THE NEXT IT REVOLUTION?: CLOUD COMPUTING OPPORTUNITIES AND CHALLENGES

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

WEDNESDAY, SEPTEMBER 21, 2011

Serial No. 112–36

Printed for the use of the Committee on Science, Space, and Technology

Available via the World Wide Web: http://science.house.gov

U.S. GOVERNMENT PRINTING OFFICE
68–317PDF WASHINGTON : 2011

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 SCIENCE, SPACE, AND TECHNOLOGY

HON. RALPH M. HALL, Texas, *Chair*

F. JAMES SENSENBRENNER, JR., Wisconsin
LAMAR S. SMITH, Texas
DANA ROHRABACHER, California
ROSCOE G. BARTLETT, Maryland
FRANK D. LUCAS, Oklahoma
JUDY BIGGERT, Illinois
W. TODD AKIN, Missouri
RANDY NEUGEBAUER, Texas
MICHAEL T. MCCAUL, Texas
PAUL C. BROUN, Georgia
SANDY ADAMS, Florida
BENJAMIN QUAYLE, Arizona
CHARLES J. “CHUCK” FLEISCHMANN, Tennessee
E. SCOTT RIGELL, Virginia
STEVEN M. PALAZZO, Mississippi
MO BROOKS, Alabama
ANDY HARRIS, Maryland
RANDY HULTGREN, Illinois
CHIP CRAVAACK, Minnesota
LARRY BUCSHON, Indiana
DAN BENISHEK, Michigan
VACANCY

EDDIE BERNICE JOHNSON, Texas
JERRY F. COSTELLO, Illinois
LYNN C. WOOLSEY, California
ZOE LOFGREN, California
BRAD MILLER, North Carolina
DANIEL LIPINSKI, Illinois
GABRIELLE GIFFORDS, Arizona
DONNA F. EDWARDS, Maryland
MARCIA L. FUDGE, Ohio
BEN R. LUJÁN, New Mexico
PAUL D. TONKO, New York
JERRY MCNERNEY, California
JOHN P. SARBANES, Maryland
TERRI A. SEWELL, Alabama
FREDERICA S. WILSON, Florida
HANSEN CLARKE, Michigan
VACANCY

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION

HON. BENJAMIN QUAYLE, Arizona, *Chair*

LAMAR S. SMITH, Texas
JUDY BIGGERT, Illinois
RANDY NEUGEBAUER, Texas
MICHAEL T. MCCAUL, Texas
CHARLES J. “CHUCK” FLEISCHMANN, Tennessee
E. SCOTT RIGELL, Virginia
RANDY HULTGREN, Illinois
CHIP CRAVAACK, Minnesota
RALPH M. HALL, Texas

VACANCY
JOHN P. SARBANES, Maryland
FREDERICA S. WILSON, Florida
DANIEL LIPINSKI, Illinois
GABRIELLE GIFFORDS, Arizona
BEN R. LUJÁN, New Mexico

EDDIE BERNICE JOHNSON, Texas

CONTENTS

Hearing Date

Opening Statements

Witnesses:

Appendix I: Answers to Post-Hearing Questions

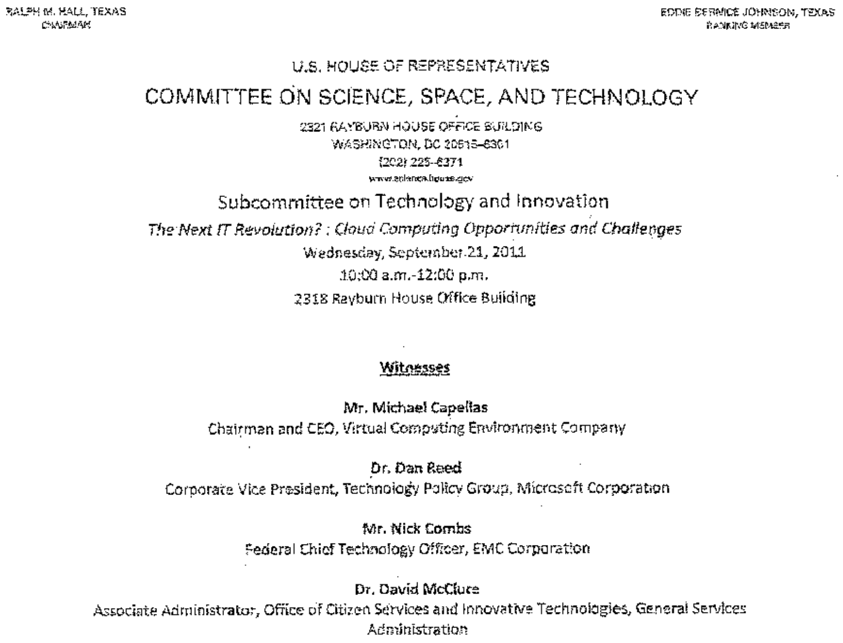
Appendix II: Additional Materials Submitted for the Record

THE NEXT IT REVOLUTION? CLOUD COMPUTING OPPORTUNITIES AND CHALLENGES

WEDNESDAY, SEPTEMBER 21, 2011

House of Representatives,
Subcommittee on Technology and Innovation,
Committee on Science, Space, and Technology,
Washington, DC.

The Subcommittee met, pursuant to call, at 10:02 a.m., in Room 2318 of the Rayburn House Office Building, Hon. Ben Quayle [Chairman of the Subcommittee] presiding.



RALPH M. HALL, TEXAS
CHAIRMAN

EDDIE BERNICE JOHNSON, TEXAS
RANKING MEMBER

U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

Subcommittee on Technology and Innovation

The Next IT Revolution? : Cloud Computing Opportunities and Challenges

Wednesday, September 21, 2011
10:00 a.m.-12:00 p.m.
2318 Rayburn House Office Building

Witnesses

Mr. Michael Capellas
Chairman and CEO, Virtual Computing Environment Company

Dr. Dan Reed
Corporate Vice President, Technology Policy Group, Microsoft Corporation

Mr. Nick Combs
Federal Chief Technology Officer, EMC Corporation

Dr. David McClure
Associate Administrator, Office of Citizen Services and Innovative Technologies, General Services Administration

HEARING CHARTER

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES
SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION

The Next IT Revolution: Cloud Computing Opportunities and Challenges

WEDNESDAY, SEPTEMBER 21, 2011
10:00 A.M. – 12:00 P.M.
2318 RAYBURN HOUSE OFFICE BUILDING

I. Purpose

On Wednesday, September 21, 2011, the Subcommittee on Technology and Innovation will convene a hearing to examine the potential opportunities and challenges associated with cloud computing, and to assess the appropriate role of the Federal Government in the cloud computing enterprise. The hearing will focus on: innovation and efficiency opportunities associated with cloud computing; challenges restraining the widespread adoption of cloud computing; and federal cloud computing adoption initiatives.

II. Witnesses

- **Mr. Michael Capellas**, Chairman and CEO, Virtual Computing Environment Company; Co-Chairman, Commission on the Leadership Opportunity in U.S. Development of the Cloud "CLOUD^2," a commission launched by TechAmerica Foundation to provide federal policy recommendations for cloud computing.
- **Dr. Dan Reed, Corporate Vice President**, Technology Policy Group, Microsoft Corporation; Vice Chairman, "CLOUD^2"
- **Mr. Nick Combs**, Federal Chief Technology Officer, EMC Corporation
- **Dr. David McClure**, Associate Administrator, Office of Citizen Services and Innovative Technologies, General Services Administration

III. Brief Overview

Cloud computing has significant implications for the way businesses, scientists, and governments access and use information technology (IT). It enables users to remotely access scalable, high-powered computing services via broadband networks from a range of devices, all on-demand. Cloud computing has the potential to provide users with increased computing capability, greater efficiency, and lower energy and infrastructure costs.

Cloud computing is not new. While many people may not be familiar with the term, "cloud computing," anyone who uses a web-based email account, such as Gmail or Hotmail, or that uses file-sharing social networking sites, such as Facebook, is already a user of cloud computing services. The data and applications on these sites are hosted on remote servers owned and operated by the service provider, rather than on an individual's hard drive.

Cloud computing promises to provide new ways of managing information for the public and private sector. Some of cloud computing's opportunities include cost savings on IT infrastructure and maintenance, increased access to high-powered computing applications for both business and academic researchers, and greater data and file accessibility for consumers.

However, there are also many challenges associated with cloud computing. Cloud consumers need assurances that their data will be secure in the cloud. Without confidence that security and privacy concerns are addressed, users may be hesitant to adopt cloud services. Users also want assurances that they will have ubiquitous access to cloud services. Therefore, network resiliency and broadband accessibility are crucial factors in determining cloud adoption. Users want the ability to move their data and applications from one service provider to another, so portability and interoperable standards within the cloud are key issues. Additional concerns of cloud users and service providers include liability and regulations governing cloud usage.

Witnesses have been asked to provide their insights on the opportunities that cloud computing offers to users and service providers, the primary challenges facing cloud computing users and service providers including security concerns, federal government initiatives to adopt cloud computing services, and the appropriate role of the federal government in the cloud computing enterprise, including in the development of standards.

IV. NIST Definition of Cloud Computing

The National Institute of Standards and Technology (NIST) has worked with various cloud stakeholders to develop a definition for cloud computing: "a model for enabling ubiquitous, 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]

To encompass all aspects of cloud computing, NIST identifies five essential characteristics, three service models, and four deployment models of cloud computing.

Essential characteristics:[2]

- *On-demand self-service.* Users can access cloud computing services at any time.
- *Broad network access.* Services are available over the Internet using any web-connected device.
- *Resource pooling.* Providers can serve multiple users simultaneously.
- *Rapid elasticity.* Cloud computing services can be scaled to meet user need.
- *Measured service.* Cloud users only pay for the services they consume, and can adjust this usage based on need.

Service models:[3]

- *Software as a Service (SaaS).* Enables a user to access provider applications from any device through a web browser. Users do not manage or control any underlying infrastructure such as servers, operating systems, storage, or application settings. The infrastructure is managed by the cloud provider.
- *Platform as a Service (PaaS).* Enables a user to deploy user-created or acquired applications on the cloud using programming tools supported by the provider. The user does not manage the infrastructure (servers, storage, etc) but has control over the deployed applications.
- *Infrastructure as a Service (IaaS).* Enables a user to rent and manage cloud infrastructure from a provider, and to deploy its own applications and software, including operating systems.

Deployment models:[4]

- *Private cloud.* The cloud infrastructure is operated solely for an organization, and may be managed by the organization or by a third-party, and may exist on-site or off-site.
- *Community cloud.* The cloud infrastructure is shared by several organizations and supports a specific community with shared concerns. The infrastructure may be managed by the organizations or by a third-party, and may exist on-site or off-site.
- *Public cloud.* The cloud infrastructure is available to the public at large and is owned and managed by the service provider.
- *Hybrid cloud.* The cloud infrastructure is made up of two or more clouds (private, community, public) which remain separate, but share certain technology to enable data portability between clouds.

V. Cloud Computing Opportunities

Cloud computing promises benefits to businesses, individuals, researchers, and governments.

[1] National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800–145: NIST Definition of Cloud Computing (DRAFT) 2 (2011).

[2] Ibid; Computer and Communications Industry Association,Public Policy for the Cloud: How Policymakers Can Enable Cloud Computing (2011), available online at http://www.ccianet.org

[3] Ibid

[4] Ibid

Opportunities for Business

Businesses can reduce their IT overhead by migrating computing functions to the cloud. This may lower cost barriers for startup companies by not requiring expensive IT hardware and infrastructure purchases in the early stages of growth. Cloud elasticity also enables businesses to pay for only the services and computing power that they actually use. This can prevent the problem of purchasing excess infrastructure capacity that may go unused, or having too little infrastructure to accomplish key work requirements. Cloud computing can also enable more businesses in data-intensive fields to access high powered computing resources, helping to level the playing field between smaller and larger companies.

Opportunities for Individuals

Cloud computing can provide consumers with unlimited access to data files from remote locations using a range of Internet-connected devices. Changes that users make to files and data stored on the cloud from one device or location will be updated when the user accesses their files and data from a different device or location.

Opportunities for Researchers

Cloud computing can enable greater collaboration between scientists and researchers both domestically and internationally. It can also provide scientists with more computing power allowing them to run high-powered simulations that were previously restricted only to those with supercomputing access. Cloud computing may also reduce the amount of time that researchers and scientists need to set up IT infrastructure and increase the time spent on performing research.

Opportunities for the Federal Government

Cloud computing has the potential to reduce federal government IT expenditures by a considerable margin. A major portion of federal IT budgets is spent on infrastructure and maintenance. Migrating computing functions to the cloud may greatly reduce these costs helping to reduce taxpayer funding for these activities.

VI. Cloud Computing Challenges

There are a range of challenges that have prevented more widespread adoption of cloud computing. Some of these challenges include concerns about security and privacy, access and network resiliency, data portability and standards, and liability protection. Each of these issues has potential policy implications for the Federal Government.

Security and Privacy

Users of cloud services must have the confidence that their data and applications are secure. Different businesses and government agencies will require more robust security thresholds to protect more sensitive data. Cloud computing service providers must be able to offer these tiered service levels. While cloud computing can make it easier for providers to continuously update security applications, it may also offer a bigger "target" for malicious actors, requiring stronger security standards and redundancy.

Network Access, Availability and Resiliency

Users of cloud computing services will require access to services at any time from any device with an Internet connection. However, there are concerns that current broadband networks may not be able to provide constant on-demand access if cloud adoption grows. Network outages preventing users from accessing applications or data on the cloud could have severe effects on business and government operations. Consequently, lack of confidence in network reliability may inhibit cloud computing adoption. Lack of adequate broadband access in areas where businesses are located or in areas where users want to access services remotely will likewise limit further widespread cloud computing adoption.

Data Portability and Standards

Users of cloud computing services require the assurance that they can move their data and applications to different cloud service providers if they feel a change would be beneficial to them, so computing standards to enable portability and interoperability are critical to the agility of the cloud. While standards can provide for greater mobility, they can also inhibit innovation if they are too prescriptive or have been adopted before markets determine certain technology preferences.

Liability and Regulations

Lack of certainty associated with the laws and regulations governing migration of services to cloud computing has prevented more widespread adoption. Different industries face different regulatory frameworks which exacerbate problems of uncertainty. Liability concerns associated with data protection may prevent companies from migrating data away from their direct control. Finally, because liability and data storage regulations differ among countries, companies may be hesitant to expose themselves to potential lawsuits by migrating services to the cloud.

VII. Federal Initiatives on Cloud Computing

The Office of Management and Budget (OMB) has estimated that the Federal Government could move 25 percent of its IT spending to the cloud. In early 2011 the White House's Chief Information Officer released a Federal Cloud Computing Strategy[5], known as "Cloud First", which requires agencies to evaluate whether using cloud computing is an option before making new IT purchases.

In early 2010, the White House released the *OMB 25 Point Implementation Plan to Reform Federal Information Technology Management*[6]. This document described government-wide policies to maximize the efficiency and management of Federal IT resources.

As part of the *OMB 25 Point Implementation Plan*, the Obama Administration launched a Federal Data Center Consolidation Initiative (FDCCI)[7] to consolidate the Federal Government's data center environment by eliminating a minimum of 800 of the more than 2000 physical data centers by 2015. Data center growth and affiliated costs are considered unsustainable and cloud computing offers a means of reducing the number of centers. Currently, as part of this initiative, more than 350 physical data centers have been identified by agencies for planned closings before the end of 2012[8].

As part of its responsibilities under the Federal Information Security Management Act (FISMA), the National Institute of Standards and Technology (NIST) must provide Federal Information Processing Standards (FIPS) and guidelines for agencies to use. As an agency considers migrations to cloud computing, NIST must develop the appropriate consensus standards and guidelines to ensure a secure and trustworthy environment for federal information.

The General Services Administration (GSA) performs a coordinating role in the Administration's IT Management Reform Agenda. GSA facilitates access to cloud-based solutions from private sector providers that meet federal requirements for federal entities, works with NIST and other federal agencies to assess and authorize cloud computing services through the Federal Risk and Authorization Management Program (FedRAMP), and identifies potential multi-agency or government-wide uses of cloud computing solutions.[9] GSA also manages apps.gov as an e-commerce website for federal entities to purchase cloud computing products and services.

Internally, GSA has implemented an agency-wide cloud-based email solution, has moved certain GSA-managed web sites (including usa.gov and data.gov) to cloud hosted environments, and expects to reduce its government owned data centers from 15 to three by Fiscal Year 2015, among other cloud computing initiatives.[10] Other federal agencies are making efforts towards implementing the Administration's Federal Cloud Computing Strategy with varying degrees of progress. National security agencies, including the Department of Defense and the Department of State, may be more hesitant about migrating sensitive information and data to a cloud environment.

The NIST Cloud Computing Program aims to shorten the adoption cycle for cloud, which will enable near-term cost savings and increased ability to quickly create and deploy enterprise applications. NIST aims to foster cloud computing systems and

[5] http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf

[6] http://www.cio.gov/documents/25–Point-Implementation-Plan-to-Reform-Federal%20IT.pdf

[7] http://www.cio.gov/documents/Federal-Data-Center-Consolidation-Initiative-02–26–2010.pdf

[8] http://explore.data.gov/Federal-Government-Finances-and-Employment/Federal-Data-Center-Consolidation-Initiative-FDCCI/d5wm-4c37?

[9] Testimony of Dr. David McClure, General Service Administration, before the Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, April 12, 2011.

[10] Ibid.

practices that support interoperability, portability, and security requirements that are appropriate and achievable for important usage scenarios.[11] NIST has published a Cloud Computing Standards Roadmap[12], Cloud Computing Reference Architecture[13], a Draft Cloud Computing Synopsis and Recommendations[14], and has held three forums and workshops bringing together government, industry and private stakeholders in support of these efforts.

Chairman QUAYLE. Good morning. Welcome to today's hearing entitled "The Next IT Revolution?: Cloud Computing Opportunities and Challenges." In front of you are packets containing the written testimony, biographies, and truth-in-statement disclosures for today's witnesses. I will now recognize myself for five minutes for an opening statement.

Good morning. I would like to welcome everyone to today's hearing, which is being held to examine the opportunities and challenges presented by cloud computing and to analyze the appropriate role of federal policy in the growing cloud computing enterprise. Over the last few decades, developments in the IT sector have driven our country's economic growth. Cloud computing has the potential to be the next wave. Its widespread adoption offers significant opportunities for new innovation and productivity gains for both the public and private sectors.

Users of cloud computing services will be able to access high-powered computing functions from a range of devices that previously were only available to entities with large IT infrastructure budgets. Cloud services will also allow individuals to share information with colleagues in real time, dramatically increasing opportunities for collaboration.

The adoption of cloud computing has the potential to significantly reduce IT infrastructure and maintenance costs. Because these services are elastic, individuals will only pay for the computing services they consume and will no longer have to worry about over-investing or under-investing in IT. Companies can potentially use these savings to help grow and expand their businesses, while governments will be able to reduce their massive taxpayer-funded IT budgets.

Finally, cloud computing provides its users with unlimited access to data and applications from any Internet-connected device.

While the benefits of cloud computing are vast, there are a wide range of challenges that will need to be addressed before its potential is fully realized.

Cybersecurity is a major concern for many users who are considering moving their computing functions to the cloud. Users must have confidence that their data and applications will be secure and that their privacy will be protected. Further, cloud service providers will need to offer users different tiers of security depending on the sensitivity of their data.

Widespread adoption of cloud computing requires broad network access and resiliency. With increased reliance on the cloud for computing functions, broadband networks must be up to the task of handling the massive amounts of data that will be transmitted over

[11] http://www.nist.gov/itl/cloud/index.cfm
[12] NIST Special Publication 500–291
[13] NIST Special Publication 500–292
[14] NIST Special Publication 800–146

the Internet. Users will also want assurances that they will be able to transport their data and applications from one service provider to another. Therefore, the development of interoperable standards is a key issue. But, as we have often discussed in this Subcommittee, it is important that these are consensus-based standards that will not be so rigid that they inhibit the opportunities for innovation that cloud computing offers. Finally, liability will need to be addressed to reflect the new cloud-computing paradigm.

While these are only a few of the relevant issues, it provides a sense of the challenges confronting industry, consumers, and policymakers in determining the appropriate path forward for this technology.

We have an excellent panel of IT industry witnesses who will share their insights on these topics with us. We have also asked each of our industry witnesses to comment on the appropriate role of the Federal Government in cloud computing. Further, we will hear about the General Services Administration's efforts to adopt cloud computing services and enable other federal agencies to do the same.

I would like to extend my appreciation to each of our witnesses for taking the time and effort to appear before us today. We look forward to your testimony.

And I now recognize the gentleman from New Mexico, Mr. Luján, for his opening statement.

[The prepared statement of Mr. Quayle follows:]

Prepared Statement of Chairman Ben Quayle

Good Morning. I'd like to welcome everyone to today's hearing, which is being held to examine the opportunities and challenges presented by cloud computing, and to analyze the appropriate role of federal policy in the growing cloud computing enterprise.

Over the last few decades, developments in the IT sector have driven our country's economic growth. Cloud computing has the potential to be the next wave. Its widespread adoption offers significant opportunities for new innovation, and productivity gains for both the public and private sectors.

Users of cloud computing services will be able to access high-powered computing functions from a range of devices that previously were only available to entities with large IT infrastructure budgets. Cloud services will also allow individuals to share information with colleagues in real time, dramatically increasing opportunities for collaboration.

The adoption of cloud computing has the potential to significantly reduce IT infrastructure and maintenance costs. Because these services are elastic, individuals will only pay for the computing services they consume, and will no longer have to worry about over-investing or under-investing in IT. Companies can potentially use these savings to help grow and expand their business, while governments will be able to reduce their massive taxpayer-funded IT budgets.

Finally, cloud computing provides its users with unlimited access to data and applications from any Internet-connected device.

While the benefits of cloud computing are vast, there are a range of challenges that will need to be addressed before its potential is fully realized.

Cybersecurity is a major concern for many users who are considering moving their computing functions to the cloud. Users must have confidence that their data and applications will be secure and that their privacy will be protected. Further, cloud service providers will need to offer users different tiers of security depending on sensitivity of their data.

Widespread adoption of cloud computing requires broad network access and resiliency. With increased reliance on the cloud for computing functions, broadband networks must be up to the task of handling the massive amounts of data that will be transmitted over the Internet.

Users will also want assurances that they will be able to transport their data and applications from one service provider to another. Therefore, the development interoperable standards is a key issue. But, as we have often discussed in this Subcommittee, it is important that these are consensus-based standards that will not be so rigid that they inhibit the opportunities for innovation that cloud computing offers.

Finally, liability will need to be addressed to reflect the new cloud-computing paradigm.

While these are only a few of the relevant issues, it provides a sense of the challenges confronting industry, consumers, and policymakers in determining the appropriate path forward for this technology.

We have an excellent panel of IT industry witnesses who will share their insights on these topics with us. We have also asked each of our industry witnesses to comment on the appropriate role of the federal government in cloud computing. Further, we will hear about the General Services Administration's efforts to adopt cloud computing services and enable other federal agencies to do the same.

I'd like to extend my appreciation to each of our witnesses for taking the time and effort to appear before us today. We look forward to your testimony.

Mr. LUJÁN. Thank you, Chairman Quayle. And good morning to our witnesses as well. I want to thank you all for being with us for this important hearing to examine both the benefits and risks of cloud computing.

As you all know, and as I expect you will hear from our witnesses today, cloud computing has many potential benefits. By sharing IT capabilities in the cloud, individuals, businesses, and government agencies are able to leverage their resources more effectively. They need only pay for what they use and can easily scale up or ramp down the computing power or amount of data storage they need.

In addition to lowering capital investment, cloud computing allows people to access their files and applications from anywhere at any time using everything from their home computer to their tablet or smartphone, as long as they have broadband connectivity. In addition to being convenient, the mobility that cloud computing offers has the potential to increase the productivity of individuals. The cloud also has the potential to drive innovation, not only by changing the way businesses operate, but also how research is conducted. I look forward to hearing more about how cloud computing can advance basic research from Dr. Reed later this morning.

However, despite all of the promise cloud computing offers, there are a number of security concerns associated with moving information to a remote data server that is operated by a third party and may be located in a foreign country with less stringent data protection laws. In fact, according to a recent report, 71 percent of federal Chief Information Officers stated that security concerns were preventing them from adopting cloud solutions. However, the same report found that the Federal Government could save over $14 billion within the first year if we were to embrace cloud computing. It is essential that we find a way to ensure the security and privacy of the cloud so that the Federal Government can reap the full benefits of this emerging technology.

I am pleased that the Administration is focusing its efforts on achieving this goal. As I understand it, this effort by GSA and NIST will provide federal agencies with tools to assess and select cloud computing services and products that satisfy federal security requirements. In addition, I am pleased that NIST has taken an active role in the development of cloud computing standards for the

Federal Government and is working closely with industry on the development of standards to support cloud computing infrastructure, metrics, interoperability, and assurance as mandated in the *America COMPETES Reauthorization Act.*

Standards are a critical component to our ability to realize the true potential of cloud computing, and I am pleased that NIST has hit the ground running with these efforts and is well on its way to delivering the required standards.

I look forward to hearing from our witnesses about the Administration's efforts and what we here in Congress can and should do to ensure progress continues and that the federal agencies have the tools and resources they need to adopt secure cloud computing solutions which will save money.

I would like to again thank the witnesses for being here today. I look forward to your testimony. Thank you, Chairman Quayle, and I yield back the balance of my time.

[The prepared statement of Mr. Luján follows:]

Prepared Statement of Representative Ben R. Luján

Thank you, Chairman Quayle, and good morning to our witnesses. I want to thank you all for being with us today for this important hearing to examine both the benefits and risks of cloud computing.

As you all know, and as I expect we will hear from our witnesses today, cloud computing has many potential benefits. By sharing IT capabilities in the cloud, individuals, businesses, and government agencies are able to leverage their resources more effectively. They only need to pay for what they use and can easily scale up or ramp down the computing power or amount of data storage they need.

In addition to lowering capital investment, cloud computing allows people to access their files and applications from anywhere at any time, using everything from their home computer to their iPad or smart phone. In addition to being convenient, the mobility that cloud computing offers has the potential to increase the productivity of individuals.

The cloud also has the potential to drive innovation not only by changing the way businesses operate, but also how research is conducted. I look forward to hearing more about how cloud computing can advance basic research from Dr. Reed later this morning.

However, despite all of the promise cloud computing offers, there are a number of security concerns associated with moving information to a remote data server that is operated by a third party and may be located in a foreign country with less stringent data protection laws.

In fact, according to a recent report, 71 percent of federal chief information officers stated that security concerns were preventing them from adopting cloud solutions.

However, that same report found that the federal government could save over $14 billion within the first year if it were to embrace cloud computing.

