

Making it happen:

Responding to federal initiatives to speed and simplify cloud adoption
February 2011

This issue brief is intended for federal executives who seek to use cloud IT infrastructure services (such as web hosting) to better achieve agency mission and business goals while reducing spend. It reviews the context for federal cloud computing acquisition decisions by describing relevant government-wide IT policies, programs and contract vehicles, and provides five key considerations for acquiring cloud services to meet federal requirements.

The push for rapid reform

The federal government spends more than \$20 billion each year on IT infrastructure. It operates and maintains more than 2,100 data centers with server utilization rates as low as 7 percent. These and other compelling facts are fueling aggressive reforms in how the federal government purchases and uses IT.

The Office of Management and Budget's *25 Point Implementation Plan to Reform Federal Information Technology Management* seeks a fundamental shift from building custom systems to shared solutions and light technologies, such as cloud computing. Key points of the plan that are aimed at reducing IT infrastructure growth include a "Cloud First" policy for services and shrinking the number of data centers by at least 800 by 2015.

Cloud computing reduces costs by leveraging IT infrastructure at 60-80+ percent utilization and provisioning services as needed. Cloud computing also increases efficiency and agility through automation and significantly reduces the administrative burden on internal IT resources. In addition, buying cloud services on demand eliminates the need for large, upfront capital expenditures and is considered an operating expense.

Moving to "Cloud First"

The federal "Cloud First" policy requires agency CIOs to identify three "must-move" services by March 2011 and to create a plan for migrating those services to the cloud. At least one service must be fully migrated within 12 months, with two more services migrated within 18 months. Migration plans will include major milestones, execution risks, adoption targets, required resources and a retirement plan for legacy services.

In addition, when evaluating options for new IT deployments, agencies are required to default to cloud-based solutions whenever a secure, reliable,

Cloud Computing Defined

The National Institute of Standards and Technology (NIST) has defined cloud computing for use throughout the federal government as follows:

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

The definition includes:

- Five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service)
- Three service models (Software as a Service, Platform as a Service and Infrastructure as a Service)
- Four deployment models (Private, Community, Public and Hybrid Cloud).

Read the full NIST definition at:
<http://csrc.nist.gov/groups/SNS/cloud-computing/index.html>

cost-effective cloud option exists. Budget submissions must include an alternatives analysis that includes a cloud-computing-based alternative.

Simplifying acquisition and certification to facilitate cloud adoption

Recognizing the need for access to cloud services designed specifically for the federal government, the General Services Administration (GSA) is making available a common set of government-wide contract vehicles for secure, scalable and stable cloud infrastructure services to support websites, portals and other hosted applications. GSA also is seeking to stand up contract vehicles for cloud-based email and other solutions such as a geospatial platform.

Certifying cloud providers to meet FISMA-Moderate security requirements

All federal agencies must comply with the Federal Information Security Management Act's (FISMA's) comprehensive framework for securing their IT. Since agencies are responsible for conducting the FISMA Certification and Accreditation (C&A) process, they will want to choose cloud services that provide FISMA security controls.

