Testimony of

Mark Ryland
Director, Solutions Architecture and Chief Architect
Worldwide Public Sector
Amazon Web Services

Before the

U.S. House of Representatives
Committee on Oversight and Government Reform's Subcommittee on IT

Field Hearing on

"The State of Cloud"

September 22, 2015

Good afternoon, Chairman Hurd and Ranking Member Kelly, my name is Mark Ryland. I serve as the senior technologist for the worldwide public sector business of Amazon Web Services (AWS). On behalf of AWS and our customers, thank you for giving me the opportunity to testify today on how cloud computing can enable the federal government to achieve substantial cost savings while also improving federal information security. We are grateful to you for exploring this important topic, including both the opportunities and challenges for the further expansion of cloud computing in federal agencies and departments.

After briefly describing the utility-based model of cloud computing, which is the model of cloud services that we offer at Amazon, my testimony will illustrate how government, education and other organizations already leverage commercial cloud solutions to save money and improve agility and security in their delivery of IT to support their missions. I will conclude by suggesting ways that this Subcommittee and the U.S. Congress could help accelerate the benefits of cloud in federal agencies by advancing effective "cloud first" approaches and policies. Specifically, I will make recommendations

related to strengthening FedRAMP, modernizing budget authorities to accelerate cloud adoption, and requiring federal agencies to adopt a GAO recommendation to fully assess their IT investments for suitability for migration to the cloud.

AWS and the Utility-based Model of Cloud

Amazon.com opened for business on the World Wide Web in July 1995 in Seattle and 20 years later offers Earth's Biggest Selection. Amazon seeks to be Earth's most customer-centric company, where customers can find and discover anything they might want to buy online, and endeavors to offer our customers the lowest possible prices and the best possible services. After over a decade of building and running the highly scalable set of web applications and databases known as Amazon.com, the company realized that we had developed a core competency in operating massive scale technology infrastructure and datacenters. So, we embarked on a much broader mission of serving a new customer segment – including government agencies – with a platform of web services through our cloud computing business: AWS.

In 2006, AWS began offering developer customers access to in-the-cloud infrastructure services based on Amazon's own back-end technology platform. Since then, a vast range of organizations from the smallest start-ups to the largest enterprises and government agencies have taken advantage of this flexible and powerful way of accessing IT resources. Previously, organizations only had an option of either making massive capital investments to build their own infrastructure or of entering into long-term contracts with a vendor for a fixed amount of datacenter capacity that they might or might not use. This choice meant either paying for wasted capacity or worrying about shortages, *i.e.*, that the capacity they forecasted was insufficient to keep pace with their growth. Businesses and government agencies spent a lot of time and money managing their own datacenters and co-location facilities, which meant time not spent on their core organizational missions of providing products and services for their customers and citizens. The ability of a customer to quickly provision resources, use them, shut them down when not needed, and pay for only what it uses is what we mean by "utility computing" or "public cloud computing" as defined by the National Institute of Standards and Technology (NIST) in its seminal cloud definition document that was published in October 2011.

As of September 2015, AWS has more than a million active customers in 190 countries, including 1,700 government agencies, 4,500 education institutions and more than 17,000 nonprofit organizations. It's a very diverse customer base that ranges from some of the most successful startups like Pinterest and Airbnb and Dropbox and Dropcam to large enterprises all over the world in every imaginable vertical segment. For example,

in oil and gas, Shell and BP; in healthcare, Johnson & Johnson, and companies such as Pfizer, Merck, and Bristol-Meyer Squibb; in financial services, Intuit, the Financial Industry Regulatory Authority (FINRA), and Sun Corp; in manufacturing, GE, Phillips and Schneider Electric; in technology, Netflix, Samsung and Adobe; in media, Time, News Corp, the Washington Post and the New York Times.

Throughout the public sector, we also have a very diverse customer base, with many of those customers right here in Texas. For instance, the Human Genome Sequencing Center at Baylor College of Medicine partnered with a company called DNAnexus to undertake the single largest human whole-genome analysis project in history. Baylor used the AWS Cloud to analyze more than 14,000 human genomes, searching for a better understanding of the relationship between genetic variation and mutation and serious heart disease as part of their work with a research consortium called CHARGE (Cohorts for Heart and Aging Research in Genomic Epidemiology).

