Written Testimony

of

Mark Kneidinger

Director, Federal Network Resilience

Office of Cybersecurity and Communications

U.S. Department of Homeland Security

Before the

U.S. House of Representatives

Committee on Oversight and Government Reform

Regarding

The State of the Cloud

Introduction

Chairman Hurd, Ranking Member Kelly, and members of the Committee, thank you for the opportunity to appear before you today to speak on "The State of the Cloud." The Federal government understands the valuable attributes that the cloud offers to agencies. At the same time, the Department of Homeland Security and our partners across the federal government realize that the cloud introduces new complexity to ensure adequate security controls. Further, the cloud introduces new challenges to ensure that agencies maintain visibility into their cloud assets and appropriately exercise their responsibility and due diligence in protecting those assets. Through Administration initiatives as "*Cloud First"* and "*Share First,"* Federal agencies were early adopters in leveraging the cloud to gain efficiencies. These efficiencies include, but are by no means limited to, commodity IT support such as website management, e-mail, help desk, and collaboration tools. Through these early engagements, agencies had a wide range of successes and challenges, from which many lessons have been learned. Building upon these experiences, the Federal government is furthering expanding its use of the cloud for new applications and services. Foundational to this expansion is the ability of individual agencies to establish contractual relationships with Cloud Service Providers (CSPs). The shift to CSPs allows the federal government to apply best practices derived from previous lessons learned, including clearly delineating role/responsibilities of both the CSP and the agency, providing necessary agency visibility to ensure implementation of appropriate security controls, and flexibility for transitioning or terminating cloud resources with minimal impact on the agency's mission.

In this testimony, I will discuss the primary impetus that has led to agency adoption of the cloud, summarize characteristics of lessons learned, highlight key roles and responsibilities

for agencies in leveraging the cloud, discuss current state of the cloud within the Federal government and conclude with approaches to further expand cloud implementation.

Kick-starting the move to the cloud

The primary drivers for adopting cloud computing across the federal government include:

- Mission Alignment: the need for alignment between mission and IT and the need for a mechanism to measure this alignment;
- Agility: responsiveness and flexibility to meet changing mission requirements
- Reduced Costs: through standardization, consolidation, and automation of IT services, processes and tasks;
- Security: improving information assurance posture, streamlining risk mitigation, and addressing regulatory requirements by centralizing and enforcing processes
- Economies of Scale: Utilization of the consumption model, without the ownership of costs and risks
- Limited Resources: capital budget constraints leading to increased efficiencies to be gained by a "Cloud First" model

Based upon these attributes, the Administration codified the "*Cloud First"* policy in 2010 with the 25 Point Implementation Plan to Reform IT Management. This Plan encouraged each agency Chief Information Officer (CIO) to identify three services to move immediately to the cloud and create a project plan for migrating each to cloud solutions and retiring the associated legacy systems. Of the three identified services, at least one was required to be fully migrated to a cloud solution within 12 months, and the remaining two were required to be moved to the cloud within 18 months. The Plan focused on migrating services to the cloud and retiring legacy applications, rather than migrating applications to the cloud as an end in itself.

The Federal "*Share First"* policy provided agencies with guidance on identifying, implementing, and operating shared services for commodity, support, and mission IT functions. This policy included in the aforementioned 25 Point Implementation Plan to Reform Federal IT Management and emphasized increasing return on investment (ROI), eliminating waste and duplication, improving the effectiveness of technology solutions, and reducing costs through shared approaches to program activities. The implementation activities were focused accelerating a broad transition intra-agency shared IT services. By March 1st 2012 agencies were asked to:

- Develop a shared services plan that included, at minimum, two commodity IT areas for migration to a shared environment (cloud).
- Establish benchmark metrics to measure quality and uptake of services provided.
- Develop a roadmap for modernization and improvement of existing services considering similar approaches.

As a first principle, an IT shared service is defined as an information technology function that is provided for consumption by multiple organizations within or between Federal Agencies. This definition generally includes three categories of IT shared services that can be delivered through cloud-based infrastructure: commodity, support, and mission. Examples include:

- Commodity IT: Websites & Content Management, Infrastructure & Asset Management, E-mail, Help Desk & Collaboration tools
- Support IT: Records management, HR management, Financial Management
- Mission IT: Performance management, Geospatial, Federal Health architecture

The "Cloud First" and "Share First" polices were promulgated widely across the federal government and catalyzed the rapid adoption of cloud computing services across the federal IT landscape. In particular, the "Cloud First" policy further reinforced this transition to cloud

computing by requiring that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option existed.