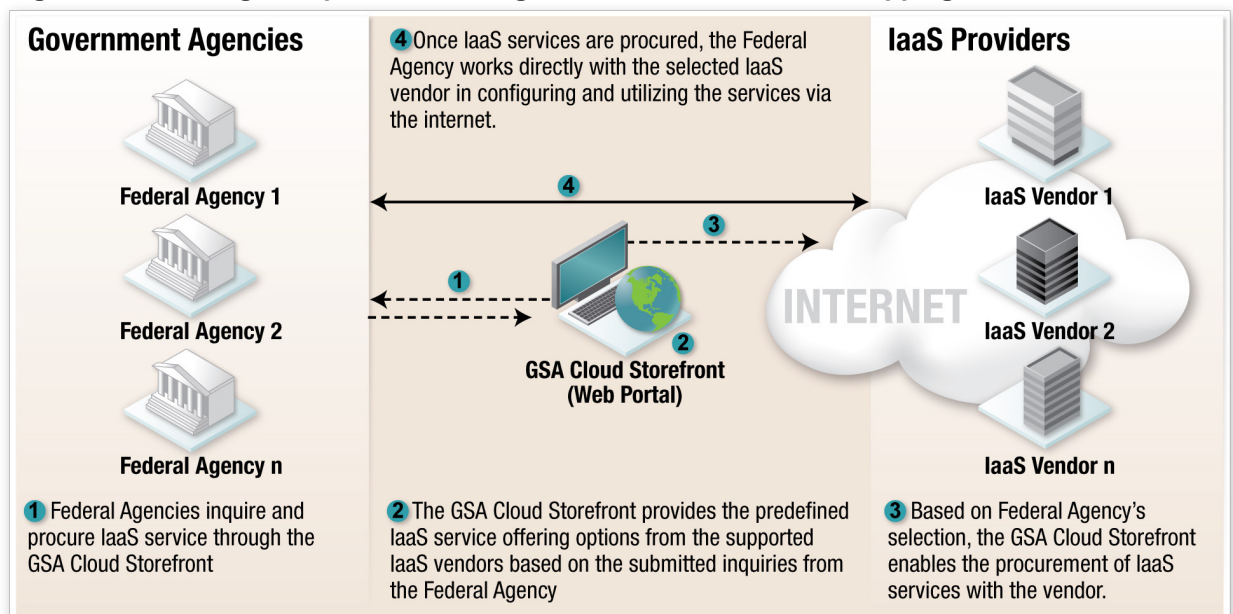
GSA's multiple-award Blanket Purchase Agreement (BPA) for Infrastructure as a Service (IaaS) allows federal agencies to procure cloud infrastructure services within a FISMA-Moderate security environment from 12 federally-certified cloud providers. State and local government agencies can also leverage these broad public sector economies of scale and buy services using the GSA BPA.

The certified cloud provider environments can be used to support the vast majority of existing and planned federal systems that are considered Low or Moderate Impact under FISMA. For systems with security requirements above FISMA Moderate, agencies can work with cloud providers to design and deploy virtual private clouds that meet more stringent security specifications. Virtual private clouds give agencies exclusive use of computing infrastructure and allow them to dictate specific security measures, while still realizing meaningful savings by leveraging the cloud providers' economies of scale.

Providing cloud infrastructure services through Apps.gov

Agencies can acquire predefined IaaS products (e.g., cloud storage, web hosting and virtual machines) through GSA's Apps.gov once the cloud providers are fully certified and accredited under the Federal Risk and Authorization Management Program (FedRAMP), which is expected by spring 2011. Agencies can then work directly with selected providers to configure their services. The procurement process is shown in Figure 1: *Procurement of IaaS services through GSA's Cloud Storefront: Apps.gov*.

Figure 1: Procuring IaaS products through GSA's Cloud Storefront: Apps.gov



11-000-007

FedRAMP at a glance

FedRAMP is an initiative of the Federal CIO to help agencies fast-track the accreditation of systems to move to the cloud. It will enable an agency to use a security authorization of another agency, or an existing authorization, with only additional agency-specific and application-specific requirements separately certified.

FedRAMP provides:

- A standard approach to assessing and authorizing cloud computing services and products
- Joint authorizations and continuous security monitoring services for government and commercial cloud computing systems intended for multi-agency use
- A common security risk model providing a consistent baseline for cloud technologies that can be leveraged across the federal government
- A set of common security requirements and process documents for agencies and providers.

Learn more at FedRAMP.gov.

GSA continues to refine its ordering processes for the BPA. For large, complex requirements, agencies can use Apps.gov to identify services and then source those requirements through task orders on the BPA from GSA's Multiple Award Schedule 70. They also can procure additional services (e.g., disaster recovery testing, database administration, and application management and monitoring) from cloud providers through task orders.

