Statement for the Record

Alan Boissy

Program Director, Government Cloud Services

VMware, Inc.

Before the

U.S. House of Representatives

Committee on Oversight and Government Reform, Subcommittee on Information Technology

The State of the Cloud

September 22, 2015

Chairman Hurd, Ranking Member Kelly, thank you for the opportunity testify today at this important field hearing. I am Alan Boissy, head of VMware's Government Cloud offering for the federal government. I have over 15 years experience working on information technology programs for the federal government and have led two Fortune 500 companies through the FedRAMP process to receive government certification for Cloud.

My employer, VMware, is the fourth largest software company in the world, with 2014 revenues of over $6 billion and over 18,000 employees. VMware has more than 500,000 customers and 75,000 partners, including 100 percent of the Fortune 100. VMware serves all sectors of the U.S. Federal Government, the Civilian agencies, the Department of Defense, and the Intelligence Community as well as state and local governments. The company is headquartered in Silicon Valley with 140 offices throughout the world.

VMware enables organizations to thrive in the cloud era by transforming the way they build, deliver and consume IT resources. Leveraging VMware's virtualization technology, which exists in over 90 percent of the government's data centers and is the most widely deployed foundation for cloud computing—VMware enables enterprises to adopt a cloud model that addresses their unique business challenges.

What's Driving Cloud Adoption

As the Committee has noted in their request for this important hearing, the federal government is currently under several mandates that dictate the movement to the cloud. The growing adoption of cloud is driven by the need to respond faster and with more agility in an effort to increase bottom-line efficiency. Although just 30% of data center workloads are cloud-based today, IT managers expect that number to rise to more than 50% within two years[1].

[1] 2015 study by IDG Research of 1000 IT managers at enterprise-class organizations

More and more organizations understand the basic benefits of what cloud computing represents. In fact, in a recent International Data Group (IDG) survey of over 100 companies, 64% stated cost efficiencies gained from consolidating IT systems and infrastructure as a key driver of adoption, while 57% cited speed of deployment and improved agility as most important[1]. Federal agencies are seeing and also experiencing the increased agility that their IT can achieve in meeting demands by moving to more dynamic forms of IT infrastructure. With flat, or decreasing federal budgets, IT is continuing to look to new innovations to optimize the limited resources they have. And, because large, static capital budgets are more and more difficult to justify and secure, organizations are looking to reduce those costs and replace them with more flexible and affordable usage-based operating expenses. Overall, the cloud promises to make IT more adaptive, cost effective and accommodating in providing IT services.

As the Subcommittee is aware, there are four definitions that National Institute of Standards and Technology (NIST) that cover the different cloud deployment models used today:

1. **Private cloud.** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. The federal government has a high rate of private clouds that due to the sensitivity of the information, they would never consider migrating away from this architecture.
2. **Community cloud.** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. An example of this could be a Department of Homeland Security Cloud where the component agencies of the Department all share space.
3. **Public cloud.** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or

government organization, or some combination of them. It exists on the premises of the cloud provider. This has been the primary cloud model used in the federal government today.

4. **Hybrid cloud.** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability. This allows agencies to move workloads back and forth to-and-from the cloud in times when extra capacity is needed; the same need as a retailer like Columbia Sportswear or the United States Postal Service who might have during the busy holidays.

Challenges in Federal Government Adoption

To date, there have been a number of challenges that keep government agencies from embracing and implementing cloud adoption:

1. **Meeting federal security requirements:** Cloud service vendors may not be familiar with security requirements that are unique to government agencies, such as continuous monitoring and interpreting industry specific regulatory requirements.
2. **Acquiring knowledge and expertise**: Agencies may not have the necessary tools or resources, such as expertise among staff, to implement cloud services that align to current application architectures such as email or human resource (HR) portals. Often the challenge isn't the understanding of what can or should move to the cloud, but more importantly what should not or cannot move to the cloud.
3. **Incompatible infrastructures**: Many cloud providers use platforms that are inconsistent with current and legacy infrastructures. Some cloud efforts can create redundancy and interoperability challenges that require manual processes, changes to application architectures and use of new tools. A common path for cloud migrations is to build a new parallel cloud environment that mirrors the current on premise legacy system with the intent of transitioning the applications over to the cloud. Before the actual transition, the agency will be paying for two

environments which can add significant costs to an already strained budget requirement. This presents a very real problem that has faced several agencies in their cloud migration plans, one that can be addressed by implementing a phased hybrid cloud approach.