Lessons Learned

The rapid adoption of cloud computing as called for in the "*Cloud First"* and*" Share First*" policies exposed a number of challenges with implementing, deploying and using cloud environments. The primary challenges including security, interoperability, and portability. Secondary challenges included optimization of resource utilization and integration of cloud systems management with business processes.

The most consistent lessons learned through this early adoption were captured and represented in a joint publication in 2012 between the federal CIO Council and Chief Acquisition Officers (CAO) Council entitled *Best Practices for Acquiring IT as a Service*. A central premise of this publication was recognition that cloud computing presented a paradigm shift that was much more expansive than IT. In so doing, the CIO and CAO Councils highlighted substantive issues that needed to be addressed in updating business and contracting models when applied to cloud services. This new paradigm required agencies to re-think how they acquired IT services in the context of deployment, as well as how the IT services they consume provide mission and support functions on a shared basis while meeting critical security requirements.

Based on the CIO and CAO Council study, the federal government gained a renewed focus on contracting and security, and yielded a series of recommendations and best practices when acquiring cloud computing services. These included:

- CSP end-user agreements and term of service need to be integrated fully into cloud contracts.

- Service Level Agreements (SLAs) need to define performance with clear terms and definitions, demonstrate how performance is being measured, and the specific enforcement mechanisms that are in place to ensure SLAs are met.

- Delineation between the responsibilities and relationships among the Federal agency, integrators, and the CSP.

- Use of the NIST cloud reference architecture and associated security controls.

- The need for agencies to clearly detail requirements for CSPs to maintain the security and integrity of data in a cloud environment.

- The need for agencies to adequately identify potential privacy risks and responsibilities within CSP contracts when the cloud services host “privacy data”.

- The importance of assuring that data stored in a CSP environment is available for legal discovery.

More recently, DHS has sponsored agency forums to build upon the earlier government-wide reports and analysis. Key focus areas of these fora include:

- Incorporation of data governance and data security controls

- Protection from Distributed Denial of Service (DDoS) attacks

- Assuring supportability from the service provider

- Determining liability management in the event of a security breach

- Availability and accessibility of data in the case of a disaster

- Contingency and survivability in the case that the Shared Service Provider ceases operations
- Confidentiality and restrictions on who has access to data
- Privacy and the Fair Information Practice Principles (FIPPs)
- Storage location for data and applications and Continuity of Operations (COOP)
- Management of data and data remnants

In December, 2011, the Federal CIO Council published a new policy document entitled: "*Security Authorization of Information Systems in Cloud Computing Environments."* This policy details the responsibility of the Federal Risk and Authorization Management Program (FedRAMP). The mission of FedRAMP is to provide agencies with a unified way to secure cloud computing services through the use of a standardized baseline set of security controls for authorizing cloud systems. FedRAMP was developed in collaboration with NIST, GSA, DOD and DHS. Although agencies continue to retain the responsibility for ensuring appropriate risk management of their systems and information, FedRAMP defines the unique security requirements of cloud computing that CSPs are required to adopt.

That said, even with substantial lessons learned and unprecedented support from DHS and organizations such as FedRAMP, adoption of agency cloud computing continues to have inherent security complexity. Key issues include effectively measuring, monitoring, and evaluating the security of the cloud environment, which diverges from the formerly cohesive system-controlled environment that was previously well-understood. Instead, cloud computing distributes the components, communications links, data repositories, authorities, responsibilities, and personnel outside of the organization's typical physical boundaries. When considered in

addition to the complexity of cloud computing systems that support multiple missions, the need for security and segregation of data becomes even more critical.

Cloud risk management

A key element to successful implementation of cloud computing is a security program that addresses the specific characteristics of cloud computing and provides the level of security commensurate with specific needs to protect government information. Effective security management should be based on risk management and not only on compliance. By adhering to a standardized set of processes, procedures, and controls, agencies can identify and assess risks and develop strategies to mitigate them.

Risk management for government assets in the cloud increases as the agency migrates across the three Cloud computing service model, described below:

- Infrastructure as a Service (IaaS): the provision of processing, storage, networks and other fundamental computing resources.

- Platform as a Service (PaaS): provisioning ability to deploy on to the cloud infrastructure consumer-created or acquired applications.

- Software as a Service (SaaS): the capability to run applications on a cloud infrastructure where the application is accessible from various client devices through a thin client interface such as a web browser.

In a tradition non-cloud environment, each agency maintains responsibility for the application, data, middleware, operating system, servers, storage, virtualization and networking. As an agency migrates to an IaaS service the agency 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. Further migrating to a PaaS environment, the agency 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 the configuration of the application hosting environment. With migration to a SaaS, the agency 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.