Five Considerations for Acquiring Cloud Services

Agencies seeking to acquire cloud infrastructure services should:

1. **Take advantage of government-wide cloud initiatives**

Much thought has gone into analyzing how agencies can use the cloud within the federal security, technology and acquisition context — from the centralized security authorizations of FedRAMP, to GWACs such as GSA's BPA for Infrastructure as a Service as well as NIST standards and guidance. By building upon these efforts, your agency can meet mandated timetables and accelerate potential savings without having to start from square one.

2. **Use federally-certified and accredited cloud providers**

Your agency can take advantage of the cloud infrastructure services that have been designed specifically to meet the demands of federal agencies for FISMA Low and Moderate security environments. Federally certified cloud providers have made significant investments in infrastructure, expert staff and service management technology to meet these requirements, providing economies of scale that can significantly reduce your costs. Using a certified provider for cloud infrastructure also frees internal agency resources to focus on value-added activities.

3. **Buy service, not just servers**

Successful cloud initiatives require integrated service management to align efficiencies and mission results. While cloud server time often is purchased as a commodity, successful agency cloud initiatives will consider all of the services required to deliver their systems. Management services that are important for federal cloud success include: system management, maintenance and security; backup and restore; access and user administration; operating system and application administration; capacity planning; change control; documentation and maintenance; help desk; disaster recovery and continuity of operations; patching; compliance; and vulnerability scanning.

4. **Distinguish between “commodity” and full-service providers**

There is a significant difference between a “commodity cloud” provider that delivers just the technology building blocks, and a full-service business solution provider that can shape services to meet client needs with a fully managed cloud. Unless your organization is prepared to synthesize and manage multiple cloud components and service providers,

you should find a partner that can. Full-service providers can manage the entire application stack to prevent gaps in security, leverage traditional hosting processes, and integrate physical servers with cloud architectures for more robust solutions.

5. ***Look beyond the technology hype to include people and process in decision making***

Cloud technology will not deliver the desired ROI without addressing all of the people and processes that are needed to manage effective systems. Without governance, ITIL best practices and change management processes in place, for example, anyone could create virtual machines, and the resulting sprawl would eliminate any value or savings.

Federal Cloud Resources Online

- NIST.gov – website of the National Institute of Standards and Technology
- CIO.gov – website of the Federal CIO
- FedRAMP.gov – Federal Risk and Authorization Management Program section on CIO.gov
- Apps.gov – GSA’s cloud computing storefront
- info.apps.gov – website for GSA’s Federal Cloud Computing Initiative

Next Steps

For agency executives seeking expert guidance to make sound cloud computing decisions quickly, CGI offers a disciplined transition process to get you to the cloud with confidence. We are one of the 12 federally-certified cloud providers under GSA’s BPA for Infrastructure as a Service. One of our expert executive consultants also chairs TechAmerica’s public sector task group which is providing industry input into FedRAMP.

CGI’s cloud offerings compel the development of well-managed cloud initiatives because processes, governance, security and compliance are all embedded in our solutions. As a leading IT and business process services provider with 35 years of experience delivering infrastructure and managed services to both government and industry, CGI can also help you to:

- Plan and implement effective cloud initiatives based on your risk profile and financial objectives
- Understand how new capabilities will impact your people and processes
- Decide how much control to retain vs. delegating to a provider
- Determine the internal resources and skill sets needed to effectively use the cloud
- Fully leverage the cloud with training, help desk and cloud integration services.

To learn more about federal cloud computing approaches, or to talk to a CGI cloud expert about your specific situation, contact your CGI Federal account partner or visit us on the web at www.cgi.com/federalcloud.

About CGI

A global leader in IT, business process, and professional services, CGI partners with federal agencies to provide end-to-end solutions for defense, civilian and intelligence missions. For more than 30 years, we have delivered quality services to help clients achieve results at every stage of program, product, and business lifecycle. We deliver end-to-end solutions in application and technology management, systems integration and consulting, business process management and services, advanced engineering and technology services, and operational support services. Our proven capabilities in high-demand areas include cloud, cybersecurity, biometrics, citizen services, data exchange, health IT and energy/ environment. CGI has 31,000 employees in 125+ offices worldwide.