4. **IT Barriers to Change: Overcoming cultural barriers:** Agency culture may act as an obstacle to implementing cloud services. Due to long standing processes, frameworks and tools, many IT staff are culturally resistant to change due to unfamiliarity with many cloud provider platforms. IT staff may be culturally resistant to change as they look at cloud as an unnecessary disruption to best practices that are currently successful in supporting short-term strategies. Cloud migrations represent a disruptive shift in platform and technology, requiring agency workforce to learn new skill sets, new operational models and new design expertise.
5. **Ensuring data portability and interoperability:** To preserve their ability to change vendors in the future, agencies may attempt to avoid platforms or technologies that "lock" customers into a particular product. In addition, many of the cloud service provider platforms do not seamlessly support bi-directional data migration or interoperability between the data center and the cloud environments.

The benefits of cloud migration are often impeded with concerns over data security in multi-tenant environments or potential impacts to compliance related requirements. The Federal Risk and Management Program (FedRAMP) was instituted in June 2012 to allay agency security concerns by requiring cloud service providers to adhere to a defined set of security and governance standard based on the NIST Special Publication 800-53 version 3 *Security and Privacy Controls for Federal Information Systems and Organizations.*

Government agencies should look to balance this equation and lower the risk of the adoption of cloud-based service delivery by investing resources to determine a clear path forward utilizing existing government guidance, a comprehensive understanding of their current environments and leveraging the security baseline offered by the FedRAMP initiative.

VMware believes there are several best practices that the government should consider when transitioning to the cloud.

1. Assess what applications should move to the cloud

When federal agencies are first considering a move to the cloud, the first step should be a complete assessment of their current application landscape such as email, databases, web portals, etc. Agencies must decide what applications would be good candidates from both an architecture and security approach. Success often hinges on selecting the best application and use cases that translate and leverage cloud technologies.

The best use cases include development/test environments; disaster recovery/business continuity scenarios and hardware refresh cycles that focus on making sure that agencies don't have too much hardware for their current needs. Some applications, including mainframes or databases that require a colocation of onsite data with onsite users to address performance or security concerns, are not good candidates for cloud migrations and can often complicate and frustrate initial cloud migration and IT transformation efforts.

Above all else, the migration to the cloud should be a business decision in addition to an IT decision. If the move to cloud cannot demonstrate a clear and definitive realization of cost efficiencies and a transition from owning infrastructure and hardware to a utility consumption service model, then agencies cannot claim success.

Moving to the cloud for the sake of answering the call for the Cloud First mandate can have disastrous consequences and actually cost the agency more money than the promise of efficiencies that the cloud is supposed to deliver. Developing a cohesive strategy and adhering to a clear and concise migration plan will necessitate an understanding of the various initiatives of the mandate as well as some of the underpinning efforts such as the Federal Data Center Consolidation Initiative. Understanding how each application migration to the cloud not only addresses and satisfies these efforts but ultimately demonstrates the business advantages are the keys to success.

These are representative of the building blocks of a migration strategy and provide important elements that guide the goals of a plan. These will also help define the success criteria that will allow the measurement of progress.

2. Expandable platform

Cloud platforms today have to support diversity in how services are developed, provisioned, consumed and architected across infrastructures. Applications built on and for the cloud still have integration dependencies to on-premises services such as access to data stored in the data center or to maintain continuity of access controls. Workloads cannot afford to be "landlocked" by proprietary platform boundaries that require repeated conversions to enable any degree of portability.

For example, many cloud environments require application changes before those applications can operate effectively on those platforms. Additionally, in the case where those applications may need to be moved back into the data center, those same applications would need to be changed again before being moved back. This limits convenience and introduces cost and lead times in keeping these applications available.

Incompatibility with backup systems, both onsite and in the cloud, can impede business continuity. In these cases, separate and incompatible cloud environments can break backup and recovery processes between the data center and the cloud, rendering them ineffective. Seamless end-to-end service fulfillment needs to happen regardless of the infrastructure boundaries between users, applications and data. Proprietary cloud platforms are not natural extensions to the data center and create disruptions to the processes and workflows that leverage applications to unite a user with the data they need.