Another example is the Texas Digital Library (TDL), a consortium of higher education institutions in Texas that has provided shared digital library services since 2005. The mission of TDL is to enable each of its member libraries to advance a program of digital initiatives in support of research, scholarship, and learning. Using AWS, TDL has been able to provide storage and access for open journal systems, open conference systems, and thesis and dissertation systems for the benefit of faculty, researchers, and students across Texas.

In addition, the Texas Department of Information Resources (DIR) and AWS make it easier for state agencies and other customers of the DIR to move to the cloud. Together, we have developed a contract that enables state customers to buy cloud services directly from the cloud service provider (CSP). Amazon is one of 22 companies the DIR has contracts with for cloud technology under its cooperative contracts program. Prior to the new arrangement, Texas agencies had to conduct their own separate procurements and vendor solicitations. Now, we have a contract between AWS and the entire state of Texas that each agency can buy from, improving speed to development and providing more agility and innovation faster to organizations throughout the state.

These three examples in Texas highlight how cloud computing enables organizations in the state to leverage shared services and cloud computing resources without complexity in the acquisition and procurement process, an approach that is also very relevant to the U.S. federal government. In fact, with the utility-based model of cloud, if a program is funded one year and then unfunded the next, or a pilot project or test program does not achieve its expected results, federal agencies no longer need to be tied to large, capital IT expenditures that cost millions of dollars. And, when a project does fail, agencies have more flexibility to adjust quickly and contain costs. In fact, IT-based projects

are far less likely to fail at all because utility computing allows for small-scale, inexpensive experiments followed by rapid adjustments in advance of any large investments, thus increasing knowledge via experimentation and decreasing the overall chance of failure. The result is achieving more return on your investment and avoiding costly overruns and high profile failures. That's how businesses operate and that is what AWS is empowering public sector organizations, including U.S. federal agencies, to do as well.

State of Cloud Adoption in the U.S. Federal Government

As this Subcommittee stated in the Hearing Announcement for this field briefing today, the U.S. federal government spends more than $80 billion annually for IT purposes, with over 70 percent of that estimated to be spent on legacy systems. That's a lot of money – over one half trillion in the last decade – that has been spent on technologies and services that are geared toward maintaining or preserving legacy systems rather than spent on new applications to tackle pressing challenges in areas such as public health and education. In today's federal budget environment, it is no longer acceptable to spend the vast bulk of federal IT dollars on maintaining legacy systems, and we applaud the efforts by the House Oversight and Government Reform Committee and this Subcommittee to highlight this as a major issue that needs to be resolved.

Since the Office of Management and Budget (OMB) issued the first *Federal Cloud Computing Strategy* in February 2011, federal civilian agencies have moved more workloads to the cloud. The federal "Cloud First" policy has resulted in departments and agencies with as diverse missions as the U.S. Department of Health and Human Services (HHS) to the U.S. Department of Treasury to begin their transition to cloud computing. But as the Government Accountability Office (GAO) report to Congress[1] issued last year found, the allocation to cloud computing services of the reviewed[2] federal agencies' overall IT budgets, is still relatively small. For example, the percent of IT spend in FY2014 budgeted for cloud at Treasury was only 6 percent and at HHS it was only 1 percent according to the GAO report. The GAO report also noted that there were seven common challenges that the federal agencies and departments that were reviewed experienced in moving services to cloud computing: 1) Meeting federal security requirements; 2) Obtaining guidance; 3) Acquiring knowledge and expertise; 4) Certifying and accrediting vendors; 5) Ensuring data portability and interoperability; 6)

[1]U.S. Government Accountability Office (GAO) Report to Congressional Requesters: Cloud Computing: Additional Opportunities and Savings Need to Be Pursued", September 2014: http://www.gao.gov/products/GAO-14-753

[2] The GAO's Report to Congressional Requesters in September 2014 reviewed the following federal departments and agencies: Agriculture, General Services Administration, Health and Human Services, Homeland Security, Small Business Administration, State, and Treasury.