It's essential that we find a way to ensure the security and privacy of the cloud so that the federal government can reap the full benefits of this emerging technology. I am pleased that the Administration is focusing its efforts on achieving this goal. As I understand it, this effort by GSA and NIST will provide federal agencies with tools to assess and select cloud computing services and products that satisfy federal security requirements.

In addition, I am pleased that NIST has taken an active role in the development of cloud computing standards for the federal government and is working closely with industry on the development of standards to support cloud computing infrastructure, metrics, interoperability, and assurance, as mandated in the America COMPETES Reauthorization Act. Standards are a critical component of our ability to realize the true potential of cloud computing and I am pleased that NIST has hit the ground running with these efforts and is well on its way to delivering the required standards.

I look forward to hearing from our witnesses about the Administration's efforts and what we here in Congress can or should do to ensure that progress continues and that the federal agencies have the tools and resources they need to adopt secure cloud computing solutions.

I'd like to again thank the witnesses for being here today and I look forward to your testimony. Thank you, Chairman Quayle. I yield back the balance of my time.

Chairman QUAYLE. Thank you, Mr. Luján. I would like to request unanimous consent that the CLOUD^2 Commission's report be added to the record at this point. Without objection, so ordered.

[The information appears in Appendix II]

Chairman QUAYLE. If there are Members who wish to submit additional opening statements, your statements will be added to the record at this point.

At this time, I would like to introduce our witnesses and then we will proceed to hear from each of them in order.

Our first witness is Mr. Michael Capellas, Chairman and CEO of the Virtual Computing Environment Company. Mr. Capellas also serves as co-chair of the TechAmerica Foundation's Commission on the Leadership Opportunity in U.S. Deployment of the Cloud, or CLOUD^2.

Next, we will hear from Dr. Dan Reed, Corporate Vice President of the Technology Policy Group at Microsoft Corporation.

Our third witness is Mr. Nick Combs, Federal Chief Technology Officer for EMC Corporation.

Our final witness is Dr. David McClure, the Associate Administrator for the Office of Citizen Services and Innovative Technologies at the GSA.

Thanks again to our witnesses for being here this morning, and as our witnesses should know, spoken testimony is limited to five minutes each. After all witnesses have spoken, Members of the Committee will have five minutes each to ask questions.

I now recognize our first witness, Mr. Michael Capellas, for five minutes. Mr.—can you turn your mic on? Thank you.

STATEMENTS OF MR. MICHAEL CAPELLAS, CHAIRMAN AND CEO, VIRTUAL COMPUTING ENVIRONMENT COMPANY; CO-CHAIRMAN, COMMISSION ON THE LEADERSHIP OPPORTUNITY IN U.S. DEVELOPMENT OF THE CLOUD "CLOUD^2"

Mr. CAPELLAS. That would be helpful. Always takes a tech guy to learn how to turn the mic on.

So again, good morning, Chairman Quayle and Members of the Subcommittee. My name is Michael Capellas, and I am Co-Chair of TechAmerica Foundation's Commission on the Leadership Opportunity in U.S. Deployment of the Cloud, and I am honored to be invited to testify on a subject of critical national importance.

Cloud computing has far-ranging economic implications of utmost relevance to U.S. job creation, productivity, and technology leadership. As many on the Subcommittee have no doubt observed, cloud computing has taken on many meanings and there is widespread confusion in the market about what cloud means, how to get it, what it is good for and what possible drawbacks might exist. But the cloud business opportunity is significant, with analysts projecting cloud revenues to top $50 billion within three years.

Those that follow the technology industry know that cloud computing has been around for many years. It is only recently that revenue projections have sharply increased, so it is important to understand why many experts think cloud computing is poised to grow rapidly over the next decade and why all the cloud hype exists in the marketplace.

The application of IT in general has been the single-most important driver of U.S. productivity for over two decades. My objective is to convey the Commission's finding around why cloud is so important in terms of U.S. competitiveness, including job creation and productivity. But first I want to suggest that most of the predictions about cloud's strong market growth are wrong. I think they are wrong because they understate cloud growth and they understate the impact cloud is going to have in reshaping the IT landscape. Cloud is like nothing we have seen before in prior waves, and why it is important to the U.S. Government.

Information Technology has been synonymous with economic prosperity since the middle of the last century. IT has experienced numerous waves of changes since that time. Previous IT waves include the World Wide Web, the proliferation of handheld mobile and tablet Internet devices, virtualization technologies that together provide anytime, anywhere, any-manner connection to data, applications, and people. Cloud computing represents the culmination of those waves, and as such, it promises to spur the most significant transformation we have seen so far.

The Cloud will bring unprecedented opportunity to both users and those engaged in the business of IT infrastructure, solutions, and services. But what is at stake is significantly larger than the tens of billions of dollars of revenue that analysts are describing. I believe that cloud computing has the potential to reshape the landscape and shift wealth between nations. Trillions of dollars of economic wealth will be balanced upon competiveness in our 24-by-7 world. Cloud computing as a foundational element of IT can make companies, agencies, and organizations more nimble and competitive by boosting productivity and increasing the speed of business. Moving to the cloud faster will thus become a key consideration as organizations seek to become more competitive.

As requested, let me take a minute to address the essence of cloud computing. Cloud computing is defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resource—for example, networks, servers, storage, applications, and services—that can be rapidly provisioned and released with minimal management efforts or service provider interaction.

Central to cloud computing are the concepts of on-demand, self-service to an elastic pool of flexible resources, and measured service. In contrast to a traditional IT environment where different teams of specialists independently manage servers, networks, or storage, in cloud computing these components are preassembled into highly standardized and automated converged infrastructure, and the users do not have to know or care about where any of the components of technology are.

As an analogy, computers used to connect together over proprietary local networks, and it was difficult and expensive for different networks to talk to each other. Information was generally compartmentalized and generally only available to a few users. IP, or the Internet Protocol, was created as a network that could span great distances, and after a few years of solid but not remarkable growth, the entire market rapidly shifted and adopted IP because it evolved to solve both the problem of distance and the problem of communicating with other networks. IP thus became the de facto standard and users no longer needed to care or know about where the underlying network was.

As a participant in the IP technology wave, I will note that IP technology development was largely led by U.S. companies and has contributed to U.S. technological leadership, job growth, and productivity. Standardizing on IP simplified IT operations, reduced costs, and spurred advances.

Cloud computing also promises to add other forms. Most social networks today run on clouds with thousands of e-commerce sites, but the misconceptions with the cloud start back with agencies, and I believe that continued leadership of the United States will depend on cloud computing.

The Commission, comprised of 71 commissioners from leading U.S. companies and academia, delivered detailed recommendations to federal officials on how to best use the cloud and how the U.S. Government can capitalize on the advantages of cloud while spurring growth and enhancing productivity.

The Commission identified a set of barriers as well. I encourage you to look at the entire set, which is 14 recommendations, which have been detailed. Each of the recommendations shows how the Federal Government can look and can help ranging from policy to the different ways that we are going to deploy economic modeling. And with that, I thank you.

[The prepared statement of Mr. Capellas follows:]

Prepared Statement of Mr. Michael D. Capellas, Chairman and CEO, Virtual Computing Environment Company

Good morning, Chairman Quayle, and Members of the Subcommittee. My name is Michael Capellas and I am Co-Chair of the TechAmerica Foundation's Commission on the Leadership Opportunity in U.S. Deployment of the Cloud. I am honored to be invited to testify on a subject of critical national importance. Cloud computing has far ranging economic implications of utmost relevance to U.S. jobs creation, productivity and technology leadership.

As many on the Subcommittee have no doubt observed, cloud computing has taken on many meanings and there is widespread confusion in the market about what cloud means, how to get it, what it's good for and what potential drawbacks to cloud might exist. But the cloud business opportunity is significant, with analysts projecting cloud revenues to top $50B within three years.

Those that follow the technology industry know that cloud computing has been around for many years. It is only recently that revenue projections have sharply increased, so it is important to understand why many experts think cloud computing is poised to grow rapidly over the next decade and why all the cloud hype exists in the marketplace.

The application of IT has been the single most important driver of U.S. productivity over the past two decades. My objective today is to convey the Commission's findings around why the cloud is so important in terms of U.S. competitiveness, including jobs creation and productivity.

But first I want to suggest that most of these predictions about strong cloud market growth are wrong. I think they are wrong because they understate cloud growth and they understate the impact cloud will have in reshaping the IT landscape. Cloud will be like nothing we've seen before. Why is this important to the U.S. government? Information Technology has been synonymous with economic prosperity since the middle of the last century. IT has experienced numerous waves of changes since that time. Previous IT waves include the world wide web, the proliferation of handheld mobile and tablet Internet devices, and virtualization technologies that together can provide anytime, anywhere, any-manner connection to data, applications and people. Cloud computing represents the culmination of many waves, and as such it promises to spur the most significant transformation we've seen to date.

Cloud computing will bring unprecedented opportunity to both users and those engaged in the business of IT infrastructure, solutions and services. But what is at stake is significantly larger than the tens of billions of dollars that analysts are describing. I believe cloud computing has the potential to both reshape the IT landscape and shift wealth between nations. Trillions of dollars of global economic wealth will be based upon competiveness in our 24x7 world. Cloud computing as a foundational element to IT can make companies, agencies and organizations more nimble and competitive by boosting productivity and increasing the speed of business. Moving to cloud faster will thus become a key consideration as organizations seek to become more competitive.

As requested, let me take a moment to address the essence of cloud computing. Cloud computing is defined as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (for example, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Central to cloud computing are concepts of on-demand, self-service to an elastic pool of flexibly provisioned resources with measured service. In contrast to a traditional IT environment where different teams of specialists independently manage servers, networking and storage, in cloud computing these components are pre-assembled in a highly standardized and automated converged infrastructure, and the users do not have to know or care about how the components are put together. As an analogy, computers used to connect together over proprietary local networks, and it was difficult and expensive for different networks to talk to each other. Information was compartmentalized and generally only available to a few users. IP—the Internet Protocol—was created as a network that could span great distances, and after a few years of solid but not remarkable growth, the entire market rapidly shifted to IP because it had evolved to solve both the problem of distance and the problem of communicating with other networks. IP thus became the de facto standard and users no longer needed to know or care about the underlying network. As a participant in the IP technology wave, I'll note that IP technology development was largely led by U.S. companies and has contributed to U.S. technology leadership, job growth and productivity. Standardizing on IP simplified IT operations, reduced cost, and spurred advances like unified communications and high definition video over IP that we enjoy in our homes today.

Cloud computing also promises to simplify IT operations, reduce costs, and increase the speed and effectiveness with which organizations can do business and accomplish missions. Most Americans already use cloud computing in one form or another. Most social networking sites and thousands of e-commerce sites are "running in the cloud."

But misconceptions and concerns with cloud may impact success for companies and agencies, and I believe continued U.S. leadership in IT is dependent upon U.S. leadership in cloud computing. The CLOUD^2 commission, comprised of 71 commissioners from leading U.S. companies and academia, delivered detailed recommendations to federal officials on how to best allow the U.S. government to capitalize on the advantages of cloud, while spurring U.S. job growth and enhancing overall U.S. competitiveness in the world market. I was privileged to co-chair the Commission, working with industry leading experts from many U.S. companies, meeting with key customers and government agencies, and leading meetings between the Commission and numerous U.S. government officials. The Commission included some of the technology industry's brightest minds, who put our nation's best interests above individual company interests for the duration of our work effort, displaying focused and intense collaboration over a multi-month period resulting in a highly successful and influential outcome.

The Commission identified a set of common barriers spanning institutional inertial, restrictive policies, and technology concerns such as security and privacy that are currently inhibiting cloud awareness and adoption. Through comprehensive analysis and collaboration, a set of fourteen actionable recommendations along with a prescriptive Cloud Buyer's Guide was delivered to government IT officials and the commercial market as a whole. The Commission recognized the need to enable many paths to cloud computing, and determined that interim steps could be instrumental in accelerating many customers' journey to cloud.

The first step in accelerating the adoption of the cloud and driving U.S. leadership in cloud innovation is earning the trust of current and potential cloud users. Trust in the cloud is a result of a combination of factors that enable individuals and organizations consuming cloud services to be confident that the services are meeting their computing needs. These needs include security, privacy, performance and availability; the factors that contribute include transparency of practices, accountability, resiliency and redundancy, access and connectivity, supply chain provenance, life cycle integrity, and governance.

In response to industry concerns about cloud trust, the Commission created recommendations to develop and provide a standard approach to assessing and authorizing cloud computing services and products for use by Federal agencies. Specific recommendations are associated with robust identity management, federal data breach laws, the promotion of privacy frameworks, cloud service level transparency, transnational data flows, and re-examining mechanisms for lawful access by law enforcement or government to data stored in the cloud via reform of the Electronic Communications Privacy Act. The Commission encouraged the government to lead by example by increasing adoption of cloud computing and pursuing interim paths to cloud such as converged infrastructure deployments and virtualized data centers. Finally, the Commission made recommendations on policies mandating public disclosure of information about relevant operational aspects of public cloud services, including portability, interoperability, security, certifications, performance and reliability.

Members of Congress are encouraged to absorb the entire set of recommendations and act on them where possible. Excerpts from the Commission recommendations follow below, and the benefits of acting swiftly are clear. Cloud computing will enable companies (and governments) to move faster and be more responsive and flexible. Companies will be able to try several prototypes at once, test their limits, and then build and deploy new, better prototypes-all within a few weeks. This may be the most important benefit of the cloud-it enables companies of all sizes and in all sectors, as well as governments, non-profits, and individuals, to more quickly build new applications and services by reducing the cost and complexity of deploying and managing IT resources. Most companies and organizations spend the vast majority of their IT budget just maintaining their current infrastructures and the applications that run on them. The cloud will enable them to devote more resources and talent to creating new products and services and improving productivity. This democratization of innovation is a huge opportunity for people, organizations, and countries around the world. To maintain its competitive position, the United States must focus on quickly and effectively harnessing the full power of cloud computing, leading in both the deployment of cloud and the development of new cloud services. This will help American companies generate high-paying jobs and compete in the global marketplace.

Recommendation 1 (Trust in the Cloud): In recent months, senior U.S. officials have described threats such as cyber crime and state-sponsored industrial espionage as outpacing many enterprise defenses. In this evolving cyber threat environment, the commission believes that cloud security services and solutions, if done correctly, may provide improved security relative to non-cloud environments.

In order to implement applicable best practices and standards around security and information assurance, the Commission supports the efforts underway on programs such as the Federal Risk and Authorization Management Program (FedRAMP) and NIST Security Content Automation Protocol (SCAP). FedRAMP is a voluntary, General Services Administration (GSA) led initiative to develop and provide a standard approach to assessing and authorizing cloud computing services and products for use by Federal agencies. The Commission believes that a well-defined FedRAMP framework will help accelerate the adoption of cloud in the Federal government. The NIST SCAP is a standard that enables the automation of reporting and verifying IT security control parameters. SCAP provides a ready method to capture, test and continuously monitor the controls and integrity settings required to achieve the respective standard and/or compliance requirements. Security metrics efforts should build upon industry and academia initiatives already chartered to address standard cloud performance measurement frameworks. As the cloud is deployed by federal agencies and businesses in multiple sectors, cloud-related security issues will become an important element of the overall security discussion for those communities. The Commission therefore recommends that cloud expertise be integrated into existing information-sharing structures, such as the Information Sharing and Analysis Centers (ISACs) and the Sector Coordinating Councils.

Recommendation 2 (Identity Management): Industry and government should accelerate the development of a private sector-led identity management ecosystem as envisioned by the National Strategy for Trusted Identities in Cyberspace (NSTIC) to facilitate the adoption of strong authentication technologies and enable users to gain secure access to cloud services and websites. Mechanisms to provide identity, authentication, and attribution in cyberspace are essential to accelerating adoption of cloud computing services and improving trust in the cloud. (For example, identity management facilitates access verification, billing, law enforcement access, and other features and capabilities.) Two characteristics of a robust identity management ecosystem are (1) enabling higher level transactions to occur electronically and (2) enabling credentials to be utilized across multiple services and websites. In addition to supporting the development of a private sector-led identity management ecosystem, the commission also suggests specific steps that the federal government could take as a user of cloud services that would contribute to advancing robust identity management: Deploy, as appropriate, multi-factor authentication for federal cloud applications as used by federal personnel and government contractors doing government contract work. And accelerate the adoption of strong authentication, including multi-factor authentication and one time passwords, to enable mobile access to secure federal cloud services and websites.

Recommendation 3: The Commission recommends a national data breach law to streamline notifications and make it simple for customers to understand their rights with regard to notification. Such a law should include preemption of state laws to provide for harmonization. In addition, the law should take into account the various types of entities that are involved in processing the covered data cloud service providers, industry, government, nonprofit organizations, academic organizations, etc., and specifically provide that notice should be given by the entity that has a direct relationship with the parties whose information was subject to the breach. Finally, the law should have notification requirements based on risk of harm. Note that the motivation for such legislation is not limited to cloud computing, but adoption of cloud computing would benefit from this action. Specifically, by clarifying responsibilities and commitments around notification, the law will enable cloud providers to prepare to take expected steps in case of a breach and enable customers to trust the providers to do so. As a complement to the above recommendations, the U.S. government should update and strengthen criminal laws against those who attack our cyber infrastructure, including cloud computing services. In addition to clarifying cyber criminal offenses and defining penalties, the Federal government must commit adequate resources and personnel to investigating and tracking down cyber criminals. As much of cyber crime is transnational, the federal government should promote further international cooperation around cross-border prosecutions and identifying countries affording safe havens to such criminals.

Recommendation 4 (Research): Government, industry, and academia should develop and execute a joint cloud computing research agenda. The Commission recommends that government, industry, and academia take responsibility for developing and carrying out a research agenda that will promote U.S. leadership in the cloud by enabling innovation that benefits customers and service providers. Relevant cloud-oriented research areas include, but are not limited to, usability, privacy, availability, integrity, confidentiality, security, cryptography, identity management, energy efficiency, resource allocation, portability, and dependability. Government research agencies, like the National Science Foundation (NSF) and the Defense Advanced Research Projects Agency (DARPA), should fund universities and other organizations to conduct long range research activities, including those that build educational and research capacity and high risk, high-reward projects. Cooperative cloud test beds will also be a critical element in advancing the overall evolution of cloud technologies.

Recommendation 5 (Privacy): The U.S. government and industry should promote a comprehensive, technology-neutral privacy framework, consistent with commonly accepted privacy and data protection principles-based frameworks such as the OECD principles and/or APEC privacy frameworks. The Commission recommends that the U.S. build upon the work of existing, accepted privacy and data protection principles-based frameworks such as the Organization for economic Cooperation and Development (OECD) and/or Asia-Pacific Economic Cooperation (APEC) to develop and promote a comprehensive, technology-neutral privacy framework. The existing U.S. laws are sector specific and state specific, and this approach is different than those in other regions (e.g., Europe). In some quarters, there is a concern that this may impede the transnational flow of data with other countries, especially those in Europe. These actions would help provide the certainty and flexibility required for continued cloud innovation and would be a step toward fostering a global market for cloud services. Industry should embrace such frameworks and utilize them to the fullest extent practicable.

Recommendation 6 (Government/Law Enforcement Access to Data): The U.S. government should demonstrate leadership in identifying and implementing mechanisms for lawful access by law enforcement or government to data stored in the cloud. The Commission recommends that the U.S. modernize legislation governing law enforcement access to digital information in light of advances in IT in general and the cloud in particular. Reform of the Electronic Communications Privacy Act (ECPA) is critical to clarifying the legal conditions under which U.S. cloud providers and their customers will operate, as technology changes have overtaken many aspects of ECPA as originally written. Various groups such as the Digital Due Process Coalition have proposed making government access to data stored in the cloud consistent with government access to data stored in in-house IT systems. The U.S. Department of Commerce should conduct a study to assess the impact of the USA PATRIOT Act and similar national security laws in other countries on a company's ability to deploy cloud in a global marketplace. This action may provide insights into how best to address the uncertainty and confusion caused by national security statutes (e.g., PATRIOT Act) and similar laws of other nations) that are perceived as impediments to a global market place for cloud services.

Recommendation 7: Critical to improving trust in the cloud and accelerating adoption is the need for best practices in collecting forensic data and information in ways that do not result in significant, adverse impacts on individuals and/or organizations using the cloud-based information. To address this, the Commission recommends that the Federal CIO work with applicable agencies such as the U.S. Department of Justice and other relevant organizations to establish best practices specifically addressing acceptable methods for collecting forensic evidence from organizations using cloud-based information systems. In addition, cloud providers should assist their customers (e.g., individuals, commercial entities, government) with technologies to facilitate ediscovery and information retrieval requirements, whether in support of regulatory compliance or litigation activities.

Recommendation 8 (Lead by Example): The U.S. government should demonstrate its willingness to trust cloud computing environments in other countries for appropriate government workloads. This recommendation highlights the role of the U.S. government both as a customer of cloud services and as a leader in enabling trustworthy use of the cloud. Government agencies, in evaluating potential models for using the cloud, should not assume or default to the notion that no government workload and/or task is suitable for cloud computing environments in other countries. Instead, they should carefully consider the types of data and tasks within their information and communications technology portfolios to match suitable workloads to the cloud computing models that achieve the required level of confidentiality, integrity, and availability at the appropriate levels of efficiency, cost, and redundancy.

Recommendation 9 (Transparency): Industry should publicly disclose information about relevant operational aspects of their cloud services, including portability, interoperability, security, certifications, performance and reliability. Industry and government should support development of metrics designed to meet the needs of different user groups. These metrics should be developed in an open and transparent environment, taking into account the global nature of cloud use. The Commission recognizes the need for information and tools that provide users with meaningful ways to evaluate the characteristics and performance of various cloud implementations, whether they are contemplating deployment or evaluating performance of their current services. Development of metrics around key cloud attributes should be driven by user needs and provider capabilities. The government and commercial sector should collaborate on lessons learned, and each should be careful to avoid dominating the development of these metrics. Different government and business sectors will likely demand different measures and tools.

Recommendation 10 (Data Portability): Cloud providers should enable portability of user data through documents, tools, and support for agreed-upon industry standards and best practices. One benefit of the cloud is its ability to store and process large quantities of data. For customers making the transition to cloud, this often raises questions about how they access or move that data, especially in cases where they are switching between cloud providers. Data portability can be achieved in a variety of ways, and cloud providers should be transparent about their conformance with industry standards and best practices as well as the documents, tools, and relevant third-party solutions they make available to their customers. Customers should recognize that early consideration of data portability in selecting and implementing cloud services can reduce the risk of vendor lock-in. A collection of data portability standards, formats, and practices is vital to encouraging widespread cloud adoption. Government and industry should collaborate on facilitating the rapid development and dissemination of these standards and other relevant tools. The collaboration between NIST and the private sector in preparing the NIST standards roadmap under the Federal Cloud Computing Strategy is an excellent example of these types of efforts.

Recommendation 11 (Federal Acquisition and Budgeting): Agencies should demonstrate flexibility in adapting procurement models to acquire cloud services and solutions. Congress and OMB should demonstrate flexibility in changing budget models to help agencies acquire cloud services and solutions. In interviews with senior government officials, the Commission found that the current Federal Acquisition Regulation (FAR) does not need alteration for agencies to acquire cloud services. The FAR is already flexible enough to allow agencies to acquire IT as a service. However, agencies should demonstrate flexibility in adapting current procurement models and existing contracts to take advantage of new cloud offerings. One of the biggest challenges agencies may face in budgeting is predicting the costs of cloud computing over the course of a fiscal year. Cloud computing is designed to scale quickly to a customer's needs, providing maximum flexibility to the user. If the cloud service is based on a predictable subscription model (such as a standard monthly fee per user), these budget projections can be easily accommodated. If the cloud service is based on pay-as-you-go usage, however, it can be difficult to predict costs unless the user can precisely forecast future computing needs. To address this challenge, the Commission recommends that the current efforts to update and streamline the OMB 300 exhibit form and associated budget scoring include tools that facilitate and encourage the new business models associated with cloud. OMB and Congress should communicate to agencies that it recognizes budgeting for cloud is not like budgeting for traditional IT services and should assure agencies it will provide support and flexibility during and after the transition to the cloud. To help agencies acquire cloud services, the Commission also recommends Congress and OMB demonstrate flexibility in changing budget models. Government must find ways to provide more flexibility for agencies to reduce and transition funds in the capital expenditure accounts to the operations and maintenance expenditure accounts as part of implementing innovative cloud solutions and achieving savings. In making decisions about budgeting and acquisition, federal agencies, through the CIO Council, would benefit from sharing best practices, tools for objective analysis of cloud performance, and ways to predict and document different contributors to the budgetary impact of switching to the cloud.

Recommendation 12 (Incentives): Government should establish policies and processes for providing fiscal incentives, rewards and support for agencies as they take steps towards implementing cloud deployments. Adopting a new technology can be difficult, and the transition of agencies to the cloud will require investment of time, resources, and political will by the federal government. In recognition of this, the Commission recommends that OMB establish incentives and provide support for agencies beginning cloud adoption.

One possible incentive is to allow agencies to retain and redirect a portion of the overall budget savings realized from cloud adoption. Another approach is to provide seed money to agencies that help with the initial investments required in moving to the cloud.

Recommendation 13 (Improve Infrastructure): Government and industry should embrace the modernization of broadband infrastructure and the current move to IPv6 to improve the bandwidth and reliable connectivity necessary for the growth of cloud services. The Commission recommends that the federal government and industry continue to expand deployment of high bandwidth networking, enhance network resilience, and advance IPv6 adoption to ensure ample broadband connections. Efforts such as those advocated in the Federal Communications Commission's National Broadband Plan, including making additional spectrum available and expanding opportunities for opportunistic and unlicensed spectrum use, are necessary to allow cloud computing to function effectively and for businesses and citizens to realize the benefits of innovative new cloud technologies. With rapidly rising demands for connectivity, the last batch of IPv4 addresses, assigned earlier this year, is unlikely to meet demand beyond the end of 2011. Since cloud computing depends on the connection of many individuals, devices, and locations, a quick transition to IPv6 is vital to ensuring the successful adoption and operation of cloud computing in the future.

Recommendation 14 (Education/Training): Government, industry, and academia should develop and disseminate resources for major stakeholder communities to be educated on the technical, business, and policy issues around acquisition, deployment and operation of cloud services. The Commission commends GSA's outreach efforts to federal agencies to provide materials, expertise, and support around investigating, procuring, and deploying cloud solutions. GSA could build on this work by creating a cloud educational portal to help agency buyers, architects, administrators, and end users in understanding all aspects of cloud computing. Government, using existing programs in technology education and workforce training,4 can facilitate and encourage academic institutions and educational organizations to develop and offer courses relevant to cloud, in partnership with industry.

