Government Contracts Advisory

FEBRUARY 28, 2011

CONTACTS

For further information regarding the topic discussed in this update, please contact one of the professionals below, or the attorney or public policy advisor with whom you regularly work.

Elizabeth A. Ferrell
202.496.7544

Erin B. Sheppard
202.496.7533

Cloud Computing Strategy Signals Fundamental Shift in Federal IT Policy

On February 8, 2011, Federal Chief Information Officer ("CIO") Vivek Kundra released the **Federal Cloud Computing Strategy** ("FCCS" or the "Strategy"), which identifies an estimated $20 billion of the $80 billion currently spent by the federal government on Information Technology ("IT") as a target for migration to cloud computing. The FCCS marks a crucial first step in implementing the federal government's "Cloud First" policy, originally articulated in **OMB's 25-Point Implementation Plan to Reform Federal IT Management** (issued in December 2010), by providing a framework for federal agencies' migration to cloud solutions. The Strategy highlights cloud computing benefits and trade-offs; provides a decision framework for assessing migration options and priorities; identifies various cloud computing resources; and discusses the federal government's role in the development of cloud policies, standards, and procedures.

The FCCS demonstrates the importance of the cloud to both the public and private sector. Cloud computing applies economies of scale to IT infrastructure resources by pooling and sharing resources across large numbers of applications and organizations. This shift from traditional IT infrastructure and toward cloud computing will require organizations to move away from substantial and often underutilized investment in locally owned and operated applications, servers, and networks and toward a more innovative vision of IT in terms of services, commoditized computing resources, and agile capacity provisioning tools. The FCCS explains the three service models for cloud computing, as defined by the National Institute of Standards and Technology ("NIST") — software as a service ("SaaS"), platform as a service ("PaaS"), and infrastructure as a service ("IaaS") — and explains how transformation to one or more of these models "can yield tremendous benefits in efficiency, agility, and innovation" by better utilizing existing assets, eliminating duplication of resources, improving service responsiveness, and increasing innovation while reducing risk.

Consistent with the Cloud First policy, each federal agency CIO must identify three "must move" IT services and develop associated migration plans. The Strategy provides a decisional framework for selecting, provisioning, and managing agencies' migration to a more innovative, secure, and efficient IT infrastructure.

First, the FCCS provides guidance on how agencies can identify high value, low-risk components of their current IT portfolios as first movers to cloud solutions. In assessing the availability of commercial or government cloud computing solutions and alignment with agency needs, agencies will consider (among other things) security, service, market, infrastructure, and readiness factors. Agencies will need to consider Federal Information Security Management Act ("FISMA") and other security requirements, such as Federal Information

Processing Standards, authorization to operate requirements, and vulnerability and event monitoring requirements. NIST is responsible for working with the public and private sectors, leading the development of standards for security, interoperability, and portability for cloud computing in both sectors, and ensuring that these statutory and regulatory requirements are satisfied. Accordingly, both government and industry should closely monitor NIST guidance in these areas.

Second, from a procurement standpoint, the FCCS encourages federal agencies to move away from commodity-focused IT acquisition (based on numbers of servers and physical infrastructure) and adopt a service-based, performance-driven purchasing paradigm. Specifically, the FCCS stresses the need for contracting programs that: minimize the risk of vendor lock-in; ensure portability; encourage competition; include explicit service level agreements; protect continuity of operations; and satisfy individual agency service needs. The Strategy advocates the use of performance metrics and express contract requirements to implement a performance-driven provisioning system. Finally, the FCCS emphasizes the importance of effective contract and program management, and reiterates the importance of performance metrics, service level agreements, and performance evaluations in such a management framework.

The initiatives described in the FCCS will have widespread impact on public and private sector IT programs. The Strategy highlights six key areas for continued, government-wide development of policies, standards, and procedures that will inevitably shape how both public and private sector customers accelerate cloud migration while mitigating risk. These focus areas include:

Encouraging government-wide collaboration. The FCCS encourages agencies with experience in cloud computing to continue providing practical guidance on issues related to security, procurement, and standards. Such knowledge centers currently exist within OMB, NIST, the General Services Administration, the Department of Homeland Security, and the Federal CIO Council, and these entities will continue to play a vital leadership role.

Implementing the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP is a process for assessing and authorizing cloud computing solutions. FedRAMP defines requirements for cloud computing security control such as vulnerability scanning, incident monitoring, logging and reporting. Federal agencies seeking to implement cloud services can sponsor a particular vendor or service provider to undergo FedRAMP authorization, and the program will likely be a key component of agency migration plans.

Further streamlining procurement processes. The FCCS highlights existing GSA government-wide vehicles for browsing and comparing IaaS and SaaS cloud offerings, and stresses the value of schedule contracting in streamlining the acquisition of cloud services. GSA will also establish working groups to facilitate commodity service migration. Finally, federal cloud computing contracts will also contain riders permitting state and local governments to utilize such cloud services.

Adopting cloud computing standards. The FCCS stresses the importance of standards to ensure

portability, efficiency, and interoperability between and among cloud services so that different providers can seamlessly integrate regardless of whether they are provided using a public, private, community, or hybrid delivery model. The Strategy contemplates that NIST "will play a central role in defining standards, and collaborating with Agency CIOs, private sector experts, and international bodies, to identify, prioritize, and reach consensus on standardization priorities."

Considering international dimensions of cloud computing. As cloud computing usage increases, this technological growth will require both government and industry to confront the global implications of that shift such as: needing to balance privacy, security, and intellectual property of national data; establishing interoperability standards; and assessing the possible need for international cloud computing legal, regulatory, or governance frameworks.

Providing a stable governance structure through clearly-defined leadership roles. The FCCS outlines the roles of NIST, GSA, DHS, the Federal CIO Council, OMB, and individual agencies in leading the process of standardization, developing procurement solutions, monitoring operational security issues, driving government-wide adoption of cloud, coordinating activities across governance bodies, and evaluating individual sourcing strategies, respectively. These roles and responsibilities will continue to shift and evolve as government coordination grows and improves.

McKenna Long & Aldridge will continue monitoring key developments in each of these areas and provide periodic updates.