Overcoming cultural barriers; and 7) Procuring services on a consumption (on-demand) basis.

Our experience in working with U.S. federal agencies has confirmed that many of the seven identified areas in the GAO report continue to be challenges for our customers and prospective customers, but the challenges that come up most in federal customer discussions are: 1) agencies overcoming cultural barriers, particularly the historical bias toward on-premise data centers, 2) agencies addressing procurement, acquisition and budget policies or approaches related to moving to a utility-based model of technology services, and 3) agencies clearly defining or understanding their security compliance requirements. Despite these ongoing challenges, we are seeing adoption of AWS increase significantly across the federal government to support a range of missions, services and applications. Below are some examples of how federal agencies and federally funded organizations are leveraging AWS today to enable innovation, improve agility and collaboration, with a secure, flexible IT infrastructure that is on-demand and cost effective:

- When the **U.S. Securities and Exchange Commission (SEC)** needed to investigate the events leading to May 6, 2010 Flash Crash, the company used Tradeworx and AWS to create an analytics platform called MIDAS (Market Information Data Analytics System) at 10 percent the cost of a traditional environment in less than four months. MIDAS ingests market data that grows at the rate of 20 million transactions per second, 20 billion records and one terabyte of data per day. Utilizing the power of MIDAS running on the AWS Cloud, the SEC can now reconstruct any market event, down to the individual record, and analyze more than 3 billion data points in 2.8 seconds instead of weeks or even months.

- **NASA's Jet Propulsion Laboratory (JPL)** decided several years ago to use the utility-based model of cloud in support of the Mars Rover-related programs and has had considerable success in doing so. AWS has enabled the Rover program to run more efficiently and at a substantially reduced cost. When the Mars Space Lab (also known as Curiosity) achieved its successful landing in 2012, cloud computing infrastructure from AWS was utilized in support of various aspects of that effort, including the data and image management pipeline dealing with all the new data streaming down from Mars, as well as live video streaming of the landing event itself. As Tom Soderstrom, the CTO of NASA JPL, has described, JPL has leveraged cloud services to dramatically reduce IT costs and, in the process, increased their agility and decreased the "time to science," while enabling JPL to have complete flexibility when using those computing resources.[3]

[3] For more information on AWS's work with NASA JPL, see "The Jet Propulsion Laboratory Reaches For the Cloud",

- The **U.S. Food and Drug Administration (FDA)** leverages cloud services to bring scale and cost effective innovation to protect and promote public health. The agency, which receives 100,000 handwritten reports of adverse drug affects each year, needed a way to make the data entry process more efficient and reduce costs. By using AWS, the FDA quickly turns manual reports into machine-readable information with 99.7 percent accuracy, reducing costs from $29 per page to $0.25 per page.

- At the **Centers for Medicaid and Medicare Services (CMS)**, there are now three major services that are part of the Healthcare.gov web application running on AWS. CMS moved to the cloud to be able to scale up and scale down the systems, particularly during an open enrollment period. John Booth, the Director of the Web and New Media Group at CMS recently said that "we are probably running about three times the number of servers in AWS that we were in a traditional data center for about the same cost." He added that "cloud computing has really been transformational."

- At the **U.S. Department of the Navy**, AWS worked with the Office of the CIO to develop a portal hosted in the cloud for the Department's Secretariat organizations. The portal met all security requirements, with a 66 percent reduction in costs.

The Security Benefits of Cloud Computing

Cloud computing security has been a top priority for both AWS and our customers for years. Once the federal government's Cloud First policy was issued in 2011, which called for CIOs to "implement a cloud-based service whenever there was a secure, reliable, and cost effective option" agencies had to determine what kinds of applications and workloads to move to the cloud first while also understanding CSPs' security models.

