail is available here.

For more information about our privacy practices, go to the full privacy policy. For questions concerning the product or your account, please check out the Google Help page.

©2010 Google - Terms

EDOLPHUS TOWNS, NEW YORK
CHAIRMAN

PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
MIKE QUIGLEY, ILLINOIS
MARCY KAPTUR, OHIO
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
PATRICK J. KENNEDY, RHODE ISLAND
DANNY K. DAVIS, ILLINOIS
CHRIS VAN HOLLEN, MARYLAND
HENRY CUELLAR, TEXAS
PAUL W. HODES, NEW HAMPSHIRE
CHRISTOPHER S. MURPHY, CONNECTICUT
PETER WELCH, VERMONT
BILL FOSTER, ILLINOIS
JACKIE SPEIER, CALIFORNIA
STEVE DRIEHAUS, OHIO
JUDY CHU, CALIFORNIA

ONE HUNDRED ELEVENTH 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) 225-5051
FACSIMILE (202) 225-4784
MINORITY (202) 225-5074

www.oversight.house.gov

DARRELL E. ISSA, CALIFORNIA
RANKING MINORITY MEMBER

DAN BURTON, INDIANA
JOHN L. MICA, FLORIDA
JOHN J. DUNCAN, JR., TENNESSEE
MICHAEL R. TURNER, OHIO
LYNN A. WESTMORELAND, GEORGIA
PATRICK T. MCHENRY, NORTH CAROLINA
BRIAN P. BILBRAY, CALIFORNIA
JIM JORDAN, OHIO
JEFF FLAKE, ARIZONA
JEFF FORTENBERRY, NEBRASKA
JASON CHAFFETZ, UTAH
AARON SCHOCK, ILLINOIS
BLAINE LUETKEMEYER, MISSOURI
ANH "JOSEPH" CAO, LOUISIANA
BILL SHUSTER, PENNSYLVANIA

July 9, 2010

Mr. Michael Bradshaw
Director, Google Federal
Google, Inc.
1818 Library Street
Suite 400
Reston, VA 20190

Dear Mr. Bradshaw:

Thank you for your testimony at the July 1, 2010, Committee on Oversight and Government Reform hearing entitled, "Cloud Computing: Benefits and Risks of Moving Federal IT into the Cloud."

As you may know, any email sent or received by White House officials may be subject to retention under the Presidential Records Act (PRA).[1] However, the use of personal email accounts, such as Gmail, to conduct official business raises the prospect that presidential records will not be captured by the White House email archiving system. In addition, the growth of social media – such as Facebook, Twitter, and G-chat – and mobile technologies – including laptops, handheld mobile devices, and iPads – pose new challenges for capturing communications under the PRA.

Problems with the White House email archiving system plagued both the Clinton and Bush Administrations,[2] and difficulties with PRA-compliance have already emerged in this Administration. In April it was revealed that Office of Science and Technology Policy (OSTP) Deputy Chief Technology Officer, Andrew McLaughlin, used his personal email account to engage in official business, including discussions on policy matters under his review with his former employer, Google, Inc. On June 24, 2010, the *New York Times* reported that "lobbyists say that they routinely get e-mail messages from

---

[1] 44 U.S.C. § 2201 *et seq.*

[2] General Accounting Office (GAO), Clinton Administration's Management of Executive Office of the President's Email System, GAO-01-446, April 2001 (GAO was renamed Government Accountability Office in 2004); R. Jeffrey Smith, *Missing White House Emails Trace, Justice Aide Says*, WASH. POST, Jan. 15, 2009, at A9 (hereinafter Smith, Jan. 15, 2009).

Mr. Michael Bradshaw
July 9, 2010
Page 2

White House staff members' personal accounts rather than from their official White House accounts."[3]

Accordingly, as I requested at the hearing, please respond to the following questions for the record.

1. Identify and describe Google, Inc.'s policy for retaining electronic records, such as emails transmitted through the public Gmail system.

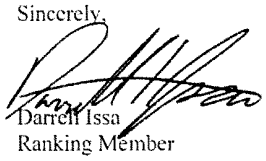
2. How long are emails retained or retrievable after a user deletes an email from their public Gmail account?

3. Identify and describe Google, Inc.'s procedures for complying with subpoenas from law enforcement agencies.

4. Has the White House or any federal agency contacted Google about retention of emails sent by personnel covered by the PRA or Federal Records Act?

Please provide your written responses no later than July 20, 2010. If you have any questions regarding this request, please contact John Ohly or Steve Castor of the Committee Staff at 202-225-5074. Thank you for your attention to this matter.

Sincerely,



Darrell Issa
Ranking Member

cc: The Honorable Edolphus Towns, Chairman

---

[3] Eric Lichtblau, N.Y. TIMES, *Across From the White House, Coffee with Lobbyists*, (June 24, 2010) *available at* http://www.nytimes.com/2010/06/25/us/politics/25caribou.html (hereinafter Lichtblau, June 24, 2010.)

○