As agencies have less direct visibility into the risk management of their assets as they progressively leverage the broader capabilities of the cloud environment, due diligence in ensuring that appropriate security controls are administered becomes more critical. During the early adoption of the cloud, agencies learned important lessons regarding the division of roles and assumed expectations of the CSPs and the degree of complexity inherent in migrating to the cloud.

Key Agency Considerations

Considerations for agencies as they become more dependent upon the CSPs, lessen their direct control of assets within the cloud environment, and need to balance risk mitigation practices include:

- The ability to monitor how changes in policies that control allocation of cloud computing resources impact the performance of mission critical applications as measured from end-users' perspective. This ability allow agencies to more fully reap maximum benefits from the deployment of cloud computing;

- Capabilities that allow agencies to measure key performance indicators for application performance in both cloud and internal environments. By defining proper benchmarks for evaluating performance of cloud services, agencies will better understand the implications of making changes in their IT management strategies and the value thereof;

- Ability to monitor actual levels of performance as experienced by mission application users and enable them to conduct root cause analysis of problems as they occur.

Current state and way forward

In 2015, many agencies are using cloud computing in a similar manner as in 2010, with a particular focus on commodity IT rather than mission IT. This is due in large part to the complexity of obtaining necessary visibility into the appropriate security of agency mission assets. Further, agencies remain wary as to their ability to effectively support an application migration to the cloud given potential budget uncertainties once the migration begins, and potential risks in re-platforming or re-architecting an application for a transition of this type.

In February, 2015, DHS conducted a data of federal agencies as part of the Department's Trusted Internet Connection program. This data call identified that CFO Act agencies have implemented 32 IaaS, 24 PaaS and 77 SaaS instances. Of those instances, the majority of services were for email, CRM, sharepoint, case management applications, collaboration tools, web hosting and help desk capabilities, with few instances where agencies had migrated high-value applications.

However, agencies will demonstrate increased interest in further migrating services and applications as CSPs provide increased visibility in the risk management approach provided to

secure agency assets. To move beyond interest to implementation, agencies and CSPs must address challenges in preparing applications for migration, especially given the potential increased costs that may be incurred for re-architecting legacy applications. Given uncertain budgets and the inevitable loss of critical staff with unique skill sets in managing legacy applications, agencies will be further challenged in implementing these transitions

But the federal government is aware of these challenges, and is responding. As part of our Continuous Diagnostic and Mitigation Program (CDM), DHS has initiated a partnership with FedRAMP to develop p recommendations in defining additional security controls in establishing a High Confidentiality, High Integrity and High Availability (HHH) cloud environment. This environment, in turn, will be used to provide CDM services for .gov agencies within a cloud. FedRAMP has currently published these added security controls for public comment. Upon adoption of the HHH baselines security controls, CSPs may offer an environment that is more compatible with legacy mission applications otherwise deemed not transferable to current cloud platforms.

DHS is also considering approaches for reducing the technical risk and costs of cloud migrations, particularly regarding identification of common work patterns or system modules that may be divided into components and offered in a cloud environment. This effort would allow common interface capabilities for legacy applications to be constructed on a one time basis rather than having development duplicated across multiple similar legacy applications. This investigation is at a very early stage, but DHS is focusing on identifying candidate applications for migration and transitioning those applications to a highly disciplined, risk-aware process cloud environment.

In sum: the federal government has already benefited from a widespread migration of commodity IT to the cloud. As agencies gain increased visibility and confidence in the security controls offered by CSPs, this migration will accelerate. DHS is working urgently with FedRAMP, the CIO Council, individual agencies, and CSPs to ensure that this transition maximize benefits for federal agencies and the American taxpayer while ensuring the security of sensitive information and critical government services.

Mark Kneidinger

Director, Federal Network Resilience
U.S. Department of Homeland Security
Arlington, VA 22201

Office: (703) 235-3938
Mobile: (202) 236-4173
Fax: (703) 235-3650
Email: mark.kneidinger@hq.dhs.gov

Mark Kneidinger is the Director of the Federal Network Resilience (FNR) Division, within the Department of Homeland Security's Office of Cybersecurity & Communications. In this position, Mr. Kneidinger leads FNR's activity in developing innovative approaches to drive change in cybersecurity risk management across the federal government working in collaboration with OMB, the CIO Council and individual agency CISOs. Prior to joining DHS, Mr. Kneidinger held leadership positions in the commercial sector, including as Vice President and Managing Partner. Mr. Kneidinger has further held Chief Information Officer (CIO) positions in New York and Virginia as well as served as a White House appointee in the position of Deputy Assistant Administrator and CIO for the U.S. Agency for International Development (USAID).