There was a certain degree of reluctance at first to trust the utility-style, multi-tenanted, so-called "public" cloud. When people first heard "the cloud" they thought of free, advertising-driven consumer services like consumer email. Also, whenever a new abstraction appears in the technology industry, it takes time for people to become accustomed to it, and the benefits that it offers. A few years ago it was server virtualization that IT pros where initially skeptical about. Then that skepticism moved over to "the cloud." As customers and IT professionals have learned about the AWS Cloud

---

InformationWeek, April 28, 2015.

and its capabilities, however, the initial concerns have turned completely to a growing realization that the cloud offers many security *benefits* over traditional IT infrastructure.

There is a growing recognition that cloud and its accompanying automation and agility provide the opportunity to *enhance* systems security, not just achieve improvements in system delivery and reductions in cost. In a recent article about the National Renewable Energy Laboratory (NREL) transition to cloud computing, Chris Webber, NREL's senior cloud architected was quoted as saying: "It's just as secure – you might even argue it's more secure, but at the same time, we've made it easier to access (the data)".[4]

For U.S. federal government customers, a critical element of progress in this area has been our commitment to meeting and exceeding government compliance standards. First, the work that NIST has done to update federal information security controls and guidelines, such as the NIST Special Publication 800-53 series,[5] has been critical as this work aligns to more modern cloud-style systems as well as international industry standards and best practices. Second, the establishment of the Federal Risk and Authorization Management Program (FedRAMP), a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring, has also been critical for expansion of federal cloud computing. FedRAMP has been emphasized in multiple OMB memoranda and guidelines, in the President's FY2015 Budget Request (on Page 41), and in the FY2015 National Defense Authorization Act (NDAA) in Section 834.

More recent guidance, such as NIST Special Publication 800-171, released in June 2015 and focused on the protection of Controlled Unclassified Information (CUI) on nonfederal systems is also another example of NIST's important work. AWS is already compliant with these guidelines, and customers can effectively comply with NIST 800-171 immediately by AWS. NIST 800-171 outlines a subset of the NIST 800-53 requirements, a guideline under which we have already been audited under our FedRAMP compliance program. With this in mind, federal customers can move forward with migrating CUI workloads to AWS, with the knowledge that AWS can maintain compliance with US federal security requirements as they evolve.

But security in the cloud is more than just meeting federal compliance requirements. Moving workloads and applications to a commercial cloud provider can significantly *improve* the security of federal agencies' systems and data. Roger Baker, the

[4] "Renewable Energy Lab Begins Moving More Sensitive Data to the Cloud", *Nextgov.com*, September 10, 2015.
[5] NIST Special Publication 800-53: "Security and Privacy Controls for Federal Information Systems and Organizations".

former CIO of the Department of Veteran Affairs (2009-2013) recognized the value of the cloud as a way of improving security in an op-ed that he penned in January 2015.[6] In that article, Baker stated that "agencies have believed that commercial cloud offerings were not secure enough for their applications, especially those requiring 'high' protections under the Federal Information Security Act" or FISMA. Baker then wrote: "But time and investment by the private sector have turned that belief into a canard. The government's own FISMA audits [of its own infrastructure] provide the primary proof. These audits observe widespread issues with configuration control, patch management, unsupported versions of hardware and software, disaster recovery and numerous other vulnerabilities." He also added that "Commercial cloud vendors aggressively avoid these problems as a fundamental part of their business model…As a result, their security posture already far surpasses that of most of the 6,000-plus legacy federal data centers."

Mr. Baker went on to identify six specific reasons why commercial clouds provide a better basis for secure systems than existing federal data centers: (1) cloud providers have new and sometimes purpose-built equipment and software, constantly updated; (2) system configurations are standardized and automatically created to eliminate variances, and for maximum efficiency; (3) security patches are automatically applied to all systems on a timely basis; (4) cloud environments are certified to multiple different national and international security standards; (5) the private sector can hire high-level system engineering and security talent more readily; and (6) the cloud vendor's brand and entire business is at risk should security be compromised, ensuring laser focus and full alignment to addressing security issues.

