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

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

July 1, 2010

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

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

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

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

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

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

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

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

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

Cloud computing is one such technology.

Benefits of the Cloud

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

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

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

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

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

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

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

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

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

Moving to the Cloud

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

[3] http://blog.rightscale.com/2008/04/23/animoto-facebook-scale-up/

[4] http://www.cars.gov/files/official-information/CARS-Report-to-Congress.pdf, pg.10-12

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

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

Security & Privacy

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

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

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

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

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

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

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

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

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

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

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

Closing the IT Gap

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

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

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

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

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

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

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

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

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

Appendix – Characteristic of Cloud Computing

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

Essential Characteristics:

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

Deployment Models:

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

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

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

Service Models:

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