In a time when the government is seeking to do more with less and the commercial sector is being called upon to create jobs and grow the economy, now is the time to act on the cloud. Cloud computing has ushered in vast improvements in the cost, agility and efficiency of computing. These benefits alone drive a strong business case; however, the more compelling return is the opportunity to leap forward; to discover new markets and improve how we interact with, serve, and support U.S. citizens, users and other nations. The cloud holds the potential to unlock widespread entrepreneurism of all shapes and sizes, and expand the scope to do entirely new things—innovations such as social networking, which we could not fully imagine just a decade ago, would not exist without IT's continued evolution to the cloud.

It is the hope of the Commission that the federal government, industry and academia will implement these recommendations and be leaders in shaping how the future unfolds through the adoption of the cloud across the United States and around the world. Furthermore, these recommendations should demonstrate that cloud computing is not a new technology that needs further validation or analysis before it can be safely adopted; it is a natural evolution in computing. Those who recognize this and take early advantage of the benefits it offers will, in the coming decades, be the leaders not in only IT but in driving the cloud's evolution, and therefore, in driving business and mission results.

Chairman QUAYLE. Thank you, Mr. Capellas.

I now recognize Dr. Dan Reed to present his testimony.

STATEMENT OF DR. DAN REED CORPORATE VICE PRESIDENT, TECHNOLOGY POLICY GROUP, MICROSOFT CORPORATION; VICE CHAIRMAN, "CLOUD^2"

Dr. REED. Thank you, Mr. Chairman, Ranking Member Luján, and Members of the Committee. My name is Dan Reed and I am the Corporate Vice President of Microsoft's Technology Policy Group. And thank you for the opportunity to testify regarding the cloud today.

Today's smartphone was yesterday's supercomputer and yesterday's national archive is today's child's digital music collection. By combining the cloud with rich devices and sensors, the possibilities ahead are even more exciting—anticipatory personalized computing, remote healthcare monitoring and early response, smart grids and more energy efficient homes, intelligent transportation systems and reduced commuting times, and a new era of scientific discovery and innovation.

As a technologist for almost 30 years working in academia and industry, my testimony concerns how the cloud can help realize this future—accelerating scientific discovery for research, creating operational efficiencies, and enabling innovation by businesses and governments. I will touch on four areas in my remarks emphasizing how the Federal Government can facilitate these benefits.

I will begin with the cloud and science. Two major shifts are underway. First, researches are deluged by observational scientific data of unprecedented richness and scale. Second, and related, many of our most pressing technical and societal questions increasingly lie at the intersection of traditional disciplines. Both shifts challenge our historical approaches to investment and discovery via computing. The cloud and associated tools can let scientists be scientists rather than being distracted by IT, as they often are now.

I believe the Federal Government can accelerate this transition by encouraging the purchase of cloud services as a complement to and rather than just supporting the acquisition of local IT infrastructure, and equally importantly, by supporting new tools that facilitate distributed collaboration and simplify access to multidisciplinary scientific and engineering data. Microsoft is acting on this belief working in partnership with the National Science Foundation.

My second point concerns the cloud's impact on business and government. Cloud computing, as it was just noted, allows elastic scaling to meet varying demand both in capability and in management. Via the cloud, companies can be nimble and they can make forward bets quickly and without large capital or IT costs. This enables smaller companies to compete globally and it enables larger companies to explore new products and markets rapidly. Government, too, can benefit from cloud efficiencies to lower costs and deliver services in new ways. Clouds can also allow data from local, state, and federal agencies, as well as the private sector, to be combined and used in ways previously difficult if not impossible.

Thus, the Federal Government should move expeditiously to adopt cloud capabilities beginning with those services and data that directly match industry experiences and best practices, and it should revise policies and regulations accordingly to accelerate cloud deployment.

Third, let us consider the infrastructure needed for clouds. Cloud services depend on broadband communication. It is the oxygen via which they breathe. In turn, digital access to information and services is an enabler of economic competitiveness—of education, of government efficiency, and of service delivery. We must continue to design and deploy new backbone networks that support higher data rates, develop new protocols for the next generation of wireless networks, and define the standards that will shape the future of the globe-encircling cloud with access for all of us.

Fourth and finally, let me come back to research and education. As this Committee well appreciates and it has helped enable, today's cloud technology is derived from basic computing research conducted over the past four decades. To ensure that the United States remains at the forefront in cloud computing—and make no mistake, it is—ongoing investment and basic research remains crucial. There are deep and open abiding questions in the endless frontier of research in areas as diverse as privacy and security, chip design, energy efficiency, data management, networks and reliability, user interfaces, and accessibility. Equally importantly, this investment must be complemented by improvements in computing education at all levels.

In summary, the cloud is a foundation of the 21st Century digital economy. It can provide access to the world's knowledge base to individuals and empower entrepreneurs and companies large and small to sell their products globally, enable scientists and engineers to discover and innovate, and deliver government services quickly and efficiently.

Thank you.

[The prepared statement of Mr. Reed follows:]

PREPARED STATEMENT OF DR. DAN REED, CORPORATE VICE PRESIDENT, TECHNOLOGY POLICY GROUP, MICROSOFT CORPORATION; VICE CHAIRMAN, "CLOUD^2"

Chairman, Ranking Member, and Members of the Subcommittee, my name is Dan Reed, and I am the Corporate Vice President of Microsoft's Technology Policy Group. Thank you for the opportunity to share perspectives on the opportunities and challenges surrounding cloud computing. I appreciate the time and attention that the

Committee is spending on this topic, and I commend you for advancing the dialogue on information technology and cloud computing to drive innovation.

My testimony begins by describing the advent of the cloud and its importance, as a major technology inflection point with far-reaching effects and significant economic and competitive benefits for the U.S. It summarizes some of the key technologies behind clouds, notably massive data centers and infrastructure, wired and wireless networking, and the never-before-seen scale and access to information facilitated by these technologies. It then outlines the major opportunities clouds can enable to (1) accelerate scientific discovery for research; (2) create efficiencies and innovation for businesses and governments; and (3) enrich and empower the experiences of individual citizens. Finally, it concludes by providing a set of recommendations and next steps for the Federal government and others to allow the U.S. to benefit fully from the potential of clouds and to maintain its global leadership.

I. The Advent of the Cloud and its Importance

There has been extensive coverage of clouds in the popular media, and, as with all new technologies, considerable excitement about the benefits, as well as potential confusion. As a technologist and computing researcher for nearly 30 years, working in both academia and industry, I would like to separate the technical realities from the publicity.

Reviewing the history of modern digital computing reveals a prevailing theme—the fundamental questions do not change, but the technological answers change repeatedly, for the costs, capacities and speeds of the component technologies shift by many orders of magnitude. Today's smartphone was yesterday's supercomputer, and yesterday's national archive is now a child's digital music collection.

Since the late 1940s, we have experienced a series of computing revolutions, from the mainframe to the minicomputer, from the minicomputer to the workstation and then the PC and a variety of mobile and embedded devices. Each of these technological revolutions further democratized access to computing and extended its benefits. Today, I believe we are in the midst of another such revolution, enabled by inexpensive client devices and powerful cloud computing services.

Cloud services are not a sudden, new development. Each time we share digital photos, shop online, use an email service, download and use applications, or query a search engine, we are using the cloud. Every day, the combination of wired and wireless broadband networks, PCs and smartphones, and online services hosted in remote data centers connect individuals, deliver valuable data and insights, and drive business efficiency and innovation.

Although the cloud has already reshaped our lives, a converging set of technology trends in infrastructure, devices and communications will drive a new generation of experiences that will benefit society in ways we cannot yet imagine.

First, there is the increasingly expansive and efficient infrastructure that supports clouds. Today's cloud data centers are the largest computing capabilities ever built, a consolidation of computing at a truly massive scale—ten or more times the size of a football field for a single cloud data center. To put that fact in perspective, one cloud data center today contains more computers than the entire Internet did just a small number of years ago, and it contains as much digital data as would equal a substantial fraction of the text holdings of the Library of Congress.

Each of the major cloud operators, Microsoft and its competitors, is building a worldwide network of those data centers to support a new generation of cloud services. In doing so, they are changing the way the computing industry designs and builds systems, and they are drawing on the best practices and insights of operating infrastructure at large scale to make those clouds reliable 24/7, to make them secure, and to make them energy efficient.

The second trend is the explosive growth and availability of powerful consumer devices. While many think that the power of the cloud is predominantly about the massive computing and storage capabilities in data centers, the truly transformative effect comes from the intersection and interaction of the cloud with increasingly powerful devices.

With powerful sensors, wireless communications, and new natural user interfaces, coupled with the power of the cloud, new kinds of experiences emerge—for governments, for businesses and for consumers. Remote health care monitoring and early response, smart grids and more energy efficient homes, intelligent transportation systems and reduced commuting times, and a host of other possibilities are now realizable.

Finally, our continued investments in more powerful networking are coming to fruition. Cloud services rest on the foundational investment the U.S. has made in broadband networking, both wired and wireless, because communication networks are the oxygen that lets cloud services breathe. Reliable, high bandwidth, inexpensive and ubiquitous communications connect us in a true global village, albeit one on which demands and expectations continue to rise.

II. The Opportunities Presented by Clouds

Cloud services and data management bring several exciting opportunities for greater efficiency, innovation and discovery in domains as diverse as scientific research, business and U.S. competitiveness, and citizen empowerment.

Accelerating Scientific Discovery for Research. Throughout the history of science, data has been scarce and precious. Indeed, the modern scientific method is defined by a careful cycle of hypothesis and experiment, which gathers experimental data to test the hypothesis. Today, the same technological economics that have given us inexpensive computing, digital cameras and ubiquitous data-generating sensors, allow scientists to capture data at rates and volumes heretofore unimaginable.

In almost all domains, scientists and engineers are now drowning in a sea of data. In a few short years, they have gone from scarcity to an incredible richness, necessitating a significant change in how they manage and extract insight from all this data. In astronomy, the Sloan Digital Sky Survey in January 2011 released "the largest digital color image of the sky ever made. . . . This terapixel image is so big and detailed that one would need 500,000 high-definition TVs to view it at its full resolution."[1] In neuroscience, the researchers working on mapping the connections among the neurons in the brain are finding that the images necessary to make that map for a cube of mouse brain a millimeter on a side require roughly one petabyte of storage; this implies that similar maps of the human brain would require millions of petabytes.[2]

In a parallel shift, many of our scientific, engineering and societal questions increasingly lie at the intersections of traditional disciplines. Consider, for example, the recent oil spill in the Gulf of Mexico. Understanding the complexities of oil distribution in water is a problem related to computational fluid dynamics, but understanding the impact of that oil on the marine ecosystem is a biological problem. In both cases, observational data are essential. To fully understand the issue, researchers from multiple disciplines—from different cultures, using different research tools-must unite to build models and analyze data from diverse sources.

Increasing data volumes and the complexity of collaboration on interdisciplinary problems are challenging our historical approaches to discovery and innovation via computing. Researchers and research institutions are ill-prepared for the large-scale computing infrastructure management challenges posed by large data sets and complex models. The cloud and associated applications and tools offer a possible solution to this challenge by letting scientists be scientists.

Computing Infrastructure.

Today researchers, graduate students, and research support staff often spend inordinate amounts of time maintaining the computing systems needed to conduct research rather than devoting their time and talents to the research itself. The cost to maintain and refresh this computing infrastructure is becoming a larger and larger burden, and the economics are unsustainable, particularly at a time when our research universities are under financial stress. As a result, much of our research funding has focused (because of the power of computing for scientific discovery) on equipment replacement and repeated infrastructure deployments on research campuses and in laboratories. Yet at even the best funded research organizations, the majority of researchers do not have access to the computing resources they need.

Cloud computing can provide software applications, computing and data analytics, with remote access via familiar tools on PCs and smartphones. Because the cloud is professionally managed and regularly upgraded, delivering computational resources on demand, one can "pay as you go," using large-scale computational capacity and data analytics only when needed. The cost to use 10,000 processors for an hour is the same as using ten processors for 1,000 hours, but will deliver results much faster to the researcher. Organizations can buy just-in-time services to process and exploit data, rather spending scare resources on infrastructure.

Enabling Computing Tools and Applications for Research.

Much of our historical investment in high-performance computing (HPC) has brought the benefits of advanced computing to only a subset of the research community. Although powerful, and offering breakthrough capabilities for scientific and en-

[1] See Sloan Digital Sky Survey Press Release of January 11, 2011 at http://www.sdss3.org/press/20110111.largestimage.php.

[2] See New York Times article of Dec. 27, 2010 on the Human Connectome Project at http://www.nytimes.com/2010/12/28/science/28brain.html.

gineering discovery, these systems are often difficult to use, with steep learning curves and software tools that are unfamiliar to many. The key lesson of the consumer computing world is the importance of the "killer app" that opens computing to a new community by solving an important problem or creating a new capability. Thus, for scientists to realize fully the acceleration enabled by the power of the cloud, they also need a full complement of powerful, yet easy to use tools that are accessible via familiar PC and smartphone interfaces.

To accelerate access to cloud computing for research discovery, data analysis and multidisciplinary collaboration, Microsoft has formed a deep partnership with the National Science Foundation (NSF) to provide researchers with scalable cloud tools and services, accessible via client PCs. Thirteen research teams from across the country, whose proposals were selected via the NSF peer review process, have been awarded funding through the program and are being given access to Windows Azure[3] for a two-year period. In addition, a Microsoft support group, composed of software developers and researchers, is working directly with the teams to help them quickly integrate cloud technology and equip them with a set of common tools, applications and data collections that can be shared with the broad academic community.

The NSF awardees cover a diverse set of topics, but two examples, as described in the NSF announcement of the awards, illustrate the opportunities made possible via the NSF–Microsoft partnership[4]:

- *University of South Carolina (Jonathan Goodall) and the University of Virginia (Marty A. Humphrey)*– Managing Large Watershed Systems. Understanding hydrologic systems at the scale of large watersheds is critically important to society when faced with extreme events, such as floods and droughts, or with concern about water quality. Climate change and increasing population are further complicating watershed-scale prediction by placing additional stress and uncertainty on future hydrologic system conditions. This project advances hydrologic science and water resource management by creating and using a cloud-enabled hydrologic model and data processing workflows to examine the Savannah River Basin in the Southeastern United States. This will provide the detail and scale necessary to address fundamental research questions related to quantifying impacts of climate change on water resources.
- *Virginia Tech (Wuchun Feng)*– Conducting Intensive Biocomputing. With DNA sequencers in the life sciences able to generate a terabyte—or one trillion bytes—of data a minute, the size of DNA sequence databases will increase 10-fold every 18 months . . . This research team aims to create a new generation of efficient data management and analysis software for large-scale, data-intensive scientific applications in the cloud. They will leverage recent experience in delivering reliable computing over volatile cloud resources to further enhance the robustness of data management and analysis software. They will strive to eliminate the need to assume "no hardware failures" or "very infrequent failures" as is the case with traditional HPC data-management techniques.

Working in collaboration with the NSF teams, Microsoft has continued to develop client tools to leverage the power of the cloud and empower the research community. One example is an addition to Microsoft's Excel spreadsheet software, called Excel Datascope. Directly from Excel, a user can share data with collaborators around the world, discover and download related data sets, or sample from extremely large data sets in the cloud. It also provides new data analytics and machine learning algorithms, the execution of which transparently takes place on Windows Azure.

Driving Efficiencies, Innovation and Agility for Businesses and Governments.

The business questions are the same for any young entrepreneur or seasoned CEO.[5] How do I differentiate myself from my competition? How do I best deploy my resources and maximize the return on my investment? How can I be nimble? How can I survive and flourish? To answer these questions, a leader must understand and use the disruptive economic and technological forces of his or her time.

The cloud offers small and large companies alike new opportunities to focus on core capabilities, compete in new ways in new markets, reduce capital costs, and increase efficiencies.

[3] Windows Azure is Microsoft's cloud computing platform that provides on-demand computing and storage to host, scale and manage applications and data through Microsoft data centers.

[4] See NSF Press Release of April 20, 2011 at http://www.nsf.gov/news/news—summ.jsp?cntn—id=119248.

[5] The business-related topics in this section were also discussed in a supplemental advertorial by Dr. Daniel A. Reed in the June 2011 issue of Harvard Business Review.

Before the cloud, a small company could only create an Internet presence or harness IT capabilities by buying and building IT infrastructure and hiring IT support staff, a daunting and financially challenging prospect for many. Large companies who used IT to support their businesses in new or increased ways faced the same challenges. The best and worst experience that could happen to a company was that its latest "widget" would be suddenly popularized in the media, and a deluge of queries or orders would appear in a short time frame, overwhelming its IT infrastructure.

Cloud computing allows elastic scaling to meet varying demand, not only in the capability but also in the management of that infrastructure. With cloud computing, companies of all sizes can be nimble and make forward bets—quickly and without large capital costs. This enables those smaller companies to compete globally with companies of all sizes, fostering an environment of innovation and growth, and enables larger companies to scale and handle burst demand, as well as experiment with new products, approaches, or business models.

Moreover, by reducing infrastructure cost and IT staff requirements, the cloud also lets companies focus on their core competencies, delivering their unique products and services to their customers. The lesson of business over time has been that success accrues to those companies who focus on their differentiated competencies, and partner with the other companies who specialize in ancillary or support services. The core competency of healthcare providers, manufacturers, retailers and others is not the management of IT infrastructure.

Further, the cloud offers unique opportunities to support global, multi-party and neutral collaborations-allowing a diverse set of scattered experts to bring their expertise to bear on a joint activity. No matter how large a business is, there is both a collaborative as well as a competitive environment with other companies or entities. The ability to share and extract insights from information by virtue of partnerships with multiple parties is a powerful concept. This is particularly important in this time of converging industry sectors-smart vehicles are bringing auto manufacturers, energy utilities, and entertainment companies together. Collaboration among these diverse parties raises a host of issues—extracting the relevant data, correlating concepts, bridging cultural and technological divides, and alleviating competitive concerns. The cloud allows all these parties to access the data in neutral ways, using shared or separate tools, and to collaborate using many different models for responsibility, data ownership, and service delivery.

Just as it does for businesses, the cloud can enable local governments and federal agencies to focus on their core competencies rather than IT and to act nimbly. Rarely is IT a government service itself; it is an enabler that allows government to conduct essential operations and deliver services. Government can take advantage of the efficiencies of the cloud to lower operating costs for government services, to deliver new services in more nimble and adaptive ways, and to partner with other organizations.

The city of Miami, for instance, is using Microsoft's Windows Azure cloud platform for Miami311, an online service that allows citizens to map some 4,500 non-emergency issues in progress. The 311 package combines multiple IT capabilities, including mapping, communications, web-based interfaces, and databases and systems for tracking calls and responses. These combined capabilities have enabled the city to transform what had been a difficult-to-use list of outstanding service requests into a visual map that shows citizens each and every "ticket" in progress in their own neighborhood and in other parts of the city.

Clouds, together with data-generating sensors, provide the mechanisms to combine and analyze large data sets in new ways and extract insights. Consider all the data that has been collected by the U.S. government, much of which has been used sparingly or by single programs or agencies. Clouds could allow data from different agencies, different levels of government, state or federal, and even the private sector to be combined and used in powerful ways. One could think about connecting historical earthquake data with local information about building codes and private information about insurance policies, or using health data to analyze populations and respond to flu outbreaks or emergencies in real time.

One example of combining input from multiple government organizations is the Pew Voting Information Project. This project is building on Microsoft's cloud to provide official, customized data for voters on relevant information, such as polling place locations, including maps and directions, along with a list of candidates and issues on the ballot. The cloud implementation allows Pew to scale up the process of merging data from multiple sources and to facilitate interfaces and tools that allow others to create and disseminate applications that build on this information.

Enriching Experiences to Empower Individual Citizens.

Today, most of us own hundreds of computers, from PCs and smartphones to embedded devices in our cars, home appliances, and entertainment systems, and we interact with thousands of others embedded in society's everyday supporting infrastructure, from health monitors to traffic sensors. The number of such devices is soon projected to exceed 50 billion, most connected to the Internet, communicating device-to-device, device-to-cloud, and cloud-to-device. The future is a seamlessly connected world of devices and services.

Today, we can already see glimpses of this. While in transit, I can use my smartphone to connect to Microsoft's Bing search engine and ask a question. With the location from the smartphone's GPS, speech-to-text translation and location-specific data, Bing can return an answer—the nearest movie theater is four blocks away; click here for directions and to purchase a ticket. Such tailored, contextually appropriate experiences are only possible through the combination of devices, sensors and diverse cloud services.

In the future, my smartphone and the cloud might well cooperate with my plug-in hybrid car. The appointments in my smartphone's calendar, together with traffic data and my car's continuously monitored energy usage will allow the cloud to plan my driving route and charging plan, even alerting the utility as to the expected energy load from all cars being charged. While this might sound like science fiction, scenarios like this are being explored today, enabled by the combination of devices, networks and clouds.

III. The Next Steps: Recommendations for Moving Forward

To realize the opportunities that the cloud creates for research, business, government, and individuals, there are specific steps the U.S. government should consider in four areas.

1. Deploy the Cloud for Government and Research Use. The U.S. government, including research agencies, should be at the forefront of deploying the cloud in innovative and effective ways.

The federal government is actively exploring and implementing cloud solutions across many agencies. In so doing, it is discovering, as has the private sector, that clouds provide operational efficiencies and new sources of value. **The federal government should move expeditiously to adopt cloud capabilities, beginning with those services and data that directly match industry experiences and best practices.** NIST can and is playing a valuable role in disseminating cloud best practices across the U.S. government, in defining standards for cloud security and in working with other groups to foster understanding of opportunities afforded by clouds. In addition, **the government should explore how clouds could allow data from different agencies, different levels of government, and even the private sector, to be combined and used in powerful new ways.**

Second, and specifically, **federal research agencies should embrace the cloud to host large-scale data sets, accelerate scientific discovery and create new opportunities for data intensive exploration and multidisciplinary collaboration.** In addition, **the federal rules for allowable research expenses should encourage and enable the use of IT services, such as the cloud,** where appropriate, rather than duplicative purchase and maintenance of IT infrastructure.

Finally, **federal research agencies should also support the development and implementation of new algorithms and tools that simplify access to the burgeoning scientific data archive, facilitating collaboration and ease of use.** These tools would reduce the time researchers, staff and students spend on IT management, allow more scientists to tap the power of the cloud and more easily build and share analyses and insights. The tools and techniques developed by and for researchers analyzing and interpreting large quantities of heterogeneous data have potentially broad applicability in domains as diverse as health, security, energy, and business analytics.

2. Ensure Adequate Wired and Wireless Connectivity. The web and cloud services depend on broadband communications. Without them, service and information sharing are impossible. Concomitantly, ensuring reliable wired and wireless connectivity, with adequate bandwidth and latency, is critical to ensuring successful adoption of the cloud and realization of its benefits. The phenomenal growth of digital data, the rise of streaming media services, and the explosive growth of Internet-connected devices are all straining our nation's broadband infrastructure.

It is critical that we **continue to design and deploy new backbone networks that support higher data rates, develop and deploy new protocols and infrastructure for the next generation of wireless networks and define the global standards that will shape the future of the globe-encircling cloud.**

We must also remember that digital access to information and services is increasingly the enabler of economic competitiveness, of lifelong education in a rapidly changing world, and of government efficiency and service delivery.

These are technology challenges, requiring new semiconductor approaches and device designs, optical networks and switches, and software and adaptive spectrum management. They are also policy challenges, where the growth of demand and shifting expectations challenge our existing approaches to network regulation, construction, deployment and operation. We need to adopt a new model that fosters innovation and rapid, large-scale deployment, recognizing that the pace of change is quickening.

3. Foster Continued Support for Computing Research and Education. Today's cloud technology-software and services, servers and storage, PCs and smart phones, wired and wireless networks-is derived from basic computing research conducted by universities, government laboratories, and companies over the past four decades. Yet each new computing era brings new questions and new research opportunities and needs. Clouds are no exception.

To ensure that the U.S. continues to remain at the forefront of cloud technology, continued investment in basic research is critical. There are deep and open questions in areas as diverse as the future of silicon scaling and system-on-a-chip design, energy-efficient system design, primary and secondary storage, data mining and analytics, wired and wireless networks, system resilience and reliability, privacy and security, and user interfaces and accessibility, to name just a few. Insights and innovations from this research will spawn new companies, create jobs and reshape our future.

In addition to continued research investment, it is critical to **support the pipeline that produces researchers, and others who will able to invent new uses of the cloud and information technology.** The Bureau of Labor Statistics estimates that the computing sector will have 1.5 million job openings over the next ten years, yet the number of graduates receiving Bachelors, Masters or Ph.D. computer science degrees in 2009 was approximately 45,000. While the number of degrees is trending upward, it falls far short of where it needs to be to meet the demand. For example, in May, Microsoft had 4,551 unfilled job openings, of which 2,629 were for computer science positions.

To meet this current and future demand, the U.S. must strengthen the quality of and access to computing education at all levels, particularly K–12. Such efforts, by federal, state, and local governments, as well as by companies and non-profit organizations, will not only provide a more capable and larger workforce for IT research and operations, but also raise the overall computing-related capabilities of the population. Strong analytical thinking and understanding of technological systems will be necessary for many careers as IT continues to permeate more and more aspects of society.

Consistent with these concerns about the IT workforce and computing education, Microsoft is a founding member of the Computing in the Core coalition, which supports computer science education, particularly at the K–12 level. To tackle these challenges, the coalition advocates for coordinated efforts on a number of fronts: improving the training, certification, and support for K–12 computer science teachers, as well as increasing their numbers; improving the available standards and assessments, and developing appropriate courses, for K–12 computer science courses; ensuring that computing courses count toward a student's core graduation requirements; and expanding access to and participation in computing courses by underrepresented populations.

4. Revise Policies in Light of Technology Change. Every new information technology shift brings change. In each case, the benefits of change accrue to the prepared and adaptable. Many of our current policies and regulations have not kept pace with new technology developments, and their revision is important to accelerating the implementation and benefits of cloud.

Many such issues are discussed in the report of the Commission on the Leadership Opportunity in U.S. Deployment of the Cloud (CLOUD^2), which has been described by another witness at this hearing. For example, policies around the Electronic Communications Privacy Act, processes for pursuing and prosecuting cybercriminals, privacy frameworks, and transnational data flows require reconsideration in light of current technologies and in recognition that technology is rapidly evolving.

The best approach in a time of rapid technological change is to establish policy goals and a flexible framework for achieving them, and to avoid focus on specific technological approaches that could chill innovation or quickly become outmoded.

***

The cloud is the foundation of the 21st century digital economy. This is an exciting time, when the future becomes the present. Access to the power of the cloud can be a great equalizer, providing access to the world's knowledge base to individuals, anywhere, anytime; empowering entrepreneurs and companies large and small to sell their products and ideas globally; and enabling scientists and engineers to discover and innovate in ways that will define the future.