We believe that the evidence fully supports the arguments made by Mr. Baker and others that security should no longer be seen as a *barrier* to cloud adoption, but an argument *in favor* of it. And indeed we are seeing more and more organizations recognize the security benefits of transitioning to a commercial cloud environment. For example, at a developer conference in late 2014, Mark Schwartz, CIO of Citizenship and Immigration Services in the Department of Homeland Security, listed his improved security and compliance posture as one of the primary benefits his team has received from using a modern "dev/ops" software development and deployment practice running on the AWS Cloud. That is also why in the U.S., the intelligence community has turned to AWS to build a cloud to serve customers across multiple intelligence agencies; that is why commercial companies with sensitive information ranging from financial institutions to healthcare providers are leveraging AWS to meet their digital infrastructure needs; and that is why federal civilian agencies such as the Federal Aviation Administration (FAA), the Department of Health and Human Services (HHS) and

[6] "Why Commercial Clouds are More Secure than Federal Data Centers", *Nextgov.com,* January 5, 2015.

the Department of Homeland Security (DHS) are also moving workloads to commercial cloud providers such as AWS.

Policy Recommendations

Both the Administration and the U.S. Congress have important roles to play to ensure that federal agencies have access to commercial cloud services and the associated benefits. Since joining the Office of Management and Budget (OMB) earlier this year, Federal CIO Tony Scott has been a strong advocate of cloud computing. The President also emphasized the importance of cloud computing in the President's FY2015 Budget Request:

> *Expanding Federal Cloud Computing.*
>
> *The Budget includes investments to transform the Government IT portfolio through cloud computing, giving agencies the ability to purchase IT services in a utility-based model, paying for only the services consumed. As a result of the Administration's Cloud First policy, Federal agencies adopting cloud-based IT systems are increasing operational efficiencies, resource utilization, and innovation across the Government. To accelerate the pace of cloud adoption, the Administration established the Federal Risk Authorization Management Program, a Government-wide program standardizing how we secure cloud solutions. To further grow the use of cloud-based services, the Government is working to establish a credential exchange system that allows citizens and businesses to securely access online services at different agencies without the need for multiple digital identities and passwords.*

Congress has already played a major role in enacting initial IT reforms that are necessary for expanding cloud computing adoption across the federal government. For example, the House Oversight and Government Reform Committee's signature IT reform bill during the 113th Congress was the Federal IT Acquisition and Reform Act (FITARA), bi-partisan legislation that Amazon has been a strong supporter of since its introduction a few years ago. Implementation of FITARA continues to be important for ensuring that procurement and acquisition reforms needed for IT transformation in federal agencies proceed as technologies evolve. We look forward to working with this Subcommittee and our federal customers as changes to IT governance and requirements under FITARA are implemented. In addition to government-wide IT reforms such as FITARA, we recommend other steps that this Subcommittee can take to foster greater adoption of cloud computing across the federal government.

First, given the importance of FedRAMP to federal cloud computing, it is vital to continue to make improvements to the program in order to strengthen it and ensure its effectiveness for years to come. For example, the existing Joint Authorization Board

(JAB) process could be further improved in order to enable more timely authorizations and reduce duplication of assessment effort between the FedRAMP Program Management Office (PMO) and the third party assessment organizations (3PAO) to stay in sync with rapid pace of changes in cloud technology, while also re-emphasizing the role of individual federal agencies to conduct security assessments of CSPs. Under the current construct, individual agencies are able to provide an Authority to Operate (ATO) under FedRAMP – HHS sponsored AWS's FedRAMP ATOs and oversaw the technical assessment in coordination with the FDA, CDC, NIH, and the FedRAMP PMO – so, some federal agencies already have substantial expertise and experience under FedRAMP. Congress should also mandate that CSPs or contractors delivering cloud services to federal agencies should be required to have a completed security assessment under FedRAMP prior to consideration for use.

