STATEMENT OF

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

BEFORE THE

HOUSE COMMITTEE ON HOMELAND SECURITY

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION and SECURITY TECHNOLOGIES

October 6, 2011

"Cloud Computing: What Are the Security Implications?"

Chairman King, Ranking Member Thompson 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 secure 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 IT reforms we have underway are enabling agencies to use information more efficiently and effectively, delivering improved mission results at lower cost.

Cloud Computing Adoption in the Federal Government

Before I discuss the security of cloud computing, and the Federal Risk Authorization and Management Program (FedRAMP) in particular, I would like to make a two important points. First, cloud computing offers a compelling opportunity to substantially improve the efficiency of the federal government. It moves us from buying and managing physical assets to purchasing IT as a commoditized service. Agencies pay for only IT resources they use in response to fluctuating program demands, avoiding the expenses of building and maintaining costly IT infrastructure. When implemented with sound security risk management approaches, cloud computing also ensures more consistent protection of the government's IT infrastructure, data and applications.

Second, practical use of cloud computing offers substantial performance benefits for the government. Federal agencies are moving to consolidate and virtualize the more than 2,000 federal data centers. Cloud technologies provide an ideal path forward to maximize value in IT investment dollars while substantially lowering costs – an essential focus given federal budget constraints. Case studies we have collected from agencies point to benefits that include:

- tangible cost reductions (data storage, web hosting and analytics performed on the government's vast data repositories);
- enhanced productivity (shifting workforce to more high value process improvements, problem solving, and customer service excellence);
- greater flexibility and scalability (enabling CIOs to be much more responsive to pressing service delivery expectations); and
- improved self-service capabilities (on-line streamlined commodity-like purchasing for IT resources rather than long, arduous IT acquisitions).

GSA is playing a leadership role in facilitating easy access to cloud-based solutions from commercial providers that meet federal requirements. This will enable agencies to analyze viable cloud computing options that meet their business and technology modernization needs, while 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. These cloud procurement vehicles ensure effective cloud security and standards are in place to lower risk and foster government-wide use of cloud computing solutions such as virtualization technologies for government data centers, cloud email, disaster recovery/backup, and infrastructure storage. Useful information about cloud computing and available solutions is accessible from our web page, Info.Apps.gov.

GSA's Federal Cloud Computing Initiative was started and is managed under GSA's e-Government program. In FY10 and FY11 GSA's Federal Cloud Computing Initiative (FCCI) Program Management Office (PMO) focused on five primary tasks:

- Establishing procurement vehicles that allow agencies to purchase IT resources as commodities, culminating in the award of the Infrastructure as a Service (IaaS) Blanket Purchase Agreement under GSA Schedule 70 to 12 diverse cloud service providers
- Addressing security risks in deploying government information in a cloud environment - resulting in the development of the Federal Risk Authorization Management Program (FedRAMP)
- Establishing a procurement vehicle that will allow agencies to purchase cloud-based e-mail services, which created GSA's Email as a Service (EaaS) Blanket Purchase Agreement
- Supporting the government-wide collection and assessment of data center inventories, and assisting agencies in the preparation and execution of plans to close and consolidate data centers. Current work includes developing a comprehensive data center Total Cost Model for agencies to use to analyze alternative consolidation scenarios, enables data-driven decision-making for infrastructure cost and performance optimization. Operationalizing 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 is also being pursued.
- Creating 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