Will we come together and take the steps necessary to prepare and enable this vision for the future? I believe we can and we will. Working together, the private and public sectors can ensure U.S. competitiveness and cloud adoption in the short term, and realize the benefits that result from the cloud's new capabilities and experiences in the long term.

In conclusion, let me thank you for this Committee's longstanding support for scientific discovery and innovation. I would be pleased to answer any questions you might have.

Chairman QUAYLE. Thank you, Dr. Reed. I now recognize Mr. Combs for five minutes.

STATEMENT OF MR. NICK COMBS, FEDERAL CHIEF TECHNOLOGY OFFICER, EMC CORPORATION

Mr. COMBS. Chairman Quayle, Ranking Member Luján, and other distinguished Members of the Subcommittee, thank you for the invitation to address both the opportunities and challenges associated with cloud computing.

My name is Nick Combs and I am the Chief Technology Officer for EMC Corporation's Federal Division. Prior to joining EMC, I spent 25 years in the Federal Government, including senior positions in the Department of Defense and the intelligence community. Over the course of my career, I experienced many of the IT challenges facing organizations today, particularly as enterprises transition to cloud services.

For today's testimony, I was asked by the Subcommittee to discuss some of the major cybersecurity challenges facing cloud service providers and adopters.

During the past couple years, the frequency, volume, and impact of cyber attacks has reached pandemic levels. Those attacks are resulting in real economic harm, as well as posing very significant national security challenges. Because the Internet is used by everyone everywhere, by large and small government and commercial organizations, there are multiple avenues of exploitation. The targets of more advanced cyber attacks now include organizations as diverse as pharmaceutical and automotive companies to the defense industrial base and government agencies, and yes, even information security companies.

As you may know, RSA, the Security Division of EMC, announced on March 17 of 2011 that it detected a sophisticated cyber attack on its systems. The attack on RSA was a stark reminder to us and for the entire information security community that no one is immune from cyber attacks. The attack also reflects the sophistication of advanced attackers in understanding the interconnections and the interdependencies organizations have in our network world and how to exploit those relationships to achieve their goals.

And this brings us to cloud computing, which is fundamentally changing the way that organizations think about IT. There is a lot of confusion in the market today, especially around what type of clouds and what type of data is appropriate to go into those clouds, whether it is public, private, community, or hybrid, CIOs must have the information available to make risk-based decisions on what information should be placed into what types of clouds. Most security architectures of today are nothing more than a broken safety net of point security solutions products.

During the next several years, cloud computing adoptions could enable organizations to improve information security by replacing the disparate and legacy IT systems that are so common today. Instead of having IT and information security organizations protecting stovepipe systems, organizations are able to implement centralized monitoring, management, and security solutions. Security is also being built into the information infrastructure that makes the foundation of the cloud, including virtualization and data storage platforms.

Cloud computing holds special promise for smaller organizations which left to their own device cannot always afford the advanced expertise and technologies necessary to protect against today's threats. Those organizations, by consuming IT services from cloud providers, can gain the benefits of advanced security in an affordable way.

Through the cloud, organizations can centrally manage their IT systems and provide uniform policy implementations. They will reduce the operating and management cost, thus freeing up resources to address other needs.

EMC supports the Administration's "cloud-first" strategy, and along with the ongoing data center consolidation efforts, we believe that the policies, if fully implemented, will save the Federal Government billions of dollars in IT budgets annually. In this skyrocketing budget deficits and new budget caps, now is the time for Federal Government agencies to adopt—to accelerate their adoption of cloud infrastructure and services.

Many federal agencies have already begun to build the cloud—the bridge to the cloud by adopting some form of virtualization. For example, right here in the House of Representatives, your IT organization has utilized virtualization in its transition to the cloud. Technologies and best practices exist today to deliver private cloud environments inside federal organizations to gain dramatic IT improvements and IT efficiency while also providing the security required to protect the sensitive information within the government enterprise.

Security must be—must evolve to become much more centered around the users and on the information they are accessing. For that reason, emerging technology practices such as adaptive authentication and data loss preventions are both widely used in the commercial world and should be increasingly used in Federal Government agencies.

As I conclude my testimony, I would like to comment on the role of NIST in advancing cloud computing and trust in the cloud. Through its cloud computing workshops, NIST has already played a vital role in bringing together the public and private sectors to zero in on security interoperability and portability challenges related to the cloud. Congress should also allow federal agencies to select the cloud deployment models that best fit the business needs and security needs rather than favoring one cloud model over the other.

I again thank the Committee for allowing me to contribute to this hearing today. Thank you and I look forward to your questions.

[The prepared statement of Mr. Combs follows:]

PREPARED STATEMENT OF MR. NICK COMBS, FEDERAL CHIEF TECHNOLOGY OFFICER, EMC CORPORATION

Written Testimony of
Nick Combs
"The Next IT Revolution? Assessing the Opportunities and Challenges of Cloud Computing"
Before
Committee on Science, Space, and Technology
Subcommittee on Technology and Innovation
September 21, 2011

Chairman Quayle and other distinguished Members of the Subcommittee, thank you for the invitation to address both the opportunities and challenges associated with cloud computing.

My name is Nick Combs and I am the Chief Technology Officer for EMC Corporation's Federal Division. EMC is one of the world's leading information technology companies and a global leader in enabling businesses and service providers to transform their operations and deliver IT as a service. Fundamental to this transformation is the topic of today's hearing -- cloud computing. Through innovative products and services, EMC and its more than 50,000 employees around the world are accelerating the journey to cloud computing, helping IT departments to store, manage, protect and analyze their most valuable asset — information — in a more agile, trusted and cost-efficient way.

Prior to joining EMC, I served for more than 25 years in the federal government, including senior government positions as the Deputy Chief for Enterprise IT Solutions at the Defense Intelligence Agency, where I was responsible for the engineering and program management of all activities in the Department of Defense Intelligence Information Systems (DoDIIS) environment. I also served as the IT Director and Chief Information Officer of the National Media Exploitation Center (NMEC) under the Office of the Director of National Intelligence. Over the course of my career in government and the IT industry, I have experienced many of the IT challenges facing organizations today, particularly as enterprises transition to cloud services.

As an industry leader on cloud computing, EMC teamed with Cisco (along with investments from VMware and Intel) to start VCE or the Virtual Computing Environment company. VCE represents 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. We will all hear more from VCE's Michael Capellas at today's hearing in his role as Co-Chairman of the TechAmerica Foundation Commission on the Leadership Opportunity in U.S. Deployment of the Cloud (Cloud2 Commission).

EMC also has a seasoned Technical Advisory Board to help shape the strategic vision of private and hybrid clouds and beyond. This Board, comprised of recognized industry experts from business and academia, focuses 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, information security, application middleware, and technical computing.

For today's testimony, I was asked by the Subcommittee to discuss some of the major cyber security challenges facing both cloud service providers and adopters.

During the past couple of years, the frequency, volume and impact of cyber attacks has reached pandemic levels. These attacks are resulting in real economic harm as well as posing very significant national security challenges. Because the Internet is used by everyone, everywhere, and by large, small, government and commercial organizations, there are multiple avenues for exploitation. The targets of more advanced cyber attacks now include organizations as diverse as pharmaceutical and automotive companies to oil and gas firms and the defense industrial base and government agencies; and yes, even information security companies.

As you may know, RSA, the Security Division of EMC, publicly disclosed on March 17, 2011, that it had detected a sophisticated cyber attack on its systems. The attack on RSA was a stark reminder for us – and for the entire information security community – that no one is immune from cyber attacks. The attack also reflects the sophistication of advanced attackers in understanding the interconnections and interdependencies organizations have in our networked world and how to exploit those relationships to achieve their goals.

And this brings us to cloud computing, which is fundamentally changing the way that organizations think about and implement IT. As the Cloud2 Commission pointed out in its recent report, cloud computing is really based on a simple idea: "By allowing [IT] users to tap into servers and storage systems scattered around the country and around the world – and tied together by the Internet – cloud service providers can give users better, more reliable, more affordable, and more flexible access to the IT infrastructure they need to run their businesses, organize their personal lives, or obtain services ranging from entertainment to education, e-government, and healthcare."

We agree and this shift brings new efficiencies, cost savings, and helps organizations gain more productivity from their IT systems. We also believe that the adoption of cloud computing will help improve cyber security over the long-term. While ensuring "trust in the cloud" is critical to spurring cloud adoption, there should be tangible improvements in security that come with the shift to the cloud that is underway.

In the next several years, cloud computing adoption could enable organizations to improve information security by replacing the disparate and legacy IT systems that are so common today. Instead of having our IT and information security organizations protecting stove-piped systems, organizations are able to implement centralized monitoring, management and security solutions. In addition, security is being built into the information infrastructure that makes up the foundation for cloud computing including virtualization and data storage platforms. Cloud computing also holds special promise for smaller organizations which, left to their own devices, cannot always afford the advanced expertise or technologies necessary for protection against today's threats. Those organizations, by consuming IT services from cloud providers, can gain the benefits of advanced security in affordable ways, with the costs spread over hundreds or even thousands of cloud customers.

I will discuss managing risk and building trust in the cloud in more later in my testimony, but before I do that I would like to provide more information about cloud computing, the benefits of cloud, and our thoughts on the current federal strategy for cloud computing.

First, I would like to comment on the term "cloud computing" and its definition. It is a term that is becoming widely used and is all around us in TV commercials and newspapers and magazines. Cloud has become one of the most common yet most misunderstood references to information technology and services. In fact, I would venture that many of us in the room have family members that are heavy cloud computing users -- without them even knowing it – whether through social media networks, Internet retailing or via the advanced capabilities of smartphones. Cloud computing is increasingly the infrastructure consumer-facing applications are built on.

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. The National Institute of Standards and Technology (NIST) at the U.S. Department of Commerce has provided definitions of these delivery models that help provide more clarity˙

- ***Private Cloud.*** *The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and 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. It may be managed by the organizations or by a third party on premise or off premise.*
- ***Public cloud.*** *The cloud infrastructure is made available to the general public or a large industry group and is owned and operated 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 that are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds.)*[1]

[1] "The NIST Definition of Cloud Computing (Draft)" by Peter Mell and Tim Grance, Special Publication 800-145 (Draft), January 2011.

The customers that we serve on a daily basis collectively deploy all of these types of cloud computing models. EMC and its subsidiary companies deploy solutions and services via private, community, hybrid and public clouds. As an enterprise, EMC has utilized its solutions, as well as virtualization technology from VMware – the foundation of cloud infrastructure – as our IT organization leverages private clouds internally, reducing our own IT costs and energy bills.

In the first phase of EMC's internal shift to a cloud-based infrastructure, our company gained $74 Million in data center equipment savings, $12 Million in power and space savings and a 34 percent increase in energy efficiency. This was just the initial savings for the company; cost savings is one of the reasons why so many organizations in both the public and private sector are moving to cloud computing. And, in both industry and government, we are seeing data center consolidation move forward – with the associated cost savings – in tandem with organizations' transition to cloud infrastructure and services.

On July 20, 2011, the White House announced plans to shut down 373 data centers within the federal government by the end of 2012 as part of the President's goal of closing 800 data centers by 2015, a move that is projected to save more than $3 billion.[2]

EMC has been enabling customers to further their virtual datacenters and embrace cloud computing through the solutions and services it offers. Some examples of the benefits of Cloud computing reflecting various segments of the U.S. economy include:

- Oregon-based Columbia Sportswear, a leading innovator in active outdoor apparel, footwear, accessories and equipment has increased the performance of its IT infrastructure using 25 percent less space after implementing a cloud computing model. At 95 percent virtualized, Columbia has reduced its storage total cost of ownership by 40 percent while enabling 50 percent more virtual machines to be supported in the infrastructure.

- Texas-based Lone Star College System, the fastest-growing community college system in Texas has deployed a private cloud to deliver IT-as-a-Service to over 90,000 faculty, staff and students at more than a dozen locations. In moving to a cloud model, Lone Star has saved more than $600,000 in capital expenditures by utilizing virtualization and consolidating its IT environment. At 90 percent virtualized, Lone Star has reduced its energy consumption by 66 percent while increasing its ability to deliver new IT services in less than a week compared to three to four months before moving to the cloud.

[2] "White House Announces Plans to Shut Down Hundreds of Duplicative Data Centers as Part of Campaign to Cut Waste", White House Press Release, Office of the Press Secretary, July 20, 2011.

- Independent Bank, a Michigan-based bank, has also achieved many benefits from moving to a cloud environment. At 70 percent virtualized, the bank has eliminated 65 servers and avoided additional server expenditures even as its environment expands. All the while, Independent Bank has reduced the time to deploy servers from at least a day to just 1-2 hours. In addition, the bank has seen server-related power consumption dramatically reduced. When it comes to backup, Independent Bank has also reduced its backup storage capacity requirements while decreasing the time to recover data of critical systems from days to just a few hours and even minutes.

The Benefits of Cloud Computing

Cloud computing provides the characteristics that organizations need by enabling IT infrastructures to be flexible, on-demand, efficient, and resilient. In short – it allows them to be more agile. For the most part, IT systems have been built the same way for the last 40 years and it is clearly time for a change – we need more efficiency, agility, productivity, and security from our information infrastructure – with better return on investment than today's more rigid and less efficient approaches. We can no longer afford to maintain legacy and stove-piped, monolithic systems in which each computing requirement has its own dedicated IT system.

To achieve this level of IT transformation and implement technology to make it possible to run IT as a service, 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 Forrester, 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. Gartner predicts that by 2014, cloud-computing experience will be a listed or demanded skill in most hiring decisions for IT projects and believe that by 2015, 50 percent of Global 1000 enterprises will rely on external cloud-computing services for the top 10 revenue-generating processes.

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 ever-changing application software for those internal processes and accounting. We are at a point where government agencies are spending a majority of their IT budgets just to maintain their 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 a means through which to address this imbalance in how taxpayer funds are spent.

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 an organization's security posture.

In short, as the Cloud2 Commission noted in its report: "Cloud technologies are transforming the way computing power is bought, sold, and delivered.

...This new business model brings vast efficiency and cost advantages to government agencies, individuals, and companies of all sizes." We firmly believe that at EMC and that's a fundamental reason why we think U.S. federal agencies should be adopting cloud computing just as aggressively as we are in the private sector.

Federal Strategy for Cloud Computing

EMC supports the Administration's "Cloud First" strategy and along with the ongoing federal data center consolidation efforts, we believe that these policies, if fully implemented, will save the federal government billions of dollars in IT budgets annually. In this area of sky-rocketing budget deficits and new budget caps, now is the time for federal agencies to accelerate their adoption of cloud infrastructure and services. As I mentioned earlier, in addition to the cost savings, the increases in energy efficiency and productivity, moving IT systems to cloud-based infrastructure and services, could also help improve cyber security.

We understand that 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 diverse 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 significant amounts of capital and maintenance costs, but enable the application and use of 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 burdensome task of managing today's complex and sometimes antiquated infrastructures. Former OMB Director Orszag made a similar point last year when he highlighted the reality 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, enabling the federal government to unleash new innovations and improve productivity.

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

Many federal organizations have already begun to build a bridge to the cloud by adopting some form of virtualization. Virtualization enables the shared use of a physical hardware resource – a simple example is a PC that is able to run multiple operating systems thanks to virtualization software. In fact, virtualization has become the foundation of the cloud and in our 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

In fact, EMC recently announced breakthrough capabilities that enable virtual storage over distance. The industry's first distributed storage federation provides unprecedented business agility by eliminating the current boundaries of physical storage. For example, the workload and information in an entire data center in the path of an approaching hurricane could be simply shifted to another one hundreds or thousands of miles away with no disruption in service and then shifted back just as easily once the storm passes. This is a key enabler to future cloud architectures.

Trust in the Cloud

Cyber security is clearly one of biggest concerns of federal CIOs who are considering implementing cloud infrastructure and services. When I speak to customers about their journey to the cloud, they consistently bring up cyber security and data privacy issues as possible barriers to adoption. 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, 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.

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.

A hybrid cloud is a result of combining a public cloud with a private cloud. Building a hybrid cloud requires new technology, new processes and trusted partners. One of the biggest benefits for hybrid clouds is the notion of "bursting". Bursting allows IT organizations to build their infrastructure for median capacity and rent additional

[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.

infrastructure from a public cloud when needed. This can dramatically reduce capital expenditures and reduce operational expenditures to a lesser degree.

Even if organizations aren't ready to do this today, they need to be building their private cloud so that this option is available when the organization and process is ready. To do this, you need an infrastructure that allows you to move and entire workload online between clouds. This requires movement of the application and the data across distance.

Second, you need a trusted service provider where you can run your workloads in the public cloud. That service provider must have compatible infrastructure to enable online movement as outlined above. The service provider must also deliver the security and controls you demand along with visibility for you to ensure compliance.

With the adoption of cloud computing infrastructure and services comes sophisticated automation, provisioning and virtualization technologies that have significant security implications, so we must look at security in a whole new way. Establishing trust first requires control and a second level of internal visibility that can be stepped up or expanded for external service providers. However, if control plus visibility is the formula for trust, how do we go about solving for it?

Solving for trust in internal (private) clouds is less challenging than in public clouds because in an internal cloud, the organization controls all IT assets, as well as the geographic location of its data. Control and visibility in internal clouds is about adapting existing processes to the virtual environment while capitalizing on the new advantages of virtualization. This is particularly the case for mission critical functions.

Mission-critical functions require control and visibility into the cloud's performance. They also require additional precautions to ensure that information in the cloud is protected against loss or system unavailability, from external or internal threats, and from data breaches. Only this heightened level of control and visibility can deliver the critical proof that leads to trust:

- Proof that cloud infrastructure meets security specifications and that information is managed in accordance with policies;
- Proof that authorized users are who they say they are; and
- Proof of performance and compliance to satisfy internal management as well as auditors and regulators.

Essential to proof is the ability to inspect and monitor actual conditions first-hand and not just rely on outside attestations, especially for applications handling regulated information or other sensitive workloads. Organizations need transparency into service providers' environments to ensure compliance with policies and Security Level Agreements (SLAs). They need an integrated view of their IT environments, both internal and external, to correlate risks, spot threats, and to coordinate the implementation of countermeasures.

Today, organizations struggle to have control and visibility in their physical IT environments. This challenge need not be exacerbated in the cloud. The good news is that virtualization technology creates the right conditions for organizations to improve control and visibility beyond what's available in today's physical environments.

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, improving information 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, emerging technology practices, such as adaptive authentication and data loss prevention, are both widely used in the commercial world and are increasingly used in federal government agencies.

We believe that in the transformation power of virtualization – so much so that we are focusing our cloud-security strategy and development initiatives on making security and compliance in the cloud 1) logical and information-centric, 2) built-in and automated, and 3) risk-based and adaptive. For years, EMC, RSA and VMware have worked to embed security, management and compliance controls into the virtualization platform.

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. 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.

As I mentioned earlier, stronger security (control) proven through direct monitoring (visibility) is one of the key best practices for trust in the cloud.

RSA, EMC's security division, is working with cloud providers to give them the means to demonstrate security and compliance to their customers, removing this barrier to greater cloud adoption. The RSA Cloud Trust Authority, announced at the RSA Conference in March of this year, gives cloud customers an easy and scalable way to ensure trusted access to multiple cloud provider, while giving the cloud providers themselves a more automated, consistent way to demonstrate compliance with cloud standards for security and confidentiality as they evolve. Over time we expect the Cloud Trust Authority to evolve to offer additional means of security and compliance for digital information and identities.

Best practices such as risk-based authentication should also be implemented in cloud environments and we think that that approach fits well within the President's National Strategy for Trusted Identities in Cyberspace (NSTIC) which was released earlier this year. This important effort, which is being coordinated by the NSTIC Office at NIST in collaboration with the private sector, should be supported by the U.S. Congress.

When implemented correctly, cloud environments can be much more secure than today's IT environments. The level of transparency cloud vendors provide is a critical aspect when choosing a cloud partner. 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 dashboards 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 success. That is one of the principle reasons that EMC supports updating the Federal Information Security and Management Act (FISMA). Enacting updated FISMA legislation that will enable continuous monitoring is essential to address today's threat environment as well as provide for an effective operational risk management framework for tomorrow's cloud computing infrastructure.

Conclusion

As I conclude my testimony, I would like to comment on the role of NIST in advancing cloud computing and trust in the cloud. Through its cloud computing workshops, NIST has already played a vital role in bringing together the public and private sector to zero in on the security, interoperability and portability challenges related to the cloud. NIST has also added clarity in its work on coming up with a comprehensive definition of cloud computing.

NIST has also played an instrumental role in the development of the Authorization Management Program (FedRAMP) and NIST Security Content Automation Protocol (SCAP). FedRAMP is a voluntary, General Services Administration (GSA)-led initiative to develop and provide a standard approach to assessing and authorizing cloud computing services and products for use by Federal agencies. The NIST SCAP standard enables the automation of reporting and verifying IT security controls. SCAP provides an effective method to capture, test and continuously monitor these controls.

Both of these initiatives are important steps in the transition of the Federal Government from the old FISMA focus on compliance, to better operational risk management and continuous monitoring under the new FISMA. This process is critical for improving cyber security today as well as positioning the federal government to fully utilize the transition to the cloud to help improve cyber security.

Congress should also allow federal agencies to select the cloud deployment models that best fit their business and security needs, rather than favoring one cloud model over the other.

I again thank the Committee for allowing EMC and me to contribute to the hearing today. Information technology is ushering in dramatic change with the shift to cloud computing and 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. Security is a legitimate concern, but the technology and best practices exist to address many of those risks and more innovation is happening right now as we sit here together today.

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 commercial organizations, government agencies and many others and we should do what we can now to embrace the shift to cloud computing that is underway.

Thank you and I look forward to your questions.

Chairman QUAYLE. Thank you, Mr. Combs. I now recognize Dr. McClure to present his testimony.

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

Dr. MCCLURE. Thank you, Chairman Quayle and Congressman Luján. It is a pleasure to be here, and I would like to applaud the Subcommittee's leadership in expanding the dialogue and understanding of new cloud technologies, and the risks and the rewards they offer for modernizing the government's IT.

As you have heard from the other witnesses today, cloud computing really offers a compelling opportunity to substantially improve the efficiency, agility, and performance of federal IT. With cloud, agencies pay only for the resources they use in response to fluctuating demand, they avoid the expenses of building and maintaining costly IT infrastructure, and ensure the appropriate level of security for data and applications.

At GSA, we are developing new cloud computing procurement vehicles that leverage the government's buying power, we are ensuring effective cloud security standards are in place to lower risk, we are identifying and leveraging government-wide adoption of cloud solutions such as email and collaboration. My written statement highlights our significant progress under the 25-point IT Reform Plan in areas like data center consolidation analysis and cost-modeling, more robust government-wide security approaches under the soon-to-be-launched FedRAMP program, and efficient procurement vehicles.

Let me summarize my written statement provided to you with three key points. First, agency executives should focus on the desired government, business, or mission outcome driving cloud adoption rather than cloud technology itself. We know there are opportunities for improving the cost-effectiveness and efficiency of IT used in the Federal Government. CIOs need to develop and deploy effective cloud solution strategies that address pressing agency needs taking into account cost savings and expected performance improvements. Agencies must analyze business needs and identify cloud solutions that best fit their requirements by making cloud adoption part of an overall IT portfolio management and sourcing strategy.

In short, cloud readiness assessments and prudent decisional roadmaps are essential to move forward both decisively and expeditiously in cloud computing.

Second, while early, we definitely are seeing concrete benefits from the adoption of cloud computing solutions in the Federal Government, particularly for low- and moderate-risk data areas. At GSA and USDA, for example, we expect to see email costs cut by 50 percent, and many other agencies are projecting similar results.

The benefits are not just around cost reduction. Cloud deployments allow for much faster deployment of systems and applications. Provisioning can occur in hours or days as opposed to traditional months or years. It can increase productivity, it gives agencies greater flexibility and scalability, it enhances our sustainability postures, and it improves self-service capabilities. As agencies consolidate their virtual data centers, cloud provides an ideal path forward.

Third, while the path forward for cloud computing is positive, we still must pay attention to the inherent risk associated with its use, as is the case in virtually all technology areas. The risks generally revolve around the evolution of some key standards designed to address technical, operational, and managerial risk associated with computing in general. Let me mention three key standard areas.

Number one is establishing baseline security standards that must be met by cloud service providers. We are taking steps to achieve this via our FedRAMP program, which we have designed with extensive industry and government-wide participation and feedback. We are establishing a common set of baseline security assessments and continuous monitoring requirements for cloud computing using NIST standards. We are providing a common, consistent, security-risk and authorization process that can be leveraged across agencies, the use-once-and-often approach.

Certifying qualified, independent, third-party assessors is another area where we are spending a great deal of attention so that we can bring some consistency and uniformity in how cloud security assessments are done. And we are shifting the risk from annual reporting under FISMA to more robust continuous monitoring providing real-time detection and demonstration of successful mitigation of vulnerabilities.

The other two standards areas involve interoperability and data portability. NIST is taking the lead in these two areas. It is aggressively pursuing use-case study approaches that can adequately demonstrate the utility of proposed standards in test scenarios so that market solutions can proceed and be moved into the Federal Government. These two things can help protect against vendor lock-in and ensure data reconstitution should an agency decide to move its services to another provider.

Thank you, Mr. Chairman. That concludes my statement. I would be glad to respond to any questions.

[The prepared statement of Mr. McClure follows:]

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

Chairman Quayle and Members of the Subcommittee:

Thank you for the opportunity to appear before you today to discuss the General Service Administration's (GSA) leadership role in ongoing efforts to enable and accelerate adoption of cloud computing across the federal government. Cloud adoption is a critical component of the Administration's plan to improve management of the government's IT resources. The reforms underway are enabling agencies to use information more efficiently and effectively, delivering improved mission results at lower cost.

Cloud computing offers a compelling opportunity to substantially improve the efficiency, agility and performance of the federal information technology portfolio. It allows agencies to pay only for the resources they use in response to fluctuating demand, avoid the expenses of building and maintaining costly IT infrastructure, and control the appropriate level of security for data and applications. Cloud computing is also a key technology for achieving cost effective IT. In fact, agencies have already started to realize numerous benefits as they begin to adopt cloud computing across their programs. These include cost reduction, faster deployment of systems and applications, increased productivity, greater flexibility and scalability and improved self-service capabilities. As agencies consolidate and virtualize their data centers, cloud provides an ideal path forward to achieve needed results while substantially lowering costs—an essential focus given federal budget constraints.

GSA is playing a leadership role in 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 reducing barriers to safe and secure cloud computing. We are developing new cloud computing procurement options with proven solutions that leverage the government's buying power, ensuring effective cloud security and standards are in place to lower risk, and identifying and leveraging government-wide uses of cloud computing solutions such as email. These are highlighted on our web page Info.Apps.gov, which provides useful information about cloud computing and available solutions.