Second, federal agencies should be given more flexibility to either use existing working capital funds, or to establish new ones, for the adoption of cutting-edge technologies such as cloud computing services. Given that commercial cloud offers an alternative way of offering IT – on demand and based on actual consumption – budgeting and spending models have to evolve too. The old way of doing IT worked well under a capital expenditure model (CAPEX), but the new way of offering IT does not. If federal agencies are going to have more options for paying for only the services consumed as outlined in the President's FY2015 Budget Request, then agencies will increasingly need to be able to acquire these services under operating expenses (OPEX).

Below is legislative language that was previously included in House-passed bills to begin to address these challenges and we believe is a good starting point for additional work in this area:

TRANSITION TO THE CLOUD

(a) SENSE OF CONGRESS.—It is the sense of Congress that transition to cloud computing offers significant potential benefits for the implementation of Federal information technology projects in terms of flexibility, cost, and operational benefits.

(b) GOVERNMENTWIDE APPLICATION.—In assessing cloud computing opportunities, the Chief Information Officers Council shall define policies and guidelines for the adoption of Governmentwide programs providing for a standardized approach to security assessment and operational authorization for cloud products and services.

(c) ADDITIONAL BUDGET AUTHORITIES FOR TRANSITION.—In transitioning to the cloud, a Chief Information Officer of an agency listed in section 901(b) of title 31, United States Code, may establish such cloud service Working Capital Funds, in consultation with the Chief Financial Officer of the agency, as may be necessary to transition to cloud-based solutions. Any establishment of a new

Working Capital Fund under this subsection shall be reported to the Committees on Appropriations of the House of Representatives and the Senate and relevant Congressional committees.

Third, as the September 2014 GAO Report recommended, federal agencies should ensure that all IT investments are assessed for suitability for migration to a cloud computing service. Until the agencies fully assess all their IT investments, these organizations will not be able to achieve the resulting benefits of operational efficiencies, enhancements to their security posture, and significant cost savings. Congress should consider enacting that requirement in legislation this year.

In closing, while much work still needs to be done to enable federal agencies to fully benefit from the utility-based model of cloud computing, significant progress has been made over the last several years. As result, the federal government is reducing costs, providing agencies more agility and flexibility in IT, and critically, is establishing a strong foundation to improve federal information security. In today's budget climate, and following major security breaches of federal government systems in 2015, now is the time to aggressively expand cloud computing adoption.

Thank you for holding this hearing today and I look forward to taking your questions.

###

Mark Ryland

DIRECTOR OF SOLUTIONS ARCHITECTURE AND CHIEF ARCHITECT
WORLD WIDE PUBLIC SECTOR, AMAZON WEB SERVICES

Mark Ryland is the technology leader for Amazon Web Service's Worldwide Public Sector (WWPS) team. Mr. Ryland leads a team of Solutions Architects and Professional Services Engineers who provide AWS technical evangelism, architectural guidance, knowledge transfer, and implementation services to government and education customers around the globe. He also serves as a key interface between the WWPS team and the engineering, security, and compliance teams at AWS, ensuring that public sector customer requirements are front-and-center in cloud service planning and roadmaps.

Ryland has more than 24 years of experience in the technology industry, beginning with Microsoft Federal Systems, where he began his career as a Senior Architectural Engineer in the early 1990s. He continued at Microsoft for ten years, serving in a variety of software engineering, technical management, and technical evangelism roles on projects like Windows Cairo, Windows NT 4.0, COM/DCOM/OLE, XML/RPC and SOAP, and others. In the late 1990s he started and ran the first standards organization at Microsoft, serving as Director of Standards Strategy until he left Microsoft in 2000. Subsequently, Ryland served as CTO of two start-up companies, as well as Vice-President and Director of the Washington DC office of a Seattle-based public policy think-tank. He rejoined Microsoft in 2008 as National Standards Officer for the USA, later switching back to an engineering role as a principal program manager in Microsoft's identity and access team, where he worked on Active Directory, Office 365 directory, and the Azure Access Control Service.

Ryland joined the AWS WWPS team as Chief Architect in September 2011, bringing a rich set of software engineering, distributed systems, cyber security, technical evangelism, and tech policy skills to the team.

More information on Ryland can be found at http://linkedin.com/in/markryland.