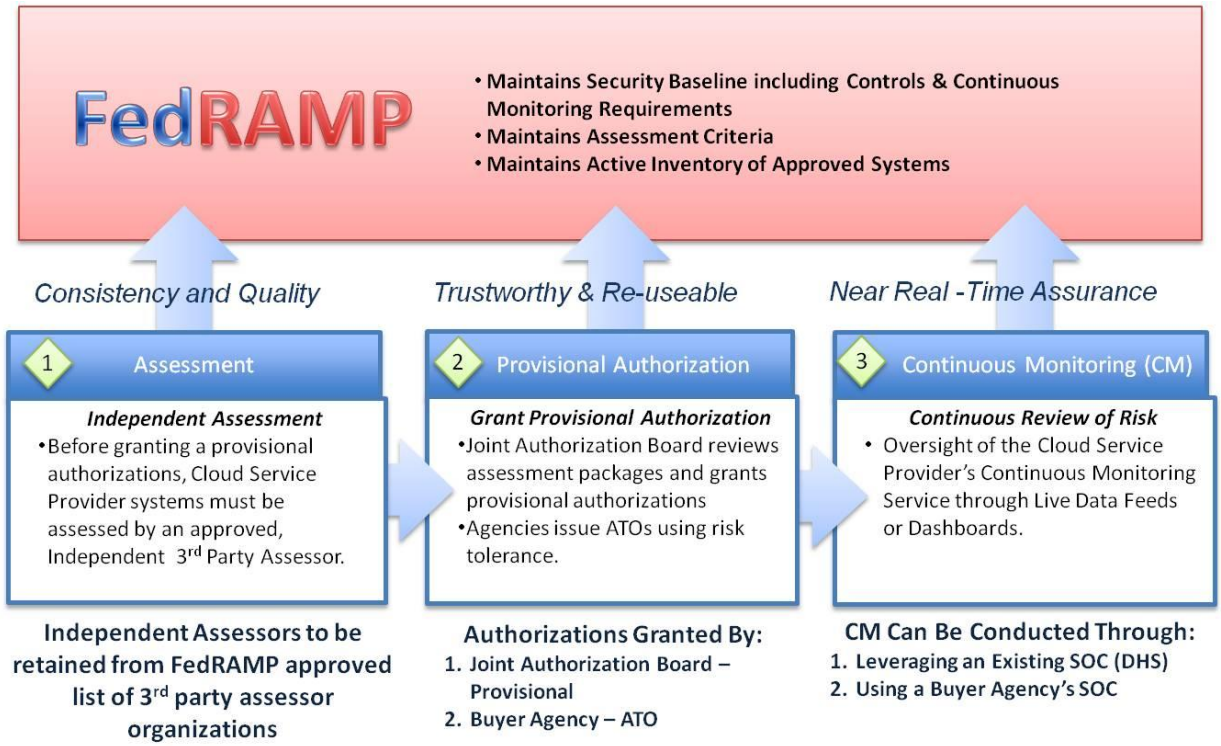
Initial funding provided by the e-Gov Fund has allowed GSA to be an effective catalyst for secure cloud technology adoption governmentwide. However, there are critical activities that still need to be accomplished to fully realize the significant cost savings and productivity improvements that GSA can help agencies achieve. The continuation of these cost-saving initiatives is dependent on FY12 eGov Fund budget levels and decisions.

FedRAMP: Ensuring Secure Cloud Systems Adoption

Cloud computing – like any technology – presents both known and new risks alongside the many benefits outlined above. To address these risks in a more uniform and comprehensive manner, we will soon launch a new government-wide cloud security program – the Federal Risk and Authorization Management Program (FedRAMP). 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. Today, each agency typically conducts its own security Certification and Accreditation (C&A) process for every IT system it acquires, leading to unnecessary expense, duplication and inconsistencies in the application of NIST derived security controls testing, evaluation, and certification procedures. According to the 2009 FISMA report to Congress, agencies reported spending $300 million annually on C&A activities alone.

At GSA, we have worked in close collaboration with cybersecurity and cloud experts in NIST, DHS, DoD, NSA, OMB, and the Federal CIO Council and its Information Security and Identity Management Subcommittee (ISIMC) to develop FedRAMP. An OMB policy memo officially establishing the FedRAMP program is expected shortly. The intent is to strengthen existing security practices associated with cloud computing solutions which, in turn, will build greater trust between providers and consumers and accelerate appropriate adoption of secure cloud solutions across government. Accordingly, FedRAMP establishes a common set of baseline security assessment and continuous monitoring requirements for FISMA low and moderate impact risk levels using NIST standards that must be adhered to by all cloud systems. Figure 1 illustrates how FedRAMP will address three fundamental challenges with how the federal government approaches ensuring cloud security.

