



INSIDE THE FEDERAL CLOUD

Mastering the Challenges, Seizing the Opportunities

CONTENTS

DRIVERS BEHIND THE FEDERAL CLOUD	3
DEFINING THE FEDERAL CLOUD	4
PREPARING FOR COMMON MIGRATION CHALLENGES	5
Business process implications	5
Cultural implications	5
Scaling implications	6
Security implications	6
ADDRESSING UNIQUE FEDERAL ISSUES	6
Expertise issues	6
Timing issues	6
Compatibility issues	6
Cultural issues	7
Contract issues	7
Multi-level partnering issues	7
Sensitivity issues	7
PARTNERING FOR MIGRATION SUCCESS	7
LINKS FOR FURTHER READING	9

While enterprise IT management has its share of challenges, even the IT needs of global organizations pale in comparison with those of the U.S. federal government.

For one thing, government is simply bigger – with more than 2.1 million full-time federal employees, each of whom use at least one IT system and likely more. Also, government has missions no enterprise faces, with wartime security and zero-fail expectations to match. Where enterprise measures success in sales and earnings per share, public agencies measure success in lives saved and property protected. Missions like hurricane response and terrorism prevention require immediate scalability in not just IT capacity, but in-field headcount and logistics, on a global scale.

DRIVERS BEHIND THE FEDERAL CLOUD

Like enterprise, government IT has observed the benefits of cloud architecture, but lags in its adoption as enterprise forges its own path. Isolated from the economy's overall innovation drivers, and too often saddled with a culture of slow change and risk aversion, federal agencies struggle to harness the consolidation, transparency and scalability benefits of cloud inside the real-time, real-life mission of government.

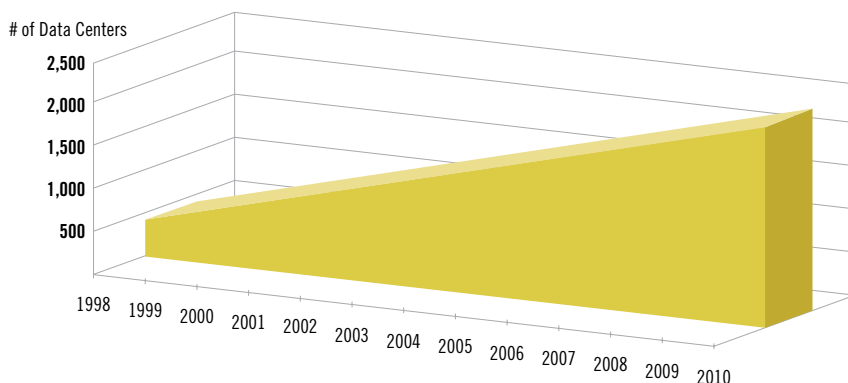
The same drivers that made cloud architecture a necessity for enterprise are at work inside government,

but even more so. To ensure capacity for worst-case emergencies and peak program needs, federal agencies are building computing and storage capacities far beyond day-to-day needs. Their unique missions (and legislated structure) amplify these pressures, fragmenting demand among duplicative systems and preventing aggregation. In time, complexity is driving federal server utilization under 30%; data center turn-up time is growing from months to years; and excessive focus on IT asset management increasingly distracts agency leadership from vital core missions.

Shrinking agency budgets are forcing agencies to find new avenues for savings. One path is to rationalize infrastructure and maintenance costs. Another is to seize the opportunity presented by retiring Baby Boomer professionals to redefine existing IT roles, and abandon legacy processes.

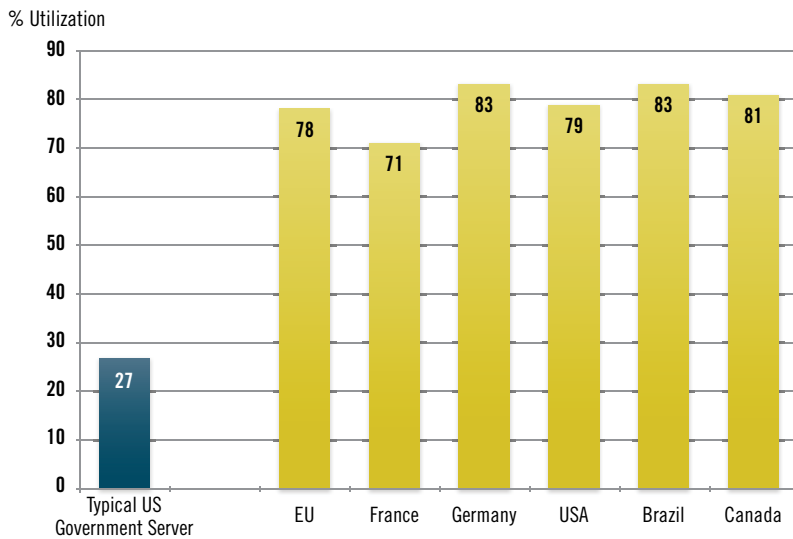
Federal IT organizations face aging issues of their own. Many systems date from more than a decade; their earlier architectures can't leverage the cost or performance benefits of today's off-the-shelf hardware, or support today's requirements for sustainability, transparency, mobility, collaboration and public participation. Individual system upgrades require separate certification and authorization processes – a time consuming process with no re-use. These systems also require annual audits without common standards, creating additional risks in networked environments where continuous monitoring is necessary for maintaining security.

Agencies like the Department of Defense (DoD) and Department of Homeland Security (DHS) need computational ability to mine civilian and commercial data, and reveal, characterize and alert agencies to real-time threats. Response may require configuring numerous virtual machines and storage to keep pace with the threat, let alone the needs of maintaining each military branch's recruiting objectives and electronic health records for millions of veterans under care.



For agencies providing direct public services, constituents expect government to move with the same pace and flexibility as enterprise. Consumer-level performance standards are driving agencies to expand not only core missions (like healthcare reform), but also provide self-service options that give consumers more ownership of their service experience. Some expectations can be difficult to predict; one-time response programs like FEMA subsidies for Hurricane Katrina survivors may have conventional data requirements but extraordinary demand. For stakeholders with scientific or economic missions, accurately modeling demand may be equally challenging, especially when users need to mash-up data from multiple agencies.

National Capacity Utilization: Major Global Manufacturing Markets vs US Government



To meet all these demands, agency IT organizations need better, more economical tools for defining applications and computing environments. And they need robust piloting capabilities that ensure a stable and predictable user experience before moving applications to production.

DEFINING THE FEDERAL CLOUD

Fortunately, with the Obama Administration's **Cloud First** initiative, those goals are now in sight. This government-wide mandate requires agencies to use cloud as their default delivery mechanism for new applications "whenever a secure, reliable, cost-effective cloud option exists."

Associated with this initiative is a cluster of services under a General Services Administration (GSA) Blanket Purchasing Agreement (BPA), designed to meet baseline storage, computation and productivity application requirements. The BPA's offerings are divided into two groups: **Infrastructure as a Service** (IaaS), and **Software as a Service** (SaaS). [Carpathia Hosting holds the distinction of being the only vendor listed in this BPA who is identified with more than one IaaS prime contractor.] The BPA creates a common architecture and taxonomy for all IaaS and SaaS offerings, designed to support most agency cloud requirements. It also includes policy controls for certification, and a standardized accreditation process to promote interoperability, portability and security.

When fully deployed, these cloud services are expected to offer government these key benefits:

- ◆ Vastly improved asset utilization across agencies, functions, and regions (