Agencies must view cloud adoption holistically and not simply as an IT decision

Because cloud migration is a change in how the agency conducts its business, agencies must involve multiple functions to truly be effective, and not just IT. Contracting Officers, Budget Officers, Mission Directors, Privacy Officers, Executive leadership and

even front line Application Developers all have a vested interest in how cloud services are adopted.

For example, government procurement processes rely on predictable pricing and costs to conform with long standing government budget frameworks. The actual procurement of hourly based services present a host of compliance and contractual issues and rarely fit into the current contract vehicle mechanisms available to the Contracts and Procurement offices. Developers with credit cards might inadvertently commit government funds to efforts that will challenge budget and cost containment boundaries.

Cloud services are increasingly available as self-service, self-procuring, pay as you go cost models which require shorter term and more frequent budget assessments, and many of these self-service options can enable agencies to bypass traditional IT acquisition processes. This type of acquisition can have a broad impact on how these services are chosen, budgeted, procured, implemented and maintained from a pricing, licensing and deployment perspective. Additionally, both Security and Privacy offices need to be aware of the impact of moving data and applications to the cloud. Data residing in the cloud is always the responsibility of the agency; these departments need to be involved in the earliest stages to ensure compliance and to protect the agency data and mission.

Cost predictability involves procuring services on a consumption (on-demand) basis. Because of the on-demand, scalable nature of cloud services, it can be difficult to define specific quantities and costs. These uncertainties make contracting and budgeting difficult due to the fluctuating costs associated with scalable and incremental cloud service procurements. With traditional software purchases, for example, an agency may purchase a term license of a software product for a predefined cost that includes ongoing annual support and maintenance. In an on-demand cloud service model, a user may acquire the service as a monthly subscription, but the month-to-month cost of that subscription could vary greatly based on the metered use or consumption of that service. This creates uncertainty from a budgeting standpoint.

3. Hybrid loud for the federal government

Agencies have a variety of evolving needs and are at different points in their purchase cycle and journey into the cloud. The public cloud enables agencies to address a common challenge of having limited IT budget and staffing in the face of growing demand for services. Investing in traditional hardware and software for servers, storage, networking and security is no longer a viable option. Unfortunately, many agencies have experienced cost overruns in their early cloud migration projects and, in other cases, limited savings. According to a GAO report in 2014:

"Agencies reported that they had cost savings from implementing 22 out of 101 cloud computing services through fiscal year 2013. Specifically, they collectively saved about $96 million by implementing these 22 services."

That represents only about 22% of these implementations actually resulting in savings. The report cites two reasons for the lack of savings: "a motivation for changing to some of the cloud-based services was not to reduce spending, but to improve service." "In selected cases, the cloud computing service opened up a new service or provided a higher quality of service; while this provided useful benefits to the agency, the associated costs negated any savings."

Government cloud services should not require costly reconfigurations or additional coding just to move government applications such as email or databases to the cloud. Agencies should be able to continue to leverage the existing tools they already use to manage and administrate workloads onsite and manage them the same way in the cloud.

Using the government's existing investments

Most successful cloud migrations evolve from on-premise solutions to hybrid cloud implementations to multi-cloud systems. Enabling agencies to maximize their existing architecture, IT skillsets and personnel to minimize and mitigate cloud migration risks is an attractive path for agencies to take. In fact, these "soft" costs that do not immediately appear on spreadsheets can include labor overruns for re-engineering efforts, additional

license procurement and duplicative software purchases. Often these are the costs that can derail migration efforts before they are green-lighted for production.

What if an agency could meet the inconsistent and fast paced demands placed upon its data center in a way that was as easy and convenient as renting a car? Almost everyone owns, operates and maintains an automobile. But if someone were traveling on business to another city, no one would buy a new car for the few days it was needed. Instead, someone would rent a car for those few days because your demand for transportation is temporary. Demand for data center capacity is also sometimes temporary. And, increasingly, that demand is very inconsistent in terms of when and how much resource is required. This volatility of demand coupled with the need for greater cost flexibility and service diversity is driving the popularity of cloud-based services.