Figure 1: FedRAMP – Addressing Three Critical Challenges to Cloud Security



Ensuring Consistency and Quality in Cloud Security Certification and Accreditation

FedRAMP approves qualified, independent third party security assessment organizations, ensuring consistent assessment and accreditation of cloud solutions based on NIST's longstanding conformity assessment approach. As noted above, security C&As are currently performed with varying quality and consistency. This is true for situations where a third party service provider is contracted to do a security assessment of a CSP provided system, product or service and where government security organizations perform the work themselves. As a result, trust levels are low for reusing this work across agencies.

To address this challenge, FedRAMP will require that cloud services providers be assessed using these approved, independent third party assessment organizations (3PAOs). The 3PAOs will initially apply for accreditation through the FedRAMP PMO and be assessed using established conformity assessment criteria developed by NIST. This will ensure higher quality assessments, done much more consistently, using agreed upon FedRAMP security assessment controls. This can save millions of dollars

in expenses borne both by government and industry in running duplicative assessments of similar solutions by each agency.

Building Trust and Re-Use of Existing C&A Work

All IT systems, including cloud solutions, must receive an Authority to Operate (ATO) from the buying agency before they can be made available for purchase and implemented. The ATO is based on a thorough review by agency security professionals of the security packages submitted following the C&A process described above. To accelerate cloud adoption and enable C&A re-use, FedRAMP will provide a single, provisional authorization that can be used by all agencies as the basis for issuing an ATO. If additional security assessment evaluation and testing is needed for specific agency cloud implementations, the C&A should only address any additional controls needed above the existing FedRAMP approved baseline.

FedRAMP establishes a Joint Authorization Board (JAB) that reviews all cloud systems that have been assessed by approved 3PAOs using FedRAMP controls and processes. The JAB membership consists of CIOs and Technical Representatives from DOD, DHS, and GSA. The JAB reviews the C&A work and decides whether to grant the "provisional authorization" – a seal of approval on the C&A work. The security packages, assessments and documented decisions will be accessible within government from a secure central repository. While each agency must grant its own ATO for systems under its control, FedRAMP will facilitate greater use of an "approve once, and use often" approach, leveraging more ATOs across government.

Moving Towards More Real-Time Security Assurance

FedRAMP 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. Using the expertise of industry, NIST, NSA, DHS and ISIMC, nine initial continuous monitoring controls have been identified that are among the most common persistent threat vulnerabilities in cloud and non-cloud systems environments. Cloud Service Providers (CSPs) must agree to near-real time reporting of continuous monitoring data feeds to DHS and/or agency Security Operations Centers (SOCs). We are finalizing data reporting details, with the expectation that the process will eventually use automated data feeds to maximize efficiencies and timeliness. When done in addition to the C&A evaluations, this will result in valuable situational cyber awareness -- a relevant and timely picture of a CSP's security posture. In addition, this approach provides visibility of prompt mitigation and tangible evidence of resolution; ensuring quick steps are taken to minimize threats to government data and operations.

In short, FedRAMP offers the following improvements for cloud security assessments conducted in the federal government:

- ✓ **Cloud Security Requirements:** Standardizes a minimum, baseline set of government-wide security controls based on *NIST Special Publication 800-53 Revision 3 Risk Management Framework* for low or moderate risk cloud systems.
- ✓ **Assessor Accreditation:** Manages process for accrediting independent, third-party assessors to ensure competency, consistency, and compliance.
- ✓ **Assessment & Authorization:** Validates cloud services provider's security authorization packages to ensure consistent application of standard controls. Empowers a Joint Authorization Board (JAB) comprised of CIOs from DoD, DHS, and GSA, to issue provisional authorization for cloud systems. Agencies can leverage this baseline in granting their own ATOs and focus on their specific requirements "delta" for any additional C&A work.
- ✓ **Continuous Monitoring:** Based on an *initial* set of controls, performs continuous monitoring, automates oversight of government-wide authorized systems, and notifies participating agencies of any system changes to the authorized risk posture.
- ✓ **Incident Response Coordination:** Coordinates control and management of incident response for FedRAMP authorized cloud systems.
- ✓ **Data Repository:** Maintains up-to-date list of all FedRAMP authorized systems; facilitates secure access to security authorization packages; maintains contracting templates, SLAs, etc.