The Administration's efforts to apply rigor to information technology management and foster cloud adoption is framed by several key guidance documents and policies, including the *OMB 25 Point Implementation Plan to Reform Federal Information Technology Management and the Federal Cloud Computing Strategy* issued by the federal CIO's office. The initiatives being implemented in response to these documents are making significant progress tackling long standing challenges in the way IT is acquired and managed. These reforms are also meeting the Administration's goals to make government more responsive, operationally effective, cost efficient, transparent, participatory, collaborative, and innovative for the citizens it serves.

The Subcommittee asked that I address the four questions outlined below.

(1) Please provide an overview of how the General Services Administration (GSA) is implementing the Office of Management and Budget's (OMB) 25 Point Implementation Plan to Reform Federal Information Technology Management, the OMB Federal Data Center Consolidation Initiative, and the Federal Chief Information Officer's Federal Cloud Computing Strategy.

GSA plays a central role in realizing the goals set forth in the Administration's initiatives and strategies to reform IT management, consolidate data centers and implement cloud computing. Below are the primary initiatives underway to achieve the policy goals of Data Center Consolidation, the Cloud Computing Strategy and the specific objectives of the 25 Point Plan.

Below is an overview of the work we are conducting to support specific objectives of the Federal IT Reform Strategy. Each objective of the 25 Point IT Reform Plan for which GSA is directly responsible is identified in bold; the specific section is in parenthesis.

Complete detailed implementation plans to consolidate at least 800 data centers by 2015 (#1)

Create a government-wide marketplace for data center availability (#2)

The Federal Data Center Consolidation Initiative (FDCCI), managed jointly by GSA and OMB, is charged with reversing the federal government's explosive data center growth to optimize and improve efficiency of federal IT infrastructure. The FDCCI is chartered to engage with agencies, support and facilitate agency data center consolidation planning, and to provide tools to federal partners.

Under the FDCCI, GSA is accomplishing the following:

- Working with a government-wide task force co-chaired by DHS and DOI that meets monthly and includes representatives from all 24 CFO Act agencies.
- Assisting agencies to maximize the return on investments for data centers to remain in their inventory after consolidation
- Ensuring consistent data collection of the federal data center inventory by developing and disseminating standard templates to collect, manage, and analyze agency data center inventory data.
- Collaborating with industry on best practices and solutions for key data center consolidation issues.
- Developing a comprehensive data center Total Cost Model for agencies to use to analyze alternative consolidation scenarios, enable data-driven decision-making for infrastructure cost and performance optimization.
- Pursuing development of a data center marketplace that would help optimize infrastructure utilization across government by matching agencies with excess computing capacity with those that have immediate requirements. A working

group is addressing consensus-building, requirements gathering, and other key facets necessary to ensure the marketplace's success.

Stand up contract vehicles for secure IaaS solutions (#4)

IT infrastructure represents a multi-billion dollar investment that requires constant maintenance, expensive technology upgrades, and dedication of valuable personnel. Agencies are faced with outdated infrastructure requiring ongoing, major investments to keep pace with growing demand and rapidly changing technology. Servers across both government and industry are highly underutilized. To address these issues, GSA's Federal Acquisition Service (FAS) established a Blanket Purchase Agreement (BPA) with 12 companies (many with multiple partners) that offer cloud storage, computing power, and cloud-based website hosting as commodity services that enable agencies to optimize their infrastructure and achieve substantial, long-term cost savings. Under these Infrastructure as a Service (IaaS) contracts, agencies pay only for what they need, define performance requirements, have the flexibility to respond to changing demands, benefit from commodity pricing, and are assured of secure solutions. At present, four contractors are offering services under the BPA, with the remaining completing the security authorization process. DHS has recently awarded a task order under this BPA for the consolidation and migration of its public facing websites to a cloud hosting service.

Stand up contract vehicles for commodity services (#5)

Working closely with email and collaboration experts from across government, GSA developed a government-wide contract vehicle to help agencies move email and collaboration solutions to the cloud. The Email as a Service (EaaS) BPA is an active procurement managed by FAS; responses are currently being evaluated. It will offer federal customers a streamlined procurement vehicle to commercially available cloud email solutions that best fits their agency's needs. Based on information from Forrester Research, average cost savings for agencies migrating to cloud-based email are expected to be $11/mailbox/month, $1 million in annual savings for every 7,500 users, or approximately 44% over existing on-premise email solutions. The BPA will offer a range of email services in public, private, and highly secured clouds, making available robust, feature-rich, secure email and collaboration service options similar to those currently being implemented at GSA, USDA, USAID, DOE, and other agencies. It can meet the needs of the 15 agencies that have identified 950,000 e-mail boxes they plan to move to the cloud under the Administration's IT Reform effort.

Launch an interactive platform for pre-RFP agency-industry collaboration (#25)

To streamline the procurement process and enhance communication with industry, GSA is establishing "cross-trained" program teams and improving the way requirements are defined. GSA is working to establish an interactive platform for pre-RFP agency-industry collaboration. Based on input from government and industry, alternatives for design and delivery of an online collaboration tool have been examined and rated. Candidates for the tool included existing government systems and commercial collaboration tools.

GSA not only is fostering adoption of cloud computing government-wide, but as required under the Cloud First policy, has recently completed a major cloud migration of our internal email and collaboration solution that demonstrates the significant potential of cloud solutions to achieve substantial cost savings. In approximately seven months, we moved 17,000 users to Google Apps for Government. Savings over the next five years are projected to be over $15M. Not only have we reduced costs, but we have also made significant gains in environmental sustainability—we shut down 45 servers, which is equivalent to taking 60 cars off the road. The lessons learned from our cloud implementation have been captured and are being shared with agencies across the government as they seek to achieve similar success.

2. Please provide an overview of the costs associated with implementing these plans at GSA, and provide a description of both the short-term and long-term budgetary impacts of these changes.

To date, GSA's Federal Cloud Computing Initiative has been funded under the e-Government program administered by the Federal Chief Information Officer. In FY10 and FY11 GSA's Federal Cloud Computing Initiative (FCCI) Program Management Office (PMO) budget of $4.8 million was allocated to five primary tasks:

- Establish procurement vehicles that allow agencies to purchase IT resources as commodities—resulting in the award of the Infrastructure as a Service (IaaS) Blanket Purchase Agreement under GSA Schedule 70

- Address security risks in deploying government information in a cloud environment—resulting in the development of the Federal Risk Authorization Management Program (FedRAMP)
- Establish a procurement vehicle that allows agencies to purchase cloud-based e-mail services—resulting in the issuance of the Email as a Service (EaaS) procurement that is currently underway Work with agencies to consolidate their data center asset—resulting in the Federal Data Center Consolidation Initiative that works with agencies to inventory their data center assets and to identify targets for consolidation and optimization Create apps.gov, an on-line storefront that provides access to over 3,000 cloud-based products and services where agencies can research solutions, compare prices and place on-line orders using GSA's eBuy system.

This initial funding provided by the e-Gov Fund allowed GSA to accomplish significant results. However, there are key activities that still need to be accomplished to realize the significant, additional potential cost savings and productivity improvements that GSA can help agencies achieve. The continuation of these cost-saving initiatives is dependent on FY12 eGov Fund budget levels and decisions.

3. What cybersecurity steps is the GSA taking to protect federal data and communications in the cloud? To what extent does GSA work with NIST on the development of cybersecurity standards for federal cloud computing use?

The primary goal of the Administration's Cloud First policy is to achieve widespread practical use of secure cloud computing to improve operational efficiency and effectiveness of government. Currently, each agency typically conducts its own security Certification and Accreditation (C&A) process for every system it acquires, leading to unnecessary expense, duplication and inconsistency. According to the 2009 FISMA report to Congress, agencies reported spending $300M on C&A activities alone.

Working in close collaboration with DHS, NIST, DoD and OMB and the Federal CIO Council, GSA is leading establishment of the Federal Authorization Risk Management Program (FedRAMP) to accelerate adoption of secure cloud solutions by agencies across government.

Key benefits include:

- Provides a single, consistent security risk assessment and authorization that can be leveraged across agencies—an "approve once, and use often" approach
- Establishes a common set of baseline security assessment and continuous monitoring requirements using NIST standards
- Approves and makes available qualified, independent third party assessors, ensuring consistent assessment and accreditation of cloud solutions and based on NIST's proven conformity assessment approach
- Shifts risk management from annual reporting under FISMA to more robust continuous monitoring, providing real-time detection and mitigation of persistent vulnerabilities and security incidents.

There is strong support and demand for FedRAMP from agencies seeking to adopt cloud services, as required by the Administration's Cloud First policy, and from industry. FedRAMP's processes, policy, governance, and technical security standards have all been arrived at via a consensus-based approach that includes agencies' Chief Information Security Officers, the Federal CIO Council, National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Defense (DoD), National Security Agency (NSA), and numerous industry organizations. This new program is expected to be initially launched this Fall.

4. What other challenges face federal agencies in adopting cloud computing services, and what steps is the GSA taking to overcome these challenges?

Considerable progress has been made in adopting successful cloud solutions. Cloud computing is now an accepted part of the federal IT lexicon. However, there continues to be a need for more thorough understanding of the cloud's deployment models, unique security implications, and data management challenges. Agency executives should not focus on cloud technology itself; rather, they should focus on the desired outcome driving the need for cloud adoption. CIOs need to work with their line of business executives and program managers to develop and deploy effective cloud roadmaps that address pressing agency mission needs, taking into account costs savings and expected performance improvements. Agencies should analyze business needs and identify cloud solutions that best fit their requirements by making cloud adoption part of an overall IT portfolio management and sourcing strategy.

NIST is currently working on a Cloud Computing Technology Roadmap that will be released in November. If linked to cloud provider products and services, it would greatly assist in this decision-making.

Cultural resistance is also a major challenge. Cloud adoption requires moving away from managing physical assets to buying services. As GSA's own experience has shown, these issues can be effectively addressed. Critical success factors include robust communication, practical training and emphasis on the benefits of cloud, and especially on the control agencies gain by buying what they need and defining performance metrics that are tied to desired performance results. GSA found that having a group of early adopters fostered buy-in and enthusiasm, and provided a ready corps of skilled users.

Conclusion

Mr. Chairman, General Services Administration is leading the Administration's charge to make government more open, transparent, and effective for the citizens it serves. In our increasingly data-centric and network—based world and workplace, effective and efficient procurement and implementation of information technology will be paramount in making sure the federal government closes the IT performance gap between it and the private sector. Cloud computing and data center consolidation are key initiatives that should be pursued aggressively to achieve needed costs savings and improve effectiveness of government operations.

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

Chairman QUAYLE. Thank you, Dr. McClure, and I want to thank all the witnesses for their testimony today.

Reminding Members that Committee rules limit questioning to five minutes, the Chair will at this point open the round of questioning, and I will recognize myself for five minutes.

Mr. Capellas, when looking at the data from the last 10, 20 years like you pointed out, a lot of the job creation was occurring in the IT sector, but it was also occurring with companies that are five years or younger, the startup IT, the startup companies. In Phoenix where I am from, we have a lot of the larger players like Honeywell, Intel, and some of the bigger players. We also have some smaller ones as well, but where do you think the opportunities for new service and application providers in the IT sector are going to come from? Does cloud computing offer a unique area for more startup companies to really be created in advance in that realm?

Mr. CAPELLAS. So what we are going to see—great question by the way. What we are going to see, I think, is something different than we have seen in the past, and we are going to have a bifurcation of the two sides of IT. The cloud basically says I don't have to care or know where the physical or underlying infrastructure is, and today, if you think about most cases, most IT shops, 70 percent of all costs go on physical hardware and only 30 percent on the real innovation, which is the application side. And when you think about what other business would you have where you spend 70 percent to keep the lifeline and 30 percent to really drive innovation?

What is happening today in the industry is a level of industry verticalization we haven't seen before, so I will be respectful to all the players in the industry. If you are a Hewlett Packard, you are starting—you are building an entire conversion infrastructure from servers to storage to capacity and you are going to buy that as a physical. If you are IBM, you have got your stack; if you are Oracle, you have got your stack; if you are EMC and Cisco in partnership with VM where you have got your stack; and it is much more tightly bundled. The big players will capture a much larger share of the physical side of the infrastructure because the end user will want to buy it from one place. And that is the beauty of it. You don't have to know or care.

The second big piece of this is of that physical piece, 30 percent of all IT resources are just screwing the pieces together to make a match. So what will happen is the job creation will come from the large players going to the physical side with vertical consolidation. Now, what that—on the good side of that says is then there will be a lot more people who are able to write much quicker applications. The whole world of application development will change.

And so one of the fun things I do is the average person has three connected devices and over 100 applications that they do on their smartphone and there are 500,000 smartphone applications because those applications can be generated very quickly because the physical infrastructure is there. So to answer your question very specifically, I think the large players who are vertically integrated will create the job growth, and it is imperative that U.S. companies continue to succeed as the foundation of the critical infrastructure and there will probably be fewer levels of innovation at the physical layer. But that will spawn a whole new generation of application developers and smaller companies can write quicker, lighter applications and those frameworks will be available because you can then drop those applications onto the physical infrastructure that is in place. And you will see in the world of business and other applications the same kind of just massive rollouts you have seen with the—with everybody who has got their, you know, iPhone. And how many of you could even count how many applications you have on your own phone? You probably paid a $1.99 on average for them.

So application development becomes a foundational piece. It opens up for lots of great innovation. That innovation allows IT spending to be placed where it belongs most, which is on being creative and the big guys take over running the physical infrastructure.

Chairman QUAYLE. Okay. And then I wanted you to expand on—because I would want to get an understanding is that the commissioner states that one of the things we should do is provide incentive for people to migrate to the cloud.

Mr. CAPELLAS. Yes.

Chairman QUAYLE. My question is if you are going to save—a company is going to save money and increase efficiency, isn't that incentive enough to have people moving—migrating to the cloud rather than—why do we need additional incentives to push people to the cloud?

Mr. CAPELLAS. A bit of our recommendation relates strictly—is focused on the manner of our procurement of the Federal Government and agencies.

Chairman QUAYLE. Okay.

Mr. CAPELLAS. If you think today the way agencies work is each of the departments has to measure against a unit of measurement. So if I have a personal computer, I can say I want it from company A, B, or C. If I want a server company A, B, or C but I want to buy a unit of computing, which can be shared, there is no benchmark, and so as a result, there tends to be a rollover of individual departments acting to simply get five or ten percent better than they used to be and groups not wanting to share.

At a fascinating exercise, which was brought about by Vivek Kundra, who brought us in to sort of say would you talk to the whole group and to see how many data centers could be shared by agencies crossing buying in a different way. So one of the incentives is to be able to say how about we put an incentive in place that says you will get to reinvest in your budget cycle what you saved in order to get more collaboration across groups but also to change the paradigm to simply buying something at five percent more.

Chairman QUAYLE. Okay. Thanks. And Dr. Reed, really quickly, one of the things that I have been talking with a lot of people within the research area is the lack of collaboration that has occurred. Do you think that the more people going to the cloud will actually increase collaboration, not just between the public and private sectors, but also within researchers who are working on tandem projects from different universities? Because you have been in the universities for a while even though it was UNC—I am a Dukie so we still count that as a university. But could you just explain that very briefly?

Dr. REED. Certainly. I think it is actually—it is the research version of part of the answer to the question that Mike was mentioning as well, which is many of the value propositions that exist by virtue of the rise of scientific data—and the reason why we have had explosive growth of scientific data is the same reason all of us have cheap digital cameras and lots of digital photos is because those kinds of sensors have made it very possible to capture large volumes of data economically. I exaggerate a bit, but that is fundamentally the technology piece.

What has happened in the research world is an analog actually of many other phenomena. It is true in industry and I think in government that much of the value lies actually in the intersection of data from multiple disciplines. And because those data tend to be held in silos within individual organizations, research universities, or federal agencies, it is extraordinarily difficult to cross-fertilize them and look at their intersection.

One of the things that the cloud brings to the table is the ability to host that data and make it broadly available so that one can extract insight. I think that is true in an entrepreneurship level where the ability to mine insight from data actually has economic value. It is certainly true in the research world as well. And so the ability to attack complex problems—because the traditional model of success in academia is depth in their own area, and yet many of the problems we care about cross not only technical domains but they cross social and other domains. The ability to bring people together to reason is one of the powers of the cloud.

Chairman QUAYLE. Okay. Thank you very much.

I now recognize Mr. Luján for five minutes.

Mr. LUJÁN. Thank you, Mr. Chairman.

And Dr. Reed, I appreciate again the panel's attention to the cost saving that is going to take place associated with IT tools, hardware and software. But I want to zero in on total cost, specifically energy. And can you briefly talk about what cloud computing means to smart grid application across the country as we talk about energy efficiency and lowering utility costs, energy consumption costs for businesses small and large, for people all around America and what this means to that?

Dr. REED. Certainly. Let me start with the cloud itself. One of the interesting things that has happened in the back-end infrastructure is the growth of that infrastructure at scale has driven an enormous focus in the industry on reducing the energy consumption of data centers themselves—more efficient packaging and cooling and other things. That is one of the enabling pieces, and so it is important not to forget energy efficiency there.

But if one looks at the larger question you are posing about how does analysis of data enable new possibilities? It is actually related to the Chairman's question in an interesting way, because if you think about the broad sort of issues about how being able to capture data appropriately, anonymized, private, and secure from individual homes, the future of hybrid and smart vehicles that are electrically powered where you could take that information and do intelligent route planning so that—reduce the energy consumption for the vehicles and the demand on the electrical grid by planning routes accordingly to give drivers advice about routes. Similar sorts of issues begin to accrue in the home about being able to plan when you turn on appliances, how you manage that energy, and then the same sort of things apply largely at the large-building scale whether they be federal or private buildings where understanding the behavior patterns make it possible to do some new things.

So what brings those two things together? One is this incredible world of sensors, and that is part of what the smart grid is about. The other is the ability to analyze data at unprecedented scale and generate and extract trends and behavior. It is true in healthcare; it is true in smart grids and energy; it is true in transportation; it is true in all kinds of other business, competitive worlds. It is the insight from the data that that makes possible.

Mr. LUJÁN. I appreciate that and especially with the conversation around the smart grid, recently there was a conversation in New Mexico that someone described the smart grid as the Internet for electricity. As you talk about the connectivity and really what it means to integrate, but it is really lower cost.

Along those lines, I would be interested in hearing your thoughts or any of the panel on what can be done with NIST or with the market as a whole as we talk about containing costs. So the cloud will allow us to lower utility consumption right now so on the desktop, the hardware that we are using as individuals, what can be done to lower the utility consumption, lowering cost for the data centers where we are having to spend so much money right now on the cooling? Because those temperatures when you walk into a server, we all—or data center, you all know that it is cooled. What is preventing us from getting to the point where those things can run at 72 to 76 degrees, lowering consumption costs without using outside air on the cooling as opposed to doing it inside? That way we are lowering costs for the government, the taxpayer, for you all and for businesses everywhere.

Mr. CAPELLAS. Well, that—please, go ahead.

Dr. REED. Well, I was going to say that is exactly what is happening. Please.

Mr. CAPELLAS. It is a couple of real simple things. The first one, you know, I always love, you know—one of my favorite things is unfortunately sense isn't common. Common sense tells you whenever you consolidate a huge number of servers which are very inefficient—so when you have all these small boxes running out there, the best you can hope for is 30 to 35 percent utilization. That is the best and—whether that is servers or storage. When you run these big virtualized machines because the way a cloud works is it says I am going to go grab a piece of capacity, I am always running at a higher level, you are going to 80 or 90 percent capacity utilization. So the first question is you have a whole lot more efficiency and a whole lot less boxes.

The second one is just the natural evolution of technology. We have designed into these next-generation boxes. They are much more environmentally friendly simply because we have taken power consumption as a fundamental design to lower it. So part of it is just the natural curve. The second place is just the much higher utilization that you get off the consumption.

Mr. LUJÁN. I appreciate that, Mr. Capellas. Anyone else? Mr. McClure?

Dr. MCCLURE. No, please, go ahead.

Mr. COMBS. I would just like to add, you know, an example of EMC's first phase in virtualization doing exactly what Michael was talking about, we had $74 million in data center equipment savings the first year. 12 million of that was in power and space cooling alone. And that was just in the very initial stage, which only represents about 20 percent of the savings that we have gained over our corporation's transition to the cloud. The best practices are out there. Industry is already doing this. The Federal Government can just look to industry and the successes that we have had in industry and apply those within the government.

Dr. MCCLURE. And I would agree. I think, you know, exactly the case at GSA and around the government, the average server—if you put it in real terms, the average server utilizes about 4 tons of carbon dioxide waste annually. Every server is the equivalent of—if you retire a server, on average, you are taking one and a half cars off the streets. So we point to over half a million dollars in savings by just doing virtualization technologies in our data centers. Up to 60, 70 cars taken off the road, you know, these are real terms that is showing that you are having an impact on sustainability in a real way. And the adoption of new technologies I think is absolutely essential as we go forward because the technology improvements will continue to occur.

Mr. LUJÁN. Thank you, Dr. McClure. I notice that time has run out. I think we will get another chance to ask a few questions here, but I really appreciate the attention to the cost savings that we will yield from energy consumption as well for businesses all over the country as well as residential. Thank you.

Thank you, Mr. Chairman.

Chairman QUAYLE. Thank you, Mr. Luján.

The Chair now recognizes the Chairman of the Full Committee, the gentleman from Texas, Mr. Hall.

Chairman HALL. Mr. Chairman, thank you.

Dr. Reed, in your testimony, you state that the need to adopt a new network policy model that fosters innovation and large-scale deployment indicates that you think that they don't already have that. I guess my question is what way do you see the current model as inadequate and what changes would be required to foster innovation and large-scale deployment?

Dr. REED. So it is really a comment on the fact that if one looks at any set of computing technologies that it is the ratios of speeds and capacities that determine the efficacy. So if we look at the rise of consumer devices, the speed and power consumption of the devices, their performance, their form, factor, and mobility really made some things possible.

One of the challenges we face in networks, there are two fundamentally in my judgment, and they are related in the spirit that I said networking is the oxygen that lets cloud services breathe because it is the conduit of the information and services from the data center to the consumer, whether that consumer be a government agency, a company, or an individual. The rate of growth and scale of the data that is being produced is challenging the speed of the broadband networks that we have deployed in this country. It is the electronic analog of saying we have too many cars on the road; we need to address the issue. So the ability to deliver that data reliably and at high volume across the country and indeed the connections of the rest of the world is a big piece of that.

The other is the pressure that we are all experiencing in wireless communications and the explosive growth of the number of devices and the expectations that we all have for not only access to data but the ability to deliver multimedia, audio and video to those devices is stressing many of the historical approaches that we have had, the spectrum allocation and management.

So what I am really saying is we have to face both of those issues and work together to address the need not only to continue to expand the speed and coverage that we have for our optical and wired networks but continue to work together to address the access issues that will deliver those just-in-time services. Because that smart grid vision of the world depends on wired and wireless access to that information to be able to make those intelligent decisions.

Chairman HALL. Well, you say that we have to address—I guess if you told me I didn't get your answer as to how, what kind of changes would be required? What special changes would you make?

Dr. REED. So it is a good question. I will try to be a bit less circular in my answer. I apologize.

We have to build out more networks and we have to find mechanisms to make that happen more rapidly. On our wired networks, if you think about the speeds that we normally denominate units in, we talk in units of the Broadband Transcontinental Network in units of 10 or 40 gigabytes per second. When you consider the fact that a large cloud data center contains a nontrivial fraction of the text holdings of the Library of Congress, you see the problem. There is a mismatch there in the ability to deliver versus the volume of data. So we need to accelerate construction.

What I was also advocating is we continue to need to advance the state of the art of the technology. How do we move beyond the current rates? How do we address in the spectrum areas some more nimble ways that would allow high bandwidth data sharing? We are going to have to change some of the standardization process, we need to invest in research, and we need to find the economic incentives that will drive the private sector to continue to build out those networks.

Chairman HALL. Thank you. I yield back my time, Mr. Chairman.

Chairman QUAYLE. I thank Chairman Hall for his questions.

The Chair now recognizes the gentleman from Illinois, Mr. Lipinski, for five minutes.

Mr. LIPINSKI. Thank you, Chairman Quayle. Thank you for holding this hearing today on this important issue. It is something I have been interested in for a while, even before the Administration announced their "cloud-first" policy, because I really think, as you talked about here today, that the cloud will have positive impacts on how the Federal Government researchers and the world will operate in the future. But I want to make sure that our implementation is done intelligently and we capitalize on the benefits while accurately assessing and mitigating the risks.

So the first question I have is probably best for Mr. Capellas, Mr. Combs, and Dr. Reed. What are the challenges to ensuring, first of all, the physical security of the servers and the security of the data stored in the cloud and how would you recommend we address these challenges? We need to gain the public's trust, but we also need to make sure that we do have adequate security in the cloud. I had a couple amendments on appropriations bills. I was just trying to address this issue. I have concerns, especially if we are talking about the, you know, obviously the Federal Government with our appropriations bills if we are going to go to cloud computing is where these servers are placed in other countries, perhaps, if there are any risks to that? But just more generally, what are the risks? How do we do all that we can to maintain both the—like I said, the physical security of the servers and also, then, the data security?

Mr. CAPELLAS. Okay. We are going to tag team this right down the row.

Mr. LIPINSKI. All right. Very good.

Mr. CAPELLAS. Very highly logical, we are simply going to go from right to left as we sit.

I will start off at kind of 100,000 feet. So the first one is the question of cybersecurity and I know there has been, you know, multiple testimonies which I diligently read last night. The problem is enormous. The threats are now extremely sophisticated. We are no longer thinking about, you know, the guy in the garage but, you know, some of the most advanced minds in computer science and engineering in terms of very systemic threats. So one, it is real.

The second is to realize that because we never built the original systems as they sit, don't think that by moving to another system or the cloud that it inherently says that what we have is fail proof because it is not. Every single security breaks at one point. The science of security says that you have data moving in three pieces in a system: one, data at rest where is it physically stored and is being used or the data is—think of it the data on your PC has records into it. The second one is called data in motion when the data is moving on a network, which is actually quite secure because we can analyze that network, we can see its patterns, we can see trends, we can analyze it.

The third one when it is in use by an application or server, in which case that server is under control. The real risk to security is data that is at rest when it is sitting there. The second big risk—and this will happen and a prediction will be is that we will have a major disruption to the Internet over the next 18 months is not particularly bold.

So the question is, when you think about a cloud, is it more or less secure? So the security answer says that you have to have an end-to-end view of how you think of all pieces with really the emphasis on how the data is sitting when it is at rest. And the second one is how do you mitigate interruption? A cloud by its definition says I am using resources. And as those resources are consumed, if I have a node or a computer that goes down, I can shift it to another one, isolate that node, and shut it down. You cannot do that in the convention.

