U.S. HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

HEARING CHARTER

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.

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

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.

[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

V. Cloud Computing Opportunities

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

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",

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

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.

---

[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.

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 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.

[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