However, even though many of the more popular public cloud providers have been excellent sources of instantaneous infrastructure availability, the net result has been multiple incompatible environments connecting to data center - each with their own set of tools, processes and skill sets for management, networking and security. In a sense, they have been renting cars that can't be conveniently refueled at any of the thousands of standard filling stations, can only be operated on certain roads and highways and can only be purchased as a one way rental to your destination, but with no return option.

Instead, agencies should look to incrementally extend their data center in a way that builds out scalable and resizable capacity in a consistent, compatible and transparent way.

Hybrid cloud's portability

A Hybrid cloud environment is the deployment of a common set of applications, tools, and services across a multi-cloud environment that allows for the unencumbered portability of applications and data across that environment. An example might be extending an email application to run in the cloud to achieve greater and more cost effective scalability, but continuing to run the processes that authenticate user access directly from the existing onsite data center.

Hybrid Cloud is, by design, the extension of traditional onsite data center resources to the public cloud. This extension requires a consistent and universal hybrid cloud platform that leverages the same core technology that agencies already use to run these data centers. This environment requires a consistent security model, seamless access to data and unified management that allow agencies to extend the same staff skills, processes, and workflows, established in their own data centers, to the cloud, on demand. This model is the foundation for cost savings in cloud migration.

Consistent Management: Many proprietary cloud platforms introduce new management tools and new processes to maintain and operate a separate cloud-based service infrastructure that would be mutually exclusive to the existing data center. This approach would introduce a level of change and redundancy resulting in additional risk and costs that would negate any associated benefits.

Hybrid management removes the IT dependency on non-IT users while still preserving centralized IT oversight and control of security, compliance and cost. With self-serviceability of cloud services, users can be authorized to create their own workspaces as needed without the need to manually request those services from IT while maintaining the ability to centrally manage the security and governance of those resources with complete oversight.

4. How to maintain security in the transition to the cloud

Concern around security, privacy and availability of critical data is the #1 barrier to adopting public cloud. IT organizations are required to sustain strict adherence to security policies and regulatory controls making it harder for them to adopt public cloud.

While the agile scalability of cloud-based infrastructure services continues to capture the imaginations of more and more businesses, one barrier is addressing concerns around security and compliance. The perceived risks of moving to a shared, off-premise cloud can stall the progress of many would be public cloud adopters. More specifically, agencies are primarily concerned with losing the ability to control and govern the confidentiality, integrity and availability of data. This perceived loss of control is further

reinforced by headlines riddled with examples of data breaches and service disruptions. The bottom line is that businesses trust their ability to secure their own onsite data center over offsite cloud systems by a wide margin.

However, the most recent cyber attacks have all occurred at on premise data centers, none were in the cloud, including the Office of Personnel Management, US Postal Service, and the Department of State. Studies of the root cause of each of these breaches illuminate gaps and failures in governance, policy/procedure and employee training rather than technical deficiencies in the platform and architecture of the applications.

Trusted security in the cloud is achieved through the partnership of shared responsibilities between the agency and provider. The provider secures the underlying infrastructure of the data center location with tenancy isolation, timely vulnerability patches, user access controls, and documented certifications and audits. The provider takes on the responsibility of securing the data center as to who has access to what, that the servers are patched for any known vulnerabilities and that the environment is monitored for any hacker attempts or inappropriate activities.

Agencies continue to own and operate the security and compliance of the actual workloads by extending their successful policies and controls to their offsite public cloud locations. The government has placed security baseline control sets on cloud service providers and enforced continuous monitoring to alleviate agency concerns over security in the cloud.

The FedRAMP program levies a comprehensive and rigorous security regimen on authorized cloud service providers to augment and reinforce existing agency security postures. One of the pillars of the FedRAMP initiative is to increase IT governance outside of technological innovation by requiring stringent management and policy driven practices bounded by a continuous monitoring requirement.

Trusted partners now offer increased innovations, best practice implementation reference architectures and purpose-built virtual appliance delivery methods to increase the manageability and consistency of security across a hybrid infrastructure. For example,

partners provide the same solutions that agencies may already use in their data centers, and improve those solutions to make them operate either as good or better in a cloud environment.