So theory number one is the cloud itself, by being able to utilize different resources really mitigates the risk that you take your whole network down. Pretty simple answer. If I have got four people sharing the workload, I lose one, the other three pick it up. If I got one person doing the work and he gets hurt, I am dead. All right? So the theory of the cloud says allocation of resources. So properly designed, denial of service is less risk.

The second point, then, is data at rest. I can tell you right now having data centrally stored in a physical location under control of all of the analytical tools is much less risky than having data spread over many machines or PCs or small servers which are open to a network because it will always break. And you understand how attacks happen. You know, you probe the network to find the weakest link. Once you find the weakest link, you enter there.

So the basic premise I would have is we have an enormous problem, networks break at their weakest link and attack data at rest. The cloud, when properly designed, allows you to offset the denial of service by being able to distribute the workload and secondarily the central storage of data is in its essence far more reliable again when properly—and so I think the answer is how do we use the cloud to make it more secure, not less secure?

Dr. REED. So I think one of the things that is important to remember is that nothing in this world is absolute and it is all about assessing risks and benefits. And I think the cloud is no exception.

I think one corollary of that is we tend to equate through most of our lives location with security and that is a piece of the story, for sure, but it is by no means the only piece of the story. What it really means with any important asset—and clouds are no exception—is that one really thinks about a multifactor protection mechanism. There are certainly physical security issues that have analogs in our traditional approach to protecting things to physical security around a data center, the vetting of the people who manage and operate the data center for their reliability and trust. Then there is a whole set of best practices and operational mechanisms that one uses to manage that. And of course there are legal recourse that ultimately comes into play when there are data breaches.

There is a perpetual cat-and-mouse game in the computing business between the attackers and the protectors. And what that means is we have to continually advance the state of the art. And that means Microsoft—and I know I speak for my colleagues here—we are continuing to invest in advancing the state of that technology. But it is a nuanced and complicated issue.

I would suggest one concrete thing to consider which is an issue that the Cloud Commission Report mentioned explicitly and that is a need to revise some of our data breach laws because right now it is somewhat difficult to distinguish between the breach of an individual account and the possibility of breaches of many more of those. And they are fundamentally treated in very similar ways, and that means that it is very difficult to take sometimes the kind of concerted legal action between the private sector and government to deal with malicious behavior when it does occur.

But it is a multifactor problem. Like all things, there is no silver bullet. It is a vigilance and continuing to advance and multifactor approach.

Mr. COMBS. Thank you for your question.

I started my career 28 years ago at NSA working on encryption systems, so security is something I have always been critically interested in my entire career. Today—as I stated in my testimony, today's security architectures are—most of them are based around point security products. We have to move to a secure ecosystem. In any secure environment, you have the identities, those people and processes that you either want to give access to or deny access to your resources.

At the other end of the spectrum you have the data. That data must either be available or restricted, however an organization's security policies exist. In between those two environments, you still have the brick-and-mortar. You have the applications, the networks, the storage, the servers. We have to have a way of applying consistent security policy across the technology stack. That is what we have to do to implement security in the cloud.

And it is the secure ecosystem. It is moving the things in identities, right, the physical protection of the environment to a risk-based authentication. Why is an engineer going to the financial resources of a company? They shouldn't be going there. Look at the patterns of the users of the information and then you need to flag it or restrict access to it. Technology exists to do that today.

Data loss prevention capabilities, right, they can be rapidly—they are widely adapted in the commercial world. If you have ever had to put your—back to identification, if you ever had to put your ZIP code in the gas station, you are using adaptive authentication. It is widely deployed. You can use that within the government on your own policies to provide access.

And then restrict the information going out. The intelligence analyst, Bradley Manning in Iraq, right, had access, had the appropriate access to the environments and had appropriate right to go look at a cable, but there is no reason he should have downloaded 250,000 cables, right, to his CD-ROM. You can set policies around the data to prevent that. And in the absence of a policy, set a standard policy.

These capabilities exist and we look forward to working with the government to implement them.

Mr. LIPINSKI. Thank you.

Chairman QUAYLE. Thank you, Mr. Lipinski.

The Chair now recognizes the gentleman from Illinois, Mr. Hultgren, for five minutes.

Mr. HULTGREN. Thank you, Mr. Chairman. Thank you all for being here, too. I apologize. I have a couple of committees meeting at the same time so I am a little bit late here.

So I do know you have addressed some of my questions, but I would like to ask and get your thoughts on this. I know on Monday morning's Politico this week, the President of Information Technology Industry Council, Dean Garfield, was quoted, "There are certain things Congress can do to help cloud computing and there are certain things they should not do at all." I would just ask if you could talk a little bit more of what are the things we should be doing? And I think you have touched on that a little bit with Chairman Hall's question and also Congressman Lipinski's question but maybe even more focused. What shouldn't we be doing? I mean where could we actually do more harm than good, which I think can happen here sometimes. So I would just appreciate thoughts you might have on that.

Mr. CAPELLAS. So I think what Congress—I am not sure what I am—to tell you what you shouldn't do but I will try to be proactive on it. The first one foremost is I think that there is a policy around the acquisition and how dollars are spent relative to it. And those tend to come up with each agency measuring a single point of unit like I was talking about before, you know, one computer, one PC. So somehow relaxing where there could be more cost collaboration relative to how money is spent. For example, you take four agencies together and create one cloud that is secure and private is better than each one doing differently and recognizing that perhaps that investment will be done in a way that is different from the normal. And I can't tell you how many times we get involved with very meaningful projects that have ROI only to get caught up in the actual procurement.

I do want to acknowledge the work of the GSA, which has been extraordinary in terms of moving in a fast way, and I don't do that just because he is my colleague because it is very real.

The second one that I would say is—and there has not been very many references to NIST—standardization is the key. All right. Now, obviously this group is probably not going to sit around and determine, you know, what the technical standards of feeds and speeds are, but to continue the promotion of standards, there was one that we addressed on, you know, the cloud is so much about trust and that trust is the end user. And we make several recommendations about what policies can be done relative to trust won by other governments trusting so that we can have global clouds, and the second one was already referred to as—when we know we have a breach and it is done, both companies should be required to have transparency in what they report, but there has to be some teeth in the law that allows them to go after the people who are really the bad guys.

And so if I had to sort of summarize standards, acquisition policy, cross-border, and finally put some teeth into the laws that are required to enable that we have trust.

Mr. HULTGREN. Any others have thoughts of what we should be doing or, again, what we shouldn't be doing? And we need to hear from you what we shouldn't be doing and, you know, so I don't ever want you to feel like you can't tell us what we should stay away from because I think we need to hear that as well if there are places where we can meddle that I think we can cause more trouble.

Mr. CAPELLAS. Can I add one more?

Mr. HULTGREN. Absolutely.

Mr. CAPELLAS. I would also encourage you to read the report. Seventy-one companies, hours and hours of testimony, I have been doing this a long time like my colleagues. I have rarely seen people put their personal companies' interest aside and sort of come up with a report that is meaningful. Of course, I was the Co-Chair, so what am I going to say. But I do encourage you. It is an enormous amount of work by some of the brightest minds, and I do encourage you to read it.

Mr. HULTGREN. We will.

Dr. MCCLURE. If I can add as the government witness here, I think what you could really do to help tremendously is to tie this cloud agenda to improving the performance of government, saving money, improving service delivery. Those are the things that I think the American public really cares about. It is not about how many virtualized servers do we have sitting in data centers? I would agree with Michael the other push—the other two pushes are in the standards area, not the long-term decades-long standards approach but the more aggressive fast-paced approach that NIST is adopting in this area.

And the third thing is in a time when we are—we know we are under fiscal constraint and budgets are certainly going to be reduced, we must recognize that innovation still has to take place. And in many agencies, it is about allowing investment to actually get these capabilities in place. While it requires spending long-term, we are going to gain from it. So we can't lose sight of that either.

Dr. REED. I might add one last thing which is something I briefly mentioned in my opening remarks. In cloud computing, there is no doubt that the United States is the world leader right now. It is ours to lose in the future. And there is a major transformation taking place in the computing industry. It seems like they happen every other week, but this is a major, major one that will change lots of the ways that we think about not only the consumer side but the production side of computing. And so the first do-no-harm rule I absolutely believe because in these competitive times, it is important that we maintain that preeminence.

Mr. HULTGREN. Great. Thank you very much. My time has expired. I yield back. Thank you, Chairman.

Chairman QUAYLE. Thank you, Mr. Hultgren.

We will now move into the last round of questioning, and I will recognize myself.

And Mr. Combs, this is actually a good segue from the last question, but how does the fundamental architecture of cloud computing influence the type of standards that are necessary? And then also when do you think that the standards should actually be put into place so that it wouldn't actually thwart any sort of innovation within the cloud? Because that would be the—really the last thing that we need. And then maybe touch briefly on some of the standards within the cloud that could be harmful in terms of actually beings barriers to entry for trade. And so how would we deal with all of those to make sure that we are not affecting trade, affecting innovation, but still coming up with the proper standards so that the cloud can be what it can be?

Mr. COMBS. Well, one of the biggest problems, right, is interoperability and data portability around clouds. One of the concerns about the government is being able—is getting vendor lock-in, right? So one of the reasons that EMC is a full supporter of open-based standards, we think that any technology that is implemented into a cloud environment should be based on open architectures. How do you connect to storage in the cloud? Simple SOAP and REST protocols exist to be able to access data anywhere in the cloud. If you enforce those, you create innovation. Industry is going to bring this innovation. The government is not going to develop it. So—but enforcing the open standards and not getting into proprietary stacks is probably the best way to continue evolution.

I think Dr. McClure might be able to add a little bit there as well.

Dr. MCCLURE. You know, I agree, I think open architectures are absolutely key and I do believe that there are actually standard protocols that exist, SOAP, otherwise, that are easily workable into cloud environments. We have an enormous amount of work being done by NIST and industry partners to aggressively take a lot of existing standards and begin to move them into this environment rather than recreating whole new sets of standards, which is what we don't want to do to slow this down. So again, the aggressive approach that NIST is taking I think is the right way. Use case demonstrates standards viability and allow market solutions to adapt to them as fast as we can.

Chairman QUAYLE. Great, thank you. I now recognize Mr. Luján for five minutes.

Mr. LUJÁN. Thank you, Mr. Chairman.

Mr. Combs, even though it is your position that government won't develop the innovation, what happens if you don't have government as a client?

Mr. COMBS. What happens if we don't have government as a client? Well, I think——

Mr. LUJÁN. Will cloud computing advance and make the advances that we are seeing now, will we reap the full benefits of what this could potentially be sooner rather than later?

Mr. COMBS. Well, as I testified last year before the Government and Oversight Committee, if you put something out in the public cloud today, in my opinion, the risk is too high for sensitive government data to go there. I think we have proven it doesn't take a security or a cloud expert to pick up the Washington Post and see the number of companies that have been breached, right? So I think there is always going to be a market for the Federal Government to maintain the sensitive data within private clouds in their organizations. So I think there will always be a marketplace.

I think Microsoft has been very successful in standing up a private cloud to support the Federal Government, right? I think you will continue to see organizations stand up these capabilities to protect the sensitive nature of the data in the federal marketplace.

Mr. LUJÁN. So a federal client is critical to the development of cloud or the future of cloud or it is an important customer?

Mr. COMBS. I think it is an important customer to continue to evolve the security required to meet what is called multi-tenancy in cloud. I think it is very easy to have community clouds—we will say—give the Department of Defense——

Mr. LUJÁN. Um-hum.

Mr. COMBS. —and the intelligence community or civil agencies, the FBI, law enforcement community. It is very easy to set multi-tenant security boundaries around similar types of data. But what I want to put—do you think Coca-Cola and Pepsi is going to have their intellectual property on the same cloud? It is probably not going to happen. So there is just this sensitive data in the commercial world that exists as there is in the Federal Government.

Mr. LUJÁN. Absolutely.

Mr. COMBS. But the Federal Government will help drive the security around protecting information in the cloud.

Mr. LUJÁN. I appreciate that.

Dr. McClure, in your testimony you note that the continuation of GSA's cloud computing cost savings is dependent on fiscal year 2012 E–Gov Fund budget levels. Can you tell us what the fiscal year 2012 budget level request included for the E–Gov Fund and how that compares to funding levels currently proposed in the House and the Senate?

Dr. MCCLURE. Absolutely. And I am glad you are bringing it up. The E–Gov Fund has been the instrument by which the Federal Government over the last 3 fiscal years has fueled innovation like cloud computing. GSA has been the steward of a lot of monies and actually uses E–Gov funds to run the Cloud Computing Program Management Office, to produce the FedRAMP program and actually help and assist OMB in the data center consolidation analysis and produce things like the total cost model that the agencies are using now.

The requested funding in '12 was for $34 million. The House mark came in at 15.8 million, which is a little bit less than a half, 50 percent reduction in that fund, and the Senate mark came in at 7.4, which is only a fifth of the money. When anyone gets less money than being requested, something has got to give. So that is our challenge I think is we are trying to use this fund to fuel innovation, to do cross-agency government-wide work, not single-agency work. This is not GSA money. And if we reduce the funding levels down to those levels, you will have essentially what I could equate to as O&M work going on on existing projects rather than fueling new creative ways to save money for the government.

Mr. LUJÁN. I appreciate that, Dr. McClure.

And Mr. Chairman, I hope that is an area that we might be able to work together with colleagues on both sides of the aisle is if we talk about the importance of this, what it means to business, cost savings all around, and also the taxpayers that this is a place important for investment.

The last line of questioning that I have, and I may only get to hear one answer and I will submit it to all of you for a response—and maybe I will just start with you, Mr. Capellas, is you stated that the physical underlying infrastructure is not important necessarily to the consumer, and I can appreciate that from the end consumer, but from a security perspective, I have a question around that that I would suggest that we should care where the components are. And what I am getting to is, one, would there be anyone that disagrees that we have enough domestic real estate associated with data server facilities to house our data centers? And two, shouldn't we be looking to increase our capacity with domestic data centers on U.S. soil, especially as we talk about the security of U.S. information?

Mr. CAPELLAS. So the first one is the—I think what is important is that the user shouldn't have to know or care where it is——

Mr. LUJÁN. Um-hum.

Mr. CAPELLAS. —right? So that is—in terms of use——

Mr. LUJÁN. I appreciate that.

Mr. CAPELLAS. From a security point of view, do we have enough real estate? We certainly have plenty of real estate. The question that we have as we start to develop these clouds is we have to understand that there are going to be some workloads—and that is how the cloud starts to think about what tasks are you trying to do on a workload—where it is not going to be relevant to where the data resides. I simply—I want a browser that I want to look at some price catalog. And I think we have to be sensitive and take a leadership point of view around the globe and so it says some workloads are going to reside in different places and we need to be savvy enough to say that those different workloads are going to be in different places. Other workloads are going to be critical to our national security, and those workloads need to take place in secure ways and secure places we know. And I think it is to having the wisdom to know which goes in which place that where we can share it globally, where we must lead and have it locally, and to know the difference between the two, because if we get too rigid on either side, then I think that is when we start to break down and we create mistrust.

One of the things that the report does call out is we need to be cautious that if we get overly sensitive to not being able to want to have some global distribution that countries around the world will cease to have confidence in us, particularly relevant to some of the nature of some of the laws we have on the books today relevant to how data is viewed by law enforcement.

So I will summarize. It is—we have plenty of real estate. A little of what my colleague Dr. Reed said is it is ours to lose. We need to think about the workloads and be sensitive to where global workloads are fine but to make sure that for those workloads that we really care about, that we do take the leadership in the United States and drive it here.

Mr. LUJÁN. I appreciate it.

Thank you, Mr. Chairman.

Chairman QUAYLE. Thank you, Mr. Luján.

I would like to thank the witnesses for their valuable testimony and the Members for their questions. The Members of the Subcommittee may have additional questions for the witnesses, and we will ask you to respond to those in writing. The record will remain open for two weeks for additional comments and statements from Members. The witnesses are excused. Thank you all for coming. This hearing is now adjourned.

[Whereupon, at 11:15 a.m., the Subcommittee was adjourned.]

Appendix I

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Mr. Michael D. Capellas, Chairman and CEO,
Virtual Computing Environment Company

Questions submitted by Chairman Ben Quayle

Q1. What steps can the U.S. government take to make sure other governments don't implement cloud computing standards that advantage their own domestic industries and serve as barriers to free trade.

A1. The U.S. should examine its own policies to ensure that U.S. companies or companies with U.S. influence and/or jurisdiction are not subject to U.S. based policies that serve as a barrier to their own success. In general, the U.S. government should encourage free trade and adopt international security and privacy frameworks rather than creating a standalone U.S. framework that can be positioned against U.S. owned or partially owned industries. As an example, the Patriot is already being publicly targeted by EU entities to promote EU cloud computing offerings. At least one EU company has publicly discussed a cloud offering where they will guarantee that data will not reside in the US, enter into infrastructure owned by U.S. entities or be subject to U.S. government confiscation. The U.S. should seek to influence and adopt existing international frameworks rather than creating a distinct framework for the U.S.

Questions submitted by Representative Ben Luján

Q1. What does the federal government need to do to ensure the security and privacy of a person or organization's information is protected?

A1. The industry should develop a service catalog (or service catalogs) for various categories of information, using industry standard language and metrics. Where the information is permitted to reside is based upon the categorization of data, the level of secureness of the data, and the policies associated with the service providers in the host nations. Policies should not overly restrict data based upon location. It is more important to ensure appropriate data security measures (advanced encryption, etc.) are applied to sensitive data.

Q2. Why is strong identity management so important to accelerating the adoption of Cloud computing?

A2. In order for cloud computing to be successful and deliver the full benefits envisioned, it needs to be trusted and it needs to be secure. One of the most significant threats to infrastructure today is represented by identity theft, where hackers and evildoers gain access to information by pretending to be something they are not. In order to minimize the threat of identity theft, whether it be person or machine credentials, strong authentication and access controls are required. Measures like dual factor authentication can ensure that a user of entity is who they say they are, and that they have access rights to the information they are trying to access.

Questions submitted by Representative Randy Neugebauer

Q1. What is the industry doing to establish best practices to protect and secure users' data and privacy rights? If standards are adopted how can we give them enough flexibility to allow the industry to evolve?

A1. The industry recognizes the potential for cloud computing to provide a more secure and easily protected model for computing than what exists today. Security threats are constantly evolving and as a result, the state of the art in security also evolve rapidly. The government should allow the market to evolve and advance security measures with minimal involvement. Government should refrain from imposing any security requirements on industry, recognizing that not all data has strict security requirements. The government should focus efforts on being aggressive in requiring industry to both report on their security provisions and, more importantly, to quickly disclose any security breaches. Having to disclose security breaches is the best way to protect other users, encourage providers to adopt the best security they can, and compete in the market based upon track record.

Q2. How quickly have industries and businesses converted to cloud services? What factors might be inhibiting large scale moves away from traditional IT services to cloud services?

A2. Industry is moving very quickly to cloud, and the march is inevitable. Barriers are largely centered around organizational inertia and internal turf resistance. Cloud computing requires transformation of technology, people and processes. While transformation presents immense opportunity, it can also be perceived as a threat by those who resist change of any kind. In many cases, running a vastly more efficient and responsive IT organization means having less headcount and less budget and is therefore seen as a step backward in authority or standing. As cloud gains more traction, organizations that are slow to move to cloud will be at a competitive disadvantage, and this will serve to dissolve existing barriers.

Responses by Dr. Daniel A. Reed, Corporate Vice President,
Microsoft Corporation's Technology Policy Group

Questions submitted by Chairman Ben Quayle

Q1. What steps can the U.S. Government take internationally to ensure that other countries do not implement cloud computing standards that advantage their own domestic industries and serve as barriers to free trade?

A1. There are two important things that the U.S. government can continue to do internationally to ensure that other countries do not implement cloud computing standards that advantage their own domestic industries and serve as barriers to free trade. First, the U.S. government can monitor other nations' promulgation of national standards and other technical measures and, via the U.S. Trade Representative, can express concerns if such standards appear to violate World Trade Organization rules or to be designed to benefit unfairly a nation's indigenous industries. The second, related, step the U.S. government can take is to lead by example. The government can, when considering its use of cloud services and associated standards, engage in the sort of behavior that it hopes to see in other nations. This includes recognizing the diversity of data and services that could move to the cloud and deploying standards and requirements in ways that allow federal agencies to access a variety of options to meet the performance, security, and other needs of specific deployments. This can be complemented by U.S. companies' participation in international activities related to standards and best practices, with the support of government expertise such as from the National Institute of Standards and Technology.

Q2. It is important to let new business models like cloud computing flourish, yet at the same we cannot allow unscrupulous actors to use new technologies for infringement. Do you believe that Congress should act in this area to address criminal and infringing behavior as applied to cloud computing? If so, what steps would actions would you recommend?

A2. Cloud computing is a major technology inflection point with far-reaching effects on the capabilities and empowerment of businesses, governments, scientists, and individuals, and significant economic and competitive benefits for the U.S. In addition, some individuals with the intent to defraud or infringe will seek to exploit the cloud. As new concerns with new forms of infringement arise, Microsoft believes that Congress should respond not by focusing on any specific technology (such as cloud computing) but rather by examining whether existing laws are adequate to address evolving forms of infringing behavior. Similarly, for criminal behavior related to cloud computing, the focus should be on examining evolving forms of attacks on computer systems and networks, including cloud computing services, and updating and strengthening criminal laws against those responsible, as noted in the CLOUD^2 Commission report, Recommendation 3.

Q3. In your response to Mr. Hultgren's question about which actions the government should not be taking in the cloud computing enterprise, you stated that you believe in the "first do-no-harm rule." Can you provide examples of government cloud computing actions that could potentially be harmful? Are there any specific principles government should follow when determining whether action is appropriate?

A3. Some of the policy challenges created by the cloud relate to the exponential rate of change we are seeing in our technological capabilities. This pace can conflict with the pace at which government and society can evaluate the implications of the deployment of these new technologies. The best approach in such times is to establish policy goals and a flexible framework for achieving them, and to avoid focus on specific technological approaches that could chill innovation or quickly become outmoded.

A specific example of flexibility that the U.S. government should embrace related to cloud computing can be seen in the above answer to Rep. Quayle's first question. Imposing overly constraining requirements or standards around all possible U.S. government uses of cloud could have a chilling effect on other nations' openness to cloud deployment, while nuanced approaches by the U.S. that recognize the different needs of various types of cloud applications would set a positive example for others.

Questions submitted by Representative Ben Luján

Q1. Security and privacy are often cited as concerns for cloud computing. Specifically, there is concern about the transnational flow of data and the possibility that confidential or proprietary information might be hosted in a data center located in a foreign country. What does the federal government need to do to ensure that the security and privacy of an individual or organization's information is protected?

A1. Security is a multifactor challenge. The physical location of a data center (and the steps taken to provide security for its physical plant) is only one component of many that help control access to data. Individuals and organizations need to understand the nature of the various types of data they handle and what their expectations are for its access and control before developing requirements for where it will be stored and processed. Decisions about the geolocation of data will have implications not only in terms of security, but also in terms of efficiency, redundancy, cost, and resiliency.

One potential role for the federal government in this space is to lead by example. Agencies can, when evaluating their potential use of cloud services, recognize the different types of data they holds and deploy targeted security and privacy requirements for different classes of information and applications. The government can also, in assessing security, recognize that it is critical to focus on how data is secured—i.e., are there adequate processes in place to protect the data against an evolving threat landscape. In the context of this evolving landscape, it can also continue to support basic research in cybersecurity, as new defenses and approaches will be needed in the future.

Questions submitted by Representative Randy Neugebauer

Q1. What is the industry doing to collaborate or establish best practices that will ensure that users' data will be secure in the cloud and privacy rights will be protected? Are there any areas which require Congressional direction to ensure a high level of safety in this regard? If standards are adopted, how can we ensure that they give enough flexibility to allow the industry and the technology to evolve?

A1. Microsoft and other companies are engaged in a variety of activities related to best practices around security and privacy. One example, in which Microsoft is a participant, is the Software Assurance Forum for Excellence in Code (SAFECode), a global, industry-led effort to identify and promote best practices for delivering more secure and reliable software, hardware, and services. Another is the privacy, confidentiality, and compliance framework for data governance that Microsoft has developed and publicly released so it can be adopted and implemented by organizations of all sizes.

In thinking about Congressional action, it is important to recognize that consumer expectations regarding online privacy are continually evolving as the technology evolves. For this reason, and to allow companies the flexibility to innovate, Congress needs to be very careful when considering legislation related to privacy and security. However, there are two areas with regard to online privacy where Microsoft has supported the idea of federal legislation. One is a comprehensive federal privacy law; and more information on Microsoft's view on the policy context for such a law is at http://go.microsoft.com/?linkid=9768689. The second is the updating of the 25-year-old Electronic Communications Privacy Act to maintain a balance between the privacy expectations of users and the needs of law enforcement in a way that reflects how people use information technology, including the cloud, today. In this area, Microsoft is a member of the Digital Due Process Coalition (http://digitaldueprocess.org/).

Q2. In a broad sense, how quickly have industries and businesses converted to cloud computing services? What factors, if any, might be inhibiting large scale departure from traditionally internal IT services to cloud computing services to save on overhead costs?

A2. Many industries and businesses have embraced cloud services. A particular niche that innately appreciates the value of cloud is start-up technology businesses, which value the inherent flexibility of cloud—the ability to scale up or down their information technology resources depending on demand or current business phase, and the ability to shift expenses from up-front costs to purchase information technology hardware to pay-as-you-go-only-for-what-you-use models. In general, many industries and government are moving forward with cloud services. In some cases, they are replacing existing information technology systems with capabilities that are similar but are deployed using the cloud (e.g. email). In other cases, they are exploring how cloud actually will provide new capabilities and opportunities, e.g. for global, multi-party and neutral collaborations, or for flexible and rapid exploration of new products and services by existing businesses. While these latter applications may be emerging more slowly, they will have a significant impact on many sectors and on our economy as a whole.

Responses by Mr. Nick Combs, Federal Chief Technology Officer, EMC Corporation

Questions submitted by Chairman Ben Quayle

Q1. What steps can the U.S. Government take internationally to ensure that other countries do not implement cloud computing standards that advantage their own domestic industries and serve as barriers to free trade?

A1. It is important for the U.S. Government to advocate for alignment of cloud computing standards (in areas such as interoperability, mobility and security) that align with current and evolving global industry standards. The U.S. Government should also push back on countries that try to impose domestic or indigenous standards in bi-lateral and multi-lateral trade negotiations. For example, there are efforts by some countries to advance specific information security or encryption requirements that could deter the adoption of cloud computing infrastructure and services provided by multi-national corporations in those markets. In addition, it is important for the U.S. government and other governments internationally to resist mandates or laws that would require a specific cloud deployment model. The U.S. Trade Representatives and the U.S. Department of Commerce can continue to play important roles in advancing effective policies in these areas internationally.