There is strong support and demand for stronger cloud security from agencies seeking to adopt cloud services, as required by the Administration's Cloud First policy. Industry cloud services providers need to know the specific cloud security capabilities for which they are accountable. They also desire more efficiency in how C&As and ATOs are leveraged government-wide to avoid unnecessary, duplicative, costly security evaluations. Ensuring IT security is an ongoing challenge. We fully expect to make improvements to the process based on collaboration with all key stakeholders, including industry, lessons learned and the continuous evolution of security standards and controls based upon the careful, deliberative work of NIST.

FedRAMP will be launched in phases that incrementally build toward sustainable operations and allows for risk management by capturing ongoing lessons learned and process improvement. Initial rollout will occur this Fall. Initial Operational Capabilities will have limited scope and cover a relatively small number of cloud service providers. Full operations are expected to begin next Spring with more robust operational capabilities and larger intake of cloud service providers for FedRAMP review and approval. Late in 2012, we expect sustaining operations to scale by demand using a privatized board for 3PAO accreditation. We will discuss the rollout in more depth with

the Congress, government executive branch agencies, industry, and the public prior to the initial launch date.

Conclusion

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 cloud 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 delivered in a secure environment.

FedRAMP will provide a sound, cost-effective framework for secure cloud computing. 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 appropriate security and risk management. Agencies should analyze business needs and identify cloud solutions that best fit their requirements by making secure cloud adoption part of an overall IT portfolio management and sourcing strategy. Consistent with the Federal Cloud Computing Strategy, NIST is currently working on the first draft of a USG Cloud Computing Technology Roadmap, to be released for public comment in November, 2011. If linked to cloud provider products and services, it would greatly assist in this decision-making.

Mr. Chairman, thank you for the opportunity to appear today. I look forward to answering questions from you and members of the Subcommittee.

David L. McClure
Associate Administrator
Citizen Services and Innovative Technologies
U.S. General Services Administration

Dave McClure was appointed as the Associate Administrator of the U.S. General Services Administration Office of Citizen Services and Communications effective August 24, 2009. In 2010, the office was re-established as the Office of Citizen Services and Innovative Technologies.

As Associate Administrator, McClure advances GSA's responsibilities in serving the American people through open and transparent government initiatives to provide increased government accessibility to the public. McClure also identifies and applies new technologies to improve government operations and service delivery.

The Office of Citizen Services and Innovative Technologies is a powerful advocate for making government operations more open, transparent, and participatory. Through the use of innovative technologies, the office connects the public to government information and services through various channels, including collaborative and public dialogue tools, call centers, and other emerging new media and citizen engagement technologies. As part of this effort, the office runs the award-winning and recently re-designed USA.gov, the official website of the federal government, Data.gov, and created and hosts Challenge.gov. In addition, he oversees the Federal Cloud Computing PMO which is responsible for implementation and evolution of the Apps.gov web site, creation of FedRamp (a governmentwide security accreditation, certification, and authorization program), and governmentwide data center consolidation.

McClure most recently served as the managing vice president for Gartner Inc.'s government research team. There, he managed the global government research agenda and analyst support, and was lead researcher on government information technology management practices. McClure also served on the Obama-Biden transformation, innovation, and government reform transition team, which examined federal agency IT plans and status for the incoming administration.

Before working at Gartner, McClure served as vice president for e-government and technology at the Council for Excellence in Government. Previously, McClure had an 18-year career with the Government Accountability Office, where he conducted wide-ranging reviews of major systems development and IT management capabilities in almost all major Cabinet departments and agencies. He also served as ex-officio member of the Federal Chief Information Officer Council from its inception in 1996 through 2001.

McClure has also provided key input on major federal government IT reform legislation, such as the Clinger-Cohen Act of 1996 that created federal government CIOs and IT business-case requirements, and the e-Government Act of 2002. He is a three-time winner of Federal Computer Week's "Top Federal 100" (1998, 2001, and 2004) for impact on government IT directions and improvements. He was elected a Member of the National Academy of Public Administration in 2009 and received AFFIRM's 2010 Government-wide IT Leadership Award.

McClure received his Bachelor of Arts and a master's degree in political science from the University of Texas, and a doctorate in public policy from the University of North Texas. He also completed post-graduate work in IT management at Harvard and George Washington universities.