Encryption is a good example of improved technology in a cloud environment. In many cases, encryption technology can be made portable so that, once data is encrypted, the protection will stay in place regardless of where that data is moved or resides either in the data center or the cloud. This partnership empowers agencies to achieve increased effectiveness in their ability to mitigate risks to their data sets in the public cloud.

Security best practices

Security standards have long been pursued by IT organizations as the most effective way to not only save on cost, but to mitigate risk by reducing the number of change variables. One of the key principles of any security framework is to establish consistency in policies and controls. As data security continues to be among the primary concerns of public cloud adoption, many cloud service providers force Security Operations teams to re-think and re-architect how they do security. By introducing proprietary platforms that are mutually exclusive to existing data center constructs, these providers require Security teams to create new policy and control frameworks that are inconsistent with how they manage and secure their existing infrastructure.

Today, multiple agencies are interconnected at various operational levels to facilitate the sharing of business systems information and/or to provide interagency support to meet common mission objectives. FedRAMP acts as a common denominator and reference point for cloud specific security guidance.

Eventually, all cloud security baselines will mirror and confluence to the controls rooted in the common NIST framework FedRAMP encompasses. The management and operational aspects of the FedRAMP designation can serve to ameliorate many of the common attack vectors of recent cyber incidents.

Address the threat – immobilize the attacker

The recent attacks on our Government that have gained public visibility have had one thing in common: the attacker, once inside the network's perimeter security, was able to move freely around the target environment. Traditional perimeter-centric security systems are structurally designed to be "doors" to the network. In order to effectively prevent an Attacker from moving freely around the network, agencies must close those doors and compartmentalize their networks by creating "Zero Trust" network environments within the data center.

New innovations allow greater isolation of data with protections that surround the data instead of just surrounding the entire network. This is commonly referred to as "micro-segmentation." Micro-segmentation restricts an attacker's ability to navigate the data center, even after the perimeter has been breached. This concept is similar to a bank robber potentially getting through the vault door in the bank only to find valuables secured in distributed safety deposit boxes, each with their own lock. These types of protections become significantly more important as agencies look to cloud migration strategies that extend the perimeters of traditional data centers.

Public cloud providers should have completed rigorous independent third-party examinations for key compliance certifications. Providers should always be invested in keeping up with the latest and greatest criteria as the standards change and audit reports for these programs should be available for agency review.

Summary

Agencies should look to incrementally extend their data center in a way that builds out scalable and resizable capacity in a consistent, compatible and transparent way. In doing so, the applications and data an agency runs today and builds tomorrow can easily run seamlessly onsite in the data center, offsite in the cloud or in any combination. Success in migrations to the cloud are based on the ability of an agency to maximize and leverage its current IT investments and environment and minimize the risks associated with the transformation of their systems from a security, financial and operational standpoint.

Whether an agency builds out a private cloud or moves directly to a public hybrid cloud, it should be able to run any application or workload, on any operating system, anywhere it best served its needs. Agencies should be able to leverage the same tools they currently use to manage data and applications, same network configurations and constructs that allow users to access the various networks they need to access and same processes, such as security monitoring and system maintenance.

VMware sincerely appreciates the opportunity to share our thoughts and best practices on this very important matter. We applaud the leadership and vision of the Chairman and Ranking Member for holding this field hearing. VMware looks forward to continuing to participate in efforts to improve the efficiency and security of the federal government.

Alan Boissy Bio

Alan Boissy is the Product Line Manager for the VMware VCloud Government Service FedRAMP offering. He has over 20 years experience in IT with a specific focus on federal government and cloud computing, having served as the subject matter expert for federal cloud computing for both VMware and Lockheed Martin where he was the Program Manager for the FedRAMP SolaS Federal Cloud offering since its inception. In addition to his Program Manager role at Lockheed, Alan served as the top resource for Lockheed Martin contracts and programs for discussions with government agencies about the Cloud First Policy and the Shared Services Strategy. He has participated in numerous panels, discussions and radio interviews on the subject and spends a great deal of time working with high level government IT to determine challenges, adoption strategies and overall cloud guidance based on his experience in the field. He has seen firsthand many of the challenges facing the government today in actual cloud deployments and IT transformation planning including technological, philosophical, financial and strategic blockers to achieving the government's Cloud First Mandate. He graduated from Boston University with a degree in 1992.