Questions submitted by Representative Ben Luján

Q1. Security and privacy are often cited as concerns for cloud computing. Specifically, there is concern about the transnational flow of data and the possibility that confidential or proprietary information might be hosted in a data center located in a foreign country. What does the federal government need to do to ensure that the security and privacy of an individual or organization's information is protected?

A1. When implemented correctly, cloud environments can be much more secure than today's IT environments. The level of transparency cloud vendors provide is a critical aspect when choosing a cloud partner. Via the regular procurement and contractual process, U.S. federal agencies should 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 dashboards provided to the customer to ensure that our information is protected and the policies are being followed.

Questions submitted by Representative Randy Neugebauer

Q1. What is the industry doing to collaborate or establish best practices that will ensure that users' data will be secure in the cloud and privacy rights will be protected? Are there any areas which require Congressional direction to ensure a high level of safety in this regard? If standards are adopted, how can we ensure that they give enough flexibility to allow the industry and the technology to evolve?

A1. Best practices such as risk-based authentication should also be implemented in cloud environments and we think that that approach fits well within the President's National Strategy for Trusted Identities in Cyberspace (NSTIC) which was released earlier this year. This important effort, which is being coordinated by the NSTIC Office at NIST in collaboration with the private sector, should be supported by the U.S. Congress.

NIST has played an instrumental role in the development of the Authorization Management Program (FedRAMP) and NIST Security Content Automation Protocol (SCAP). FedRAMP is a voluntary, General Services Administration (GSA)-led initiative to develop and provide a standard approach to assessing and authorizing cloud computing services and products for use by Federal agencies. The NIST SCAP standard enables the automation of reporting and verifying IT security controls. SCAP provides an effective method to capture, test and continuously monitor these controls.

Both of these initiatives are important steps in the transition of the Federal Government from the old FISMA focus on compliance, to better operational risk management and continuous monitoring under the new FISMA. This process is critical for improving cyber security today as well as positioning the federal government to fully utilize the transition to the cloud to help improve cyber security. Congress should update FISMA.

Congress should reduce the regulatory complexity that businesses and critical infrastructure organizations have to deal with complying with myriad state data breach disclosure laws in the U.S. In an advanced threat environment, it does not make sense to have organizations devoting their resources and focus to complying with 46 separate state laws on breach notification when they need to invest more time and resources in managing operational cyber security risks. Simplifying the compliance requirements with a reasonable and uniform federal standard (with preemption of the existing state laws) would allow security organizations to focus more on risk management.

Q2. In a broad sense, how quickly have industries and business converted to cloud computing services? What factors, if any, might be inhibiting large scale departure from traditionally internal IT services to cloud computing serves to save on overhead costs?

A2. A shift to cloud computing is a journey that occurs in phases. EMC's own journey to the cloud has provided significant savings and efficiency. In both industry and government, we are seeing data center consolidation move forward—with the associated cost savings—in tandem with organization' transition to cloud infrastructure and services.

Responses by Dr. David L. McClure, Ph.D., Associate Administrator, Office of Citizen Services and Innovative Technologies, General Services Administration

Questions submitted by Chairman Ben Quayle

Q1. What steps can the U.S. Government take internationally to ensure that other countries do not implement cloud computing standards that advantage their own domestic industries and serve as barriers to free trade?

A1. The National Institute of Standards and Technology (NIST) has the lead federal role in standards setting. NIST is actively encouraging the establishment of international, consensus based standards, which is one of the primary recommendations of the recently published NIST Cloud Computing Roadmap. In fact, the NIST definition of cloud computing was the U.S. contribution to the International Committee for Information Technology Standards (INCITS). International standards are critical to avoid development of country specific standards that may create barriers to trade. The broad adoption of international standards ensures a level playing field and fair trading conditions for all products and services, both in the U.S. and overseas.

In addition, the Department of Commerce, Department of State, and other Federal agencies are working on policies that will ensure that differences between the U.S. approach to data privacy and security, and those of our international partners, do not become barriers to the global free flow of information. This approach involves the development of domestic policy recommendations and engagement with industry and our trading partners.

Questions submitted by Representative Ben Luján

Q1. Security and privacy are often cited as concerns for cloud computing. Specifically, there is concern about the transnational flow of data and the possibility that confidential or Proprietary information might be hosted in a data center located in a foreign country. What does the federal government need to do to ensure that the security and privacy of an individual or organization's information is protected?

A1. The Federal Risk and Authorization Management Program (FedRAMP) has been established to provide a standard approach to Assessing and Authorizing (A&A) cloud computing services and products. Leveraging a common security approach and baseline will not only allow for greater efficiency, but will ensure the entire Federal Government and Cloud Service Providers are working together to ensure government and citizen information stored in the cloud is protected and privacy concerns are addressed. Government contracts for cloud computing services and solutions require compliance with the Federal Information Security Management Act of 2002 (FISMA). FISMA establishes a strict set of legal requirements for information security that apply to all federal information systems, including those implemented through cloud computing. These requirements and guidelines apply regardless of where data is stored. It is essential that federal acquisition professionals and contracting officers be knowledgeable in the latest requirements and take advantage of common contract language that is helpful to address key issues specific to cloud computing solutions.

With respect to privacy, the Federal CIO recently released the FedRAMP Memorandum, which indicates that the CIO Council will "publish the standardized baseline of security controls, privacy controls, and controls selected for continuous monitoring" from NIST SP 800–53. See Memorandum for Chief Information Officers, Security Authorization of Information Systems in Cloud Computing Environments, Dec. 8, 2011, p 5. The controls at issue are based on existing Federal privacy law. Under this provision, Federal agencies should take steps to ensure that they consider and implement the appropriate controls before releasing sensitive or personal information into a cloud solution. The Memorandum also requires previously deployed solutions to meet these requirements within a fixed period of time, which should mitigate the risks you identified.

Questions submitted by Representative Randy Neugebauer

Q1. What is the industry doing to collaborate or establish best practices that will ensure that users' data will be secure in the cloud and privacy rights will be protected? Are there any areas which require Congressional direction to ensure a high level of safety in this regard? If standards are adopted, how can we ensure *that they give enough flexibility to allow the industry and the technology to evolve?*

A1. Cloud policies and standards are being developed in collaboration with industry and other stakeholders to ensure acceptable balance of risks and benefits of cloud computing. Congress should continue to encourage cloud adoption by ensuring sufficient resources are invested in programs such as FedRAMP and Cyberscope. The Cloud Security Alliance works with industry and governments across the world regarding best practices for cloud security. Their mission statement is: To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.

Q2. In a broad sense, how quickly have industries and businesses converted to cloud computing services? What factors, if any, might be inhibiting large scale departure from Traditionally internal IT services to cloud computing services to save on overhead costs?

A8. Data collected on both industry and public sector movement to cloud solution indicates steady, pervasive interest and broad adoption as an inevitable technology market direction. Key barriers and mitigations are shown in the table below.

Risks	Mitigation Strategies
Security	▪ Standardized C&A Process - FedRAMP ▪ Ongoing monitoring ▪ Match security level of cloud computing implementation to security risk level • Data separation
Data Ownership	▪ Implement policy to establish agency ownership ▪ Enforce policy
Records Management	▪ Records disposition in place across categories of records ▪ Refine e-discovery and forensic processes and policies
Performance	▪ Define specific internal requirements prior to acquisition ▪ Clear contractual requirements and validation of vendor capability prior to acquisition ▪ Define performance metrics, SLAs and monitoring methods
Change Management	▪ Secure buy-in of management ▪ Educate personnel on advantages, risks and mitigations of cloud implementation ▪ Start with pilot activities, keep activities feasible ▪ Use modular approach
Privacy	▪ Conduct Privacy Impact Assessment (PIA) ▪ Ensure Privacy Act System of Record Notice, (SOR), exists where applicable ▪ Ensure provider compliance (disclosures, subpoena, data deletion, etc.) ▪ Ensure accountability measures are in place for the service provider. ▪ Clear and distinct policies of Personal Identifiable Information, (PII), usage, storage, transmission and manipulation. ▪ Apply NIST Guidance – Special Publication 800-53 Appendix J Draft Privacy Control Catalog

Appendix II

Additional Materials Submitted for the Record

MATERIAL SUBMITTED BY REPRESENTATIVE BEN R. LUJÁN

TechAmerica
FOUNDATION

Cloud First, Cloud Fast: Recommendations for Innovation, Leadership and Job Creation

A Report from the Commission on the Leadership
Opportunity in U.S. Deployment of the Cloud (CLOUD^2)*

*Pre-publication copy – subject to minor technical corrections. Final printed version available Aug 2, 2011 at www.techamericafoundation.org/cloud2.

CLOUD^2 COMMISSION REPORT

FOREWORD

Cloud technologies are transforming the way computing power is bought, sold and delivered. Rather than purchasing licenses or hardware, users may now obtain computing power as a service, buying only as much as they need, and only when they need it. This new business model brings vast efficiency and cost advantages to government agencies, individuals, and companies of all sizes. The numerous benefits of cloud computing have already won over many adopters and are generating significant cost savings, efficiencies, flexibility, innovation, and new market opportunities.

This report reflects the growing imperative to fully embrace and capitalize upon the power of cloud computing. The Commission on the Leadership Opportunity in U.S. Deployment of the Cloud (CLOUD^2) developed the report at the encouragement of the Federal Chief Information Officer and the U.S. Department of Commerce. The Commission's mandate was to generate recommendations for accelerating adoption of cloud technologies in the U.S. government and in the commercial space and to identify public policies that will help foster U.S. innovation and leadership in cloud computing.

The Commission was composed of representatives from 71 companies and organizations, including cloud providers, cloud users, and other businesses that are involved in enabling cloud deployment. To build on this diverse set of expertise and perspectives, the Commissioners interviewed numerous government representatives, heard presentations from a variety of organizations, and analyzed relevant past reports.

Actionable Recommendations — Trust, Transnational Data Flows, Transparency and Transformation

Moving to cloud computing is a change that involves people, policies, processes, and technology. The Commission identified barriers that have kept some government agencies from moving to the cloud and recommended actionable solutions to overcome these. In addition, the Commission identified barriers to commercial deployment of cloud services and recommended actions to eliminate them. Since government, industry and academia share the responsibility to accelerate adoption and drive U.S. innovation and leadership, the recommendations reflect actions for all three key stakeholders. Industry, as represented by the Commission members, is committed to enabling the transition to the cloud by companies and government agencies and accepts the responsibility for taking actions that enable cloud adoption.

In this report, the Commission has focused on 14 specific recommendations, categorized into four thematic areas: Trust, Transnational Data Flows, Transparency, and Transformation. For each recommendation, the report identifies why the action is needed, how it should be implemented, who should implement it, and what benefits should be expected from implementation. The Commission intentionally made these recommendations direct and prescriptive.

The four areas are briefly discussed below.

Trust

Users of cloud computing want assurance that when using cloud services, their workloads and data will be treated with the highest integrity and their security, privacy, and availability needs will be met. To enable trust and confidence in cloud services, the Commission recommends that government and industry develop common frameworks, best practices and metrics around security and information assurance to assist users in choosing and deploying the security level most appropriate for their workloads. The Commission also recommends strengthening the identity management ecosystem and data breach laws, as well as supporting increased research on cloud computing as an investment in future cloud innovation.

Transnational Data Flows

In a global economy, it is common for businesses to operate in multiple countries and for cloud providers and users to work and transfer information across national borders. This adds complexity to cloud adoption because of the data, processes, and people residing on multiple continents with different laws and cultures. In this context, the Commission recommends that industry and the U.S. government promote privacy frameworks, that the U.S. government identify and implement mechanisms to clarify processes and mechanisms around lawful government access to data, and that the U.S. continue international discussions in these areas. We also recommend that the U.S. government lead by example by demonstrating its willingness to trust cloud computing environments in other countries for appropriate government workloads.

Transparency

Users want an abundance of information about the cloud services they buy and unfettered access to the data and processes they entrust to the service provider. To meet these needs, cloud providers must be open and transparent regarding the characteristics and operations of the services they provide. Government and industry should collaboratively develop metrics that facilitate this information sharing and customers' ability to compare cloud offerings. Additionally, to ensure that data is available to customers should they wish to change cloud services, cloud providers should enable portability through industry standards and best practices.

Transformation

The transition to cloud computing is placing new requirements on purchasing processes, infrastructure, and people's skills. For government agencies, the fact that buying cloud computing services can be fundamentally different from buying in-house IT systems poses a challenge. Therefore, agencies, the Office of Management and Budget (OMB), and Congress must demonstrate more flexibility around budgeting and acquisition processes. Such flexibility, in combination with OMB incentives for moving to the cloud, will increase the rate of adoption by government agencies. Additionally, to accommodate the bandwidth and reliable connectivity necessary for the growth of cloud computing, the nation's currently stretched and aging IT broadband infrastructure should be updated, in conjunction with embracing IPv6. To help acquisition and IT personnel understand and carry out the transition to cloud, government agencies, companies, and academia should develop and disseminate appropriate educational resources.

In addition to the recommendations in the body of the report, the Commission also produced a *Cloud Buyer's Guide*. The guide walks potential government buyers through questions to ask and steps to take prior to purchasing a cloud computing solution. Designed to be a living document, the guide is available online at http://www.cloudbuyersguide.org/. As cloud technology evolves, this online resource can be easily updated with new frequently asked questions (FAQs) and guidance.

By providing clear, actionable recommendations, the Commission hopes to help accelerate the deployment of cloud computing at companies and government agencies. Cloud's widespread adoption will drive increased efficiencies and job growth and continue to position the United States as a technology leader in a global marketplace.

Introduction/Purpose of Report

For more than 50 years, the United States has taken advantage of new developments in Information Technology (IT). U.S. companies and government agencies were early adopters of the mainframe computer, the minicomputer, the personal computer, and the World Wide Web. We are now entering a new phase in the history of computing that will be at least as transformative as the mainframe or the Web and provide at least as much benefit to all Americans. Cloud computing represents a powerful new way to provide computing power and storage—and it will unleash huge new opportunities for companies and citizens able to harness it.

Cloud computing[1] is based on a simple idea. By allowing computer users to tap into servers and storage systems scattered around the country and around the world—and tied together by the Internet—cloud service providers can give users better, more reliable, more affordable, and more flexible access to the IT infrastructure they need to run their businesses, organize their personal lives, or obtain services ranging from entertainment to education, e-government, and healthcare. Most Americans already use cloud computing in one form or another to do email or back up the files on their laptop or smartphone. Most social networking sites and thousands of e-commerce sites (large and small) are running in the cloud. Cloud computing is not a technology of the future; it is already being used for business and government applications worldwide.

On the other hand, cloud computing does represent a fundamental shift in how computing is accomplished. The cloud is not only a new way to more easily and cheaply get the computing power needed to do what companies and individuals are doing today; the cloud, like the Web, will also generate new business models and drive companies to reorganize and change the way they go to market, team with partners, and serve their customers. It will enable companies (and governments) to move faster and be more responsive and flexible.

Companies will be able to try several prototypes at once, test their limits, and then build and deploy new, better prototypes—all within a few weeks. This may be the most important benefit of the cloud—it enables companies of all sizes and in all sectors, as well as governments, non-profits, and individuals, to more quickly build new applications and services by reducing the cost and complexity of deploying and managing IT resources. However, that requires cloud providers to make services simple and easy to use and deploy, and it requires that cloud customers make the effort to understand the new capabilities clouds can provide.

[1] The National Institute of Standards and Technology, in consultation with industry and government, has drafted a definition of cloud, including descriptions of the essential characteristics, service models, and deployment models. See http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf.

Most companies and organizations spend the vast majority of their IT budget just maintaining their current infrastructures and the applications that run on them. The cloud will enable them to devote more resources and talent to creating new products and services and improving productivity.

This democratization of innovation is a huge opportunity for people, organizations, and countries around the world. To maintain its competitive position, the United States must focus on quickly and effectively harnessing the full power of cloud computing, leading in both the deployment of cloud and the development of new cloud services. This will help American companies generate high-paying jobs and compete in the global marketplace.

Whether the United States will benefit as much from this new phase in the evolution of computing as it did from the mainframe and the Web depends upon many factors. Will the iconic U.S. companies that have pioneered and promoted the cloud continue to lead in the development of cloud services? Will companies embrace cloud computing and take advantage of the capabilities it provides? Will the public sector be able to move to the cloud? Will individuals be comfortable with their data and software located in the cloud rather than on a device in their hand? Will government policies—both in the United States and abroad—facilitate deployment of and innovation in cloud services? We firmly believe that the answer to all these questions can and should be an unequivocal YES.

We are convinced that cloud computing is developing extremely rapidly, much like the Web did in the 1990s, and will have a major impact on computing and the economy. How cloud computing develops will be shaped by key choices and policy decisions that will be made over the next two or three years. It is critical that industry and government work together to make the right choices.

In some cases, the U.S. government may choose NOT to take action and allow market forces to guide the evolution of the digital economy. U.S. national policies that conflict with those of other countries, even if designed to achieve worthy goals like security or consumer protection, could end up constraining how the cloud develops or discouraging investment in new cloud services and applications.

The most effective way for governments to shape the evolution of the cloud is not through law and regulation but by being smart users of the technology. This is particularly true in the area of security, where some government agencies have especially challenging requirements. As agencies work with industry to ensure that the cloud services deployed are at least as secure and trusted as the IT systems in use today, the agencies can provide a model that cloud customers in governments and corporations around the world can emulate.

This report provides recommendations for government, including the White House and key Federal agencies, on how they, in cooperation with industry, academia, and other nations, can (1) adopt policies that will foster development and growth of the cloud and (2) deploy the cloud effectively, making government work better, cheaper, and smarter. These recommendations cover a lot of territory but focus on four areas: Trust, Transnational Data Flows, Transparency, and Transformation. Responsibility for success also lies with cloud providers, and the Commission makes specific recommendations to providers throughout the report. The report also includes a "Buyer's Guide" that advises Federal agencies on how to accelerate adoption of cloud services.

TRUST

The first step in accelerating the adoption of the cloud and driving U.S. leadership in cloud innovation is earning the trust of current and potential cloud users. Trust in the cloud is a result of a combination of factors that enable individuals and organizations consuming cloud services to be confident that the services are meeting their computing needs. These needs include security, privacy, and availability; the factors that contribute include transparency of practices, accountability, resiliency and redundancy, access and connectivity, supply chain provenance, life cycle integrity, and governance.

Cloud computing is the natural evolution of IT, and it will continue to evolve. Similarly, enabling trust in the cloud is an evolution—trust is not a static state, and cloud services are not static deployments. As cloud computing evolves, one element that will enable trust is the monitoring of characteristics that impact the quality of cloud service delivery and continuity. Monitoring can expose what is happening in a cloud deployment, and, coupled with systems for analysis, improvement, and accountability, can help enable trust in the functioning and security of the cloud.

Risk management is an important element of enabling trust because it is integral to the process of monitoring and accelerating cloud adoption and implementation in the short term. Risk management capabilities need improvement for enterprises adopting cloud services, for communications providers connecting cloud services to people, for cloud service providers, and for application providers. Areas relevant to the cloud include review of current and emerging standards, industry best practices, understanding risk simultaneously at a system level and asset level, risk transfer in cyberspace, methods for assessing and meeting security needs of data whose sensitivity varies over time, and mitigation of abuse of cloud assets.

This Commission believes that trust is a ubiquitous concept, central to cloud adoption and U.S. leadership. Enabling trust, as with all of the recommendations, is an incremental process and should not become a reason to resist moving to the cloud. The Commission recognizes that enabling trust is a pillar of cloud adoption and notes that recommendations in subsequent sections of this report also support enabling trust in the cloud.

In recent months, senior U.S. officials have described threats such as cyber crime and state-sponsored industrial espionage as outpacing many enterprise defenses. In this evolving cyber threat environment, the commission believes that cloud security services and solutions, if done correctly, may provide improved security relative to non-cloud environments.

Recommendation 1 (Security & Assurance Frameworks): Government and industry should support and participate in the development and implementation of international, standardized frameworks for securing, assessing, certifying and accrediting cloud solutions.

The Commission recommends that cloud-computing service providers collaborate with the National Institute of Standards and Technology (NIST), relevant associations and standards bodies to assess and evolve current best practices and standards, to strengthen cloud security metrics, and to facilitate information sharing.

***Best Practices and Standards*:** Collaboration on best practices and standards should focus on identifying and addressing gaps in relevant domestic and international best practices and existing standards related to security, privacy, transparency, and accountability with respect to delivering trusted cloud computing services. The best practices and standards should be assessed in the context of the industry segments served by their respective provider types.[2]

In order to implement applicable best practices and standards around security and information assurance, the Commission supports the efforts underway on programs such as the Federal Risk and Authorization Management Program (FedRAMP) and NIST Security Content Automation Protocol (SCAP).

FedRAMP is a voluntary, General Services Administration (GSA) led initiative to develop and provide a standard approach to assessing and authorizing cloud computing services and products for use by Federal agencies. The Commission believes that a well-defined FedRAMP framework will help accelerate the adoption of cloud in the Federal Government. The NIST SCAP is a standard that enables the automation of reporting and verifying IT security control parameters. SCAP provides a ready method to capture, test and continuously monitor the controls and integrity settings required to achieve the respective standard and/or compliance requirements.

***Metrics*:** The Commission believes that cloud-related security metrics are critical for establishing a basis for trust in the cloud and recommends that industry collaborative efforts also address security measurement frameworks. Security measurement frameworks should include relevant security metrics that will allow potential customers to compare and select appropriate security levels for their cloud services. For example, a standard set of risk-based performance measures weighted and tailored for relevance to needs and matters of importance to each customer would enable potential customers to determine the appropriate security levels for their workload and data.

[2] Examples include the International Standards Organization (ISO 27001/27002), NIST (SP-800-53), and the Payment Card Industry Security Standards Council (PCI DSS)

Security metrics efforts should build upon industry and academia initiatives already chartered to address standard cloud performance measurement frameworks. Examples of such initiatives include the Carnegie Mellon University Cloud Service Measurement Initiative Consortium (CSMIC), the Distributed Management Task Force's (DMTF) Cloud Management Working Group, and the Cloud Security Alliance (CSA). This is also an opportunity to build on similar efforts of government agencies to develop standards, best practices, and key performance indicators (KPIs), such as in the work underway at NIST, the National Security Agency (NSA), GSA, and the Federal CIO Council.

To foster the development of measures and metrics, these collaborative efforts should also promote educational and research programs around cloud security. These types of frameworks and tailored criteria will allow public sector organizations to develop specifications pertinent to government and help formulate procurement guidance for cloud services.

By establishing and adopting standardized frameworks for securing, assessing, certifying, and accrediting cloud systems, cloud providers can deliver a higher level of transparency and trust to consumers. Transparency of real-time status and performance metrics associated with the confidentiality, integrity, and availability of cloud systems will further contribute to enhanced trust and confidence in secure cloud services.

Information Sharing: As the cloud is deployed by federal agencies and businesses in multiple sectors, cloud-related security issues will become an important element of the overall security discussion for those communities. The Commission therefore recommends that cloud expertise be integrated into existing information-sharing structures, such as the Information Sharing and Analysis Centers (ISACs) and the Sector Coordinating Councils.

Recommendation 2 (Identity Management): Industry and government should accelerate the development of a private sector-led identity management ecosystem as envisioned by the National Strategy for Trusted Identities in Cyberspace (NSTIC) to facilitate the adoption of strong authentication technologies and enable users to gain secure access to cloud services and websites.

Mechanisms to provide identity, authentication, and attribution in cyberspace are essential to accelerating adoption of cloud computing services and improving trust in the cloud. (For example, identity management facilitates access verification, billing, law enforcement access, and other features and capabilities.) Two characteristics of a robust identity management ecosystem are (1) enabling higher level transactions to occur electronically and (2) enabling credentials to be utilized across multiple services and websites. For the cloud, these have two benefits. First, a more robust authentication system would facilitate the transition of a wider variety of workloads and interactions to cloud services. Second, multi-use credentials would facilitate interoperability and allow customers to assemble the systems most appropriate for their workloads. In this case, a community of identity management systems will enable seamless transitions when data, processing tasks, and other applications reside on different platforms at different service providers with different access control requirements, or when cloud services have to integrate with traditional IT systems.

The need for identity management capabilities is not new or unique to the cloud, and there is an opportunity to build on existing initiatives and innovation underway in this area. The National Strategy for Trusted Identities in Cyberspace (NSTIC, http://www.nstic.us/), released in April 2011, is aimed at developing a broad, private-sector led, identity management ecosystem that enables the identification and authentication of the individuals, organizations, and underlying infrastructure involved in an online transaction. The Commission endorses NSTIC's goal of facilitating creation and broad deployment of identity capabilities, and the adoption of cloud services by business and government will provide additional opportunities and motivation for development of this identity ecosystem.

In addition to supporting the development of a private-sector led identity management ecosystem, the Commission also suggests specific steps that the Federal Government could take as a user of cloud services that would contribute to advancing robust identity management:

- Deploy, as appropriate, multi-factor authentication for Federal cloud applications as used by Federal personnel and government contractors doing government contract work
- Accelerate the adoption of strong authentication, including multi-factor authentication and one time passwords, to enable mobile access to secure Federal cloud services and websites

These actions are important because implementation of strong authentication will increase resilience of the cloud ecosystems. The Commission notes that the adoption of cloud technologies in the Federal Government continue in parallel with the coordinated development of these recommended systems rather than wait for a particular identity management solution.

The two preceding recommendations address some aspects of security and trust in the cloud; while security is certainly a critical element of trust in the cloud, it is not the only element. Good security is a continuous effort. This is true for all IT systems, not just the cloud.

A hypothetical target of perfect or near perfect security should not be used as an excuse for failing to use the cloud. Instead, the focus should be on whether the cloud provides security as good as or better than in-house IT deployments. The Government should, of course, always seek to enable continuous improvement of security and the human and technical systems that connect to the cloud. This point is consistent with the discussions and recommendations throughout this report, such as those on monitoring, measuring, and information sharing; on risk assessment and management; on the importance of policies, people, and practices; and on research.

Recommendation 3 (Responses to Data Breaches): Government should enact a national data breach law to clarify breach notification responsibilities and commitments of companies to their customers, and also update and strengthen criminal laws against those who attack computer systems and networks, including cloud computing services.

Cloud services, like existing IT systems, will be the target of malicious actors. In addition to defending against attacks, the Commission notes that clarity around what should happen in the event of a data breach will serve both cloud consumers and providers. Timely notification and transparency to customers (individuals, organizations and governments) enables rapid response and the opportunity to minimize damage. Also, cloud service providers and law enforcement should have the tools needed to take action against criminal activity against clouds, such as breaching of data.

Specifically, the Commission recommends a national data breach law to streamline notifications and make it simple for customers to understand their rights with regard to notification. Such a law should include preemption of state laws to provide for harmonization. In addition, the law should take into account the various types of entities that are involved in processing the covered data cloud service providers, industry, government, nonprofit organizations, academic organizations, etc., and specifically provide that notice should be given by the entity that has a direct relationship with the parties whose information was subject to the breach. Finally, the law should have notification requirements based on risk of harm.

Note that the motivation for such legislation is not limited to cloud computing, but adoption of cloud computing would benefit from this action. Specifically, by clarifying responsibilities and commitments around notification, the law will enable cloud providers to prepare to take expected steps in case of a breach and enable customers to trust the providers to do so.

As a complement to the above recommendations, the U.S. government should update and strengthen criminal laws against those who attack our cyber infrastructure, including cloud computing services. In addition to clarifying cyber criminal offenses and defining penalties, the Federal government must commit adequate resources and personnel to investigating and tracking down cyber criminals. As much of cyber crime is transnational, the Federal government should promote further international cooperation around cross-border prosecutions and identifying countries affording safe havens to such criminals.

Recommendation 4 (Research): Government, industry, and academia should develop and execute a joint cloud computing research agenda.

The Commission recommends that government, industry, and academia take responsibility for developing and carrying out a research agenda that will promote U.S. leadership in the cloud by enabling innovation that benefits customers and service providers. Relevant cloud-oriented research areas include, but are not limited to, usability, privacy, availability, integrity, confidentiality, security, cryptography, identity management, energy efficiency, resource allocation, portability, and dependability.

In conducting research on the cloud, industry should undertake short- and medium-term research where practical impacts are clear and investment risk is lower. Government research agencies, like the National Science Foundation (NSF) and the Defense Advanced Research Projects Agency (DARPA), should fund universities and other organizations to conduct long-range research activities, including those that build educational and research capacity and high-risk, high-reward projects. Cooperative cloud test beds will also be a critical element in advancing the overall evolution of cloud technologies.

Cloud technology has matured rapidly and will continue to develop. This recommendation should not be perceived as concern about cloud's current capabilities but rather as an investment in ensuring that the U.S. maintains a leadership role in the development, commercialization, and deployment of new cloud technologies and the expansion of cloud to new workloads, sectors, and activities.   Basic research investments a decade ago yielded the ideas, technologies and capabilities that are fueling today's cloud developments. Continued innovation in the cloud will benefit directly from a sustained research agenda.

TRANSNATIONAL DATA FLOWS

The development and use of latest-generation information and communication technologies has allowed organizations and individuals to operate cloud-based services in any location around the world. The expansion of trade and business operations on a global level has also brought new challenges for operating in the global market. The globalization of business and trade through technology has resulted in multi-directional data flows and an exploding volume of data sources and stakeholders. This adds complexity to cloud adoption because of the data, process, and people residing on multiple continents with different laws and cultures. Despite these challenges, transferring data is an integral part of the cloud and must be addressed.

The recommendations classified within Transnational Data Flows address the need for collaboration across national borders and the need for international frameworks to standardize the process. The Commission believes that recommendations to promote privacy frameworks, utilize performance-based criteria over proxy criteria that do not reflect specific and measurable attributes, and actions that overcome real and perceived challenges of transnational data flows are critical for the U.S. to adopt and lead in cloud computing. These actions are important because the United States must act as both a consumer of the cloud and as a leader in cloud innovation and markets. If the United States does not take a proactive position in both of these roles, the potential of a powerful global cloud market that enables individuals, industries and governments to innovate rapidly may not be fully realized.

Recommendation 5 (Privacy): The U.S. government and industry should promote a comprehensive, technology-neutral privacy framework, consistent with commonly accepted privacy and data protection principles-based frameworks such as the OECD principles and/or APEC privacy frameworks.

The Commission recommends that the U.S. build upon the work of existing, accepted privacy and data protection principles-based frameworks such as the Organization for Economic Cooperation and Development (OECD) and/or Asia-Pacific Economic Cooperation (APEC) to develop and promote a comprehensive, technology-neutral privacy framework. The existing U.S. laws are sector specific and state specific, and this approach is different than those in other regions (e.g., Europe). In some quarters, there is a concern that this may impede the transnational flow of data with other countries, especially those in Europe. These actions would help provide the certainty and flexibility required for continued cloud innovation and would be a step toward fostering a global market for cloud services. Industry should embrace such frameworks and utilize them to the fullest extent practicable.

Concepts of privacy are evolving in the Internet age, when information seldom has a single physical location, and duplication and sharing can occur quickly and easily. In addition, expectations around the norms and goals associated with privacy differ by culture, generation, and other factors. In this environment, the above recommendation is designed to demonstrate that the U.S. and U.S. companies take privacy seriously and to provide a basis for international discussions around mechanisms to resolve conflicting privacy policies. Such actions will also help overcome misunderstandings and confusion around the U.S. position on privacy; where uncertainty may be causing multinational and foreign organizations to avoid U.S.-based clouds or cloud computing altogether.

Recommendation 6 (Government/Law Enforcement Access to Data): The U.S. government should demonstrate leadership in identifying and implementing mechanisms for lawful access by law enforcement or government to data stored in the cloud.

The Commission recommends that the U.S. modernize legislation governing law enforcement access to digital information in light of advances in IT in general and the cloud in particular. Reform of the Electronic Communications Privacy Act (ECPA) is critical to clarifying the legal conditions under which U.S. cloud providers and their customers will operate, as technology changes have overtaken many aspects of ECPA as originally written. Various groups such as the Digital Due Process Coalition have proposed making government access to data stored in the cloud consistent with government access to data stored in in-house IT systems.

The U.S. Department of Commerce should conduct a study to assess the impact of the USA PATRIOT Act and similar national security laws in other countries on a company's ability to deploy cloud in a global marketplace. This action may provide insights into how best to address the uncertainty and confusion caused by national security statutes (e.g., PATRIOT Act[3] and similar laws of other nations) that are perceived as impediments to a global market place for cloud services.

In addition, the U.S. government should take the lead on entering into active dialogues with other nations on processes for legitimate government access to data stored in the cloud and processes for resolving conflicting laws regarding data. These discussions should build on existing agreements and arrangements with other nations (e.g., expedited Mutual Legal Assistance Treaties and bilateral and multilateral agreements).

These three steps all will contribute to increasing clarity around the rules and processes cloud users and providers should follow in an international environment. Without U.S. leadership and cooperative international efforts, the world will face a far more complex legal environment, one that is not conducive to fully leveraging the cloud.

Recommendation 7 (E-Discovery and Forensics): Government and industry should enable effective practices for collecting information from the cloud to meet forensic or e-discovery needs in ways that fully support legal due process while minimizing impact on cloud provider operations.

Critical to improving trust in the cloud and accelerating adoption is the need for best practices in collecting forensic data and information in ways that do not result in significant, adverse impacts on individuals and/or organizations using the cloud-based information. To address this, the Commission recommends that the Federal CIO work with applicable agencies such as U.S. Department of Justice and other relevant organizations to establish best practices specifically addressing acceptable methods for collecting forensic evidence from organizations using cloud-based information systems. In addition, cloud providers should assist their customers (e.g., individuals, commercial entities, government) with technologies to facilitate e-discovery and information retrieval requirements, whether in support of regulatory compliance or litigation activities.

Specific issues that will need to be addressed include methods to facilitate cooperation among service providers, how best to maintain a verifiable chain of custody, how best to collect data from proprietary technologies, and how best to minimize service availability impacts resulting from seizures of data and equipment. Improving the processes and practices around evidence collection and forensics will improve cloud customers' confidence in continuity of service and

[3] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

their ability to meet legal requirements. It will also provide tools to support the tracking and prosecution of cybercriminals (as discussed in Trust Recommendation 3).

Recommendation 8 (Lead by Example): The U.S. government should demonstrate its willingness to trust cloud computing environments in other countries for appropriate government workloads.

This recommendation highlights the role of the U.S. Government both as a customer of cloud services and as a leader in enabling trustworthy use of the cloud.

Government agencies, in evaluating potential models for using the cloud, should not assume or default to the notion that no government workload and/or task is suitable for cloud computing environments in other countries. Instead, they should carefully consider the types of data and tasks within their information and communications technology portfolios to match suitable workloads to the cloud computing models that achieve the required level of confidentiality, integrity, and availability at the appropriate levels of efficiency, cost, and redundancy. Evaluation of the specific workload and/or task needs is necessary to determine suitable potential cloud computing environments and models.

By evaluating cloud services based on the performance needs of specific workloads, the U.S. Government can show leadership in the adoption of approaches that recognize the multiple factors that contribute to ensuring trust in the cloud (see discussion around Trust Recommendation 1). The development of the frameworks, best practices, metrics, and standards to enable this approach should help businesses and other governments take a similarly comprehensive approach to trusted cloud deployment.

While the Commission is not declaring that no circumstances exist in which certain types of Federal data could be limited to U.S. storage, it is critical to understand that location is but one factor in the security of information, and location should not be viewed as a proxy for security in the cloud. For example, effective use of security technologies, including technologies to make data unreadable and unusable, is as important, if not more important than location in enhancing the security of data in the cloud.

Cloud providers typically locate data centers based on a variety of factors, including technical issues like network topology, economic issues like the price of electricity, and business issues like proximity to markets. Once data centers have been built, however, the storage and processing of data can occur in multiple data centers and across geographic boundaries and legal jurisdictions. For some customers and workloads, the preference might be to allocate storage and processing locations based on technical and economic factors (perhaps to maximize speed, or minimize cost). For other customers and workloads, there may be concerns about data touching certain legal jurisdictions that impose data handling requirements around privacy, retention or other legal or regulatory burdens.

To service customers with such concerns, cloud providers could enable the setting of policies around specific data and workloads to control what legal jurisdictions those data or workloads may enter and enable tags to carry provenance attesting to those locations. (The discussion above about the need to conduct international dialogues on methods for resolving inconsistent rules between countries is also a critical step toward dealing with these concerns.)

The Commission encourages adoption of approaches that give cloud providers the flexibility to develop and deploy services for a diversity of workloads in innovative ways, rather than constrain cloud services by geography. This will allow users, when appropriate, to take advantage of the potential benefits in access, reliability, resiliency, efficiency, and costs that can result from geographical distribution of workloads.

TRANSPARENCY

U.S. leadership in the cloud will be facilitated if cloud providers make a firm commitment to transparency. Transparency in the context of cloud computing requires vendors to share relevant information about their capabilities, offerings, and service levels.

Transparency by cloud vendors will encourage the shift to the cloud by addressing some of the primary reasons Federal agencies and commercial companies do not move to the cloud: uncertainty about how systems outside of their control will perform and fear of being unable to access or move their data. We offer two recommendations specifically designed to allay these concerns by ensuring customers maintain control over the performance of their systems and access to their data while still realizing the cost, efficiency, and scalability advantages of cloud computing.

Recommendation 9 (Transparency): Industry should publicly disclose information about relevant operational aspects of their cloud services, including portability, interoperability, security, certifications, performance and reliability. Industry and Government should support development of metrics designed to meet the needs of different user groups. These metrics should be developed in an open and transparent environment, taking into account the global nature of cloud use.

The Commission recognizes the need for information and tools that provide users with meaningful ways to evaluate the characteristics and performance of various cloud implementations, whether they are contemplating deployment or evaluating performance of their current services. Development of metrics around key cloud attributes should be driven by user needs and provider capabilities. The Government and commercial sector should collaborate on lessons learned, and each should be careful to avoid dominating the development of these metrics. Different Government and business sectors will likely demand different measures and tools.

Currently, the lack of transparency and standard metrics make it difficult for customers to compare the cloud offerings of different providers. Unsure about what they are being offered and unclear on the differences among the cloud options available, many customers hesitate before moving to the cloud or decide to delay moving to the cloud until there is agreement on common metrics that facilitate easy comparison of cloud providers. The Commission encourages industry to work with the appropriate government agencies to create customer tools that make "apples-to-apples" comparisons possible among different cloud providers and the services that they provide. This will increase the confidence commercial and government customers have in moving to the cloud and will accelerate cloud adoption.

Recommendation 10 (Data Portability): Cloud providers should enable portability of user data through documents, tools, and support for agreed-upon industry standards and best practices.

One benefit of the cloud is its ability to store and process large quantities of data. For customers making the transition to cloud, this often raises questions about how they access or move that data, especially in cases where they are switching between cloud providers. Data portability can be achieved in a variety of ways, and cloud providers should be transparent about their conformance with industry standards and best practices as well as the documents, tools, and relevant third-party solutions they make available to their customers. Customers should recognize that early consideration of data portability in selecting and implementing cloud services can reduce the risk of vendor lock-in.

A collection of data portability standards, formats, and practices is vital to encouraging widespread cloud adoption. Government and industry should collaborate on facilitating the rapid development and dissemination of these standards and other relevant tools. The collaboration between NIST and the private sector in preparing the NIST standards roadmap under the Federal Cloud Computing Strategy is an excellent example of these types of efforts. This work should serve as a model for future efforts around data portability and could be extended to other facets of cloud including workload and application portability. Both Government and industry should continue to emphasize open, multi-vendor, unencumbered standards and best practices.

TRANSFORMATION

Cloud computing is a disruptive technology that has significantly changed the IT landscape. Although cloud computing offers many benefits to adopters, it also poses challenges to Federal agencies and commercial organizations that are trying to adapt to the technological changes ushered in by the cloud. To achieve the benefits offered by cloud computing, Government and industry need to be open to re-envisioning the role of IT and willing to make the investments necessary to harness the power of the cloud.

The first two recommendations in this section focus specifically on actions that the Federal government can take to facilitate the transition to cloud. By stepping forward as a leader in the adoption of cloud computing, the Federal Government can play a key role in driving innovation and economic growth in the IT industry and demonstrate that it considers the cloud an important, effective, safe and secure environment. The second two recommendations focus on the transformation in infrastructure and workforce that are necessary for widespread cloud adoption.

Recommendation 11 (Federal Acquisition and Budgeting): Agencies should demonstrate flexibility in adapting procurement models to acquire cloud services and solutions. Congress and OMB should demonstrate flexibility in changing budget models to help agencies acquire cloud services and solutions.

In interviews with senior Government officials, the Commission found that the current Federal Acquisition Regulations (FAR) do not need alteration for agencies to acquire cloud services. The FAR is already flexible enough to allow agencies to acquire IT as a service. However, agencies should demonstrate flexibility in adapting current procurement models and existing contracts to take advantage of new cloud offerings.

One of the biggest challenges agencies may face in budgeting is predicting the costs of cloud computing over the course of a fiscal year. Cloud computing is designed to scale quickly to a customer's needs, providing maximum flexibility to the user. If the cloud service is based on a predictable subscription model (such as a standard monthly fee per user), these budget projections can be easily accommodated. If the cloud service is based on pay-as-you-go usage, however, it can be difficult to predict costs unless the user can precisely forecast future computing needs. To address this challenge, the Commission recommends that the current efforts to update and streamline the OMB 300 exhibit form and associated budget scoring include tools that facilitate and encourage the new business models associated with cloud. OMB and Congress should communicate to agencies that it recognizes budgeting for cloud is not like budgeting for traditional IT services and should assure agencies it will provide support and flexibility during and after the transition to the cloud.

To help agencies acquire cloud services, the Commission also recommends Congress and OMB demonstrate flexibility in changing budget models. Agencies currently face challenges transitioning funds between capital expenditure (also known as acquisition) accounts and operations and maintenance expenditure accounts when adopting and implementing cloud services and solutions. Most in-house information systems rely upon funding from capital expenditure accounts, while cloud services and solutions do not have intensive capital expenditures and are funded more from the operations and maintenance expenditure accounts. Agencies today, however, are hampered and even prevented from transitioning funds from the capital expenditure accounts to the operations and maintenance expenditure accounts, even when there are overall savings to be realized by the shift in IT approaches that requires the transition of the funds. This creates a disincentive for agencies to really drive savings and efficiencies through adoption of cloud services and solutions. Government must find ways to provide more flexibility for agencies to reduce and transition funds in the capital expenditure accounts to the operations and maintenance expenditure accounts as part of implementing innovative cloud solutions and achieving savings.

In making decisions about budgeting and acquisition, Federal agencies, through the CIO Council, would benefit from sharing best practices, tools for objective analysis of cloud performance, and ways to predict and document different contributors to the budgetary impact of switching to the cloud. To ensure that the CIO Council can provide this support to Federal agencies, it should include experts from a wide array of communities, including chief financial officers, chief acquisition officers, human capital officers, and program managers. Additionally, staffing OMB's other councils, such as the CAO and CFO Council, with cloud expertise could ensure these councils can also provide support to agencies implementing cloud.

As agencies are creating their business cases and preparing to move to the cloud, it is important to remember that the adoption of cloud is a multi-stage process. Initial deployments by government may not take full advantage of the potential capabilities and benefits of the cloud, but these steps are necessary for customers to explore new (and sometimes fundamentally different) approaches to selecting, acquiring, and utilizing IT. When agencies are in a transition to the cloud, it is critical that they take care that the policies and standards of the cloud provider do not lock the agency into an early deployment model. Agencies should require that policies be flexible enough to allow evolution of use and innovation through the adoption of new infrastructure, services, and applications.

Recommendation 12 (Incentives): Government should establish policies and processes for providing fiscal incentives, rewards and support for agencies as they take steps towards implementing cloud deployments.

Adopting a new technology can be difficult, and the transition of agencies to the cloud will require investment of time, resources, and political will by the Federal government.
In recognition of this, the Commission recommends that OMB establish incentives and provide support for agencies beginning cloud adoption.

On the fiscal side, agencies may be hesitant to undertake a significant change to their IT structure during a time of budgetary constraint or may have difficulty finding and justifying the costs associated with an IT transition. One possible incentive is to allow agencies to retain and redirect a portion of the overall budget savings realized from cloud adoption. Another approach is to provide seed money to agencies that help with the initial investments required in moving to the cloud.

OMB could also support agencies in the cloud transition by providing assistance in the processes that govern the transition. OMB and GSA assistance on moving from static to more dynamic assessment and authorization processes, change management, and compliance with OMB guidance would help facilitate the transition.

In addition to financial support and process assistance, public recognition and praise for agencies that are early adopters of cloud computing or deploy the cloud in particularly innovative ways is important. Individuals within agencies who have played key roles in enabling a cloud transition should also be recognized with service or financial awards. This sort of public support should be complemented by public acknowledgement by agency and Administration leadership that there are risks inherent in adopting a new technology infrastructure; this would provide some support for agency staff during the process of implementing the cloud transition.

Recommendation 13 (Improve Infrastructure): Government and industry should embrace the modernization of broadband infrastructure and the current move to IPv6 to improve the bandwidth and reliable connectivity necessary for the growth of cloud services.

The Commission recommends that the Federal government and industry continue to expand deployment of high bandwidth networking, enhance network resilience, and advance IPv6 adoption to ensure ample broadband connections.

The Commission recommends government and industry initiatives designed to increase the deployment and adoption of both wired and wireless broadband, especially to underserved areas of the country. Efforts such as those advocated in the Federal Communications Commission's National Broadband Plan, including making additional spectrum available and expanding opportunities for opportunistic and unlicensed spectrum use, are necessary to allow cloud computing to function effectively and for businesses and citizens to realize the benefits of innovative new cloud technologies.

With rapidly rising demands for connectivity, the last batch of IPv4 addresses, assigned earlier this year, is unlikely to meet demand beyond the end of 2011. Since cloud computing depends on the connection of many individuals, devices, and locations, a quick transition to IPv6 is vital to ensuring the successful adoption and operation of cloud computing in the future. The Commission applauds the Government's move to enable the use of IPv6 on external servers by October 2012 and on internal networks by 2014.

Recommendation 14 (Education/Training): Government, industry, and academia should develop and disseminate resources for major stakeholder communities to be educated on the technical, business, and policy issues around acquisition, deployment and operation of cloud services.

The transition to the cloud will require new capabilities for a variety of communities. The business community (and agency leaders) will need to understand how cloud changes the economics of their IT expenses and provides new capabilities through which to carry out their lines of business (or agency missions). Acquisition workforces will need new skills to gather and assess the information necessary to make informed purchasing choices. The responsibilities of IT workforces will expand to manage new cloud capabilities and, within cloud customers, the IT expertise needed will evolve as activities such as operations, maintenance, and development are shared or shifted to cloud providers.

Acquisition Workforce: The Commission commends GSA's outreach efforts to Federal agencies to provide materials, expertise, and support around investigating, procuring, and deploying cloud solutions. GSA could build on this work by creating a cloud educational portal to help agency buyers, architects, administrators, and end users in understanding all aspects of cloud computing. Resources for this portal might include white papers, articles, and training materials.

IT Workforce: Government, using existing programs in technology education and workforce training,[4] can facilitate and encourage academic institutions and educational organizations to develop and offer courses relevant to cloud, in partnership with industry. Industry and academia can help develop curriculum relevant to new technologies and skills (in partnership with the educational institutions and organizations), and support employee retraining.

Workforce education should embrace a spectrum from informal outreach to disseminate introductory or reference materials to targeted courses in specific skills and areas to integration of cloud-related topics into overall curricula in formal programs in computer science and engineering, project management, business schools, and other relevant areas. On the informal side, outreach to IT professionals could disseminate information about cloud issues, skills, and opportunities. Within the government, outreach and support networks for acquisition personnel would provide an opportunity to share experiences and best practices.

[4] The Department of Labor, the Department of Education, and the National Science Foundation all have programs in technology education and workforce training that might support activities relevant to cloud computing.

CONCLUSION

In a time when the government is seeking to do more with less and the commercial sector is being called upon to create jobs and grow the economy, now is the time to act on the cloud. Cloud computing has ushered in vast improvements in the cost, agility and efficiency of computing. These benefits alone drive a strong business case; however, the more compelling return is the opportunity to leap forward; to discover new markets and improve how we interact with, serve, and support U.S. citizens, users and other nations. The cloud holds the potential to unlock widespread entrepreneurism of all shapes and sizes, and expand the scope to do entirely new things — innovations such as social networking, which we could not fully imagine just a decade ago, would not exist without IT's continued evolution to the cloud.

Despite the clear benefits of cloud computing, many challenges impede its widespread adoption. These challenges face both those ready to embrace the cloud and those grappling with doubts about making the move. Those who are ready address challenges such as training acquisition personnel and determining which workloads should be moved to the cloud; those who are hesitant have concerns about, for example, the security of and control over data stored and workloads processed in the cloud. If unaddressed, these challenges threaten to slow the acceptance of cloud computing and delay the enormous advantages and opportunities it provides. To address the challenges and allay concerns, the Commission has offered in this report a range of practicable recommendations; these show the way forward to those ready to adopt the cloud, and guide cloud providers and users in addressing the issues of those not yet prepared to shift.

The Commission recognizes that industry and government share responsibility for enabling cloud's adoption and for leading in the cloud evolution. Reflecting the urgency to provide incremental movement, create momentum and lead through actions, many of the recommendations target short-term tactical and operational advances. Complementing these are longer term recommendations that reflect the strategic importance of the evolution, and the mandate to look beyond the cloud we know today, to the opportunities it creates for the future.

It is the hope of this Commission that the Federal Government, industry and academia will implement these recommendations and be leaders in shaping how the future unfolds through the adoption of the cloud across the United States and around the world. Furthermore, these recommendations should demonstrate that cloud computing is not a new technology that needs further validation or analysis before it can be safely adopted; it is a natural evolution in computing. Those who recognize this and take early advantage of the benefits it offers will, in the coming decades, be the leaders not in only IT but in driving the cloud's evolution, and therefore, in driving business and mission results.

Recommendation	Industry	Government	Academia	Short-Term	Long-Term
Recommendation 1 (Security & Assurance Frameworks): Government and industry should support and participate in the development and implementation of international, standardized frameworks for securing, assessing, certifying and accrediting cloud solutions.	•	•			•
Recommendation 2 (Identity Management): Industry and government should accelerate the development of a private sector-led identity management ecosystem as envisioned by the National Strategy for Trusted Identities in Cyberspace (NSTIC) to facilitate the adoption of strong authentication technologies and enable users to gain secure access to cloud services and websites.	•	•		•	
Recommendation 3 (Responses to Data Breaches): Congress should enact a national data breach law to clarify breach notification responsibilities and commitments of companies to their customers, and also update and strengthen criminal laws against those who attack computer systems and networks, including cloud computing services.		•		•	
Recommendation 4 (Research): Government, industry, and academia should develop and execute a joint cloud computing research agenda.	•	•	•		•
Recommendation 5 (Privacy): The U.S. government and industry should promote a comprehensive, technology-neutral privacy framework, consistent with commonly accepted privacy and data protection principles-based frameworks such as the OECD principles and/or APEC privacy frameworks.		•			•

Recommendation	Industry	Government	Academia	Short-Term	Long-Term
Recommendation 6 (Government/Law Enforcement Access to Data): The U.S. government should demonstrate leadership in identifying and implementing mechanisms for lawful access by law enforcement or government to data stored in the cloud.		•		•	
Recommendation 7 (E-Discovery and Forensics): Government and industry should enable effective practices for collecting information from the cloud to meet forensic or e-discovery needs in ways that fully support legal due process while minimizing impact on cloud provider operations.	•	•		•	
Recommendation 8 (Lead by Example): The U.S. government should demonstrate its willingness to trust cloud computing environments in other countries for appropriate government workloads.		•			•
Recommendation 9 (Transparency): Industry should publicly disclose information about relevant operational aspects of their cloud services, including portability, interoperability, security, certifications, performance and reliability. Industry and Government should support development of metrics designed to meet the needs of different user groups. These metrics should be developed in an open and transparent environment, taking into account the global nature of cloud use.	•	•		•	
Recommendation 10 (Data Portability): Cloud providers should enable portability of user data through documents, tools, and support for agreed-upon industry standards and best practices.	•			•	

Recommendation	Industry	Government	Academia	Short-Term	Long-Term
Recommendation 11 (Federal Acquisition and Budgeting): Agencies should demonstrate flexibility in adapting procurement models to acquire cloud services and solutions. Congress and OMB should demonstrate flexibility in changing budget models to help agencies acquire cloud services and solutions.		•		•	
Recommendation 12 (Incentives): Government should establish policies and processes for providing fiscal incentives, rewards and support for agencies as they take steps towards implementing cloud deployments.		•			•
Recommendation 13 (Improve Infrastructure): Government and industry should embrace the modernization of broadband infrastructure and the current move to IPv6 to improve the bandwidth and reliable connectivity necessary for the growth of cloud services.	•	•		•	
Recommendation 14 (Education/Training): Government, industry, and academia should develop and disseminate resources for major stakeholder communities to be educated on the technical, business, and policy issues around acquisition, deployment and operation of cloud services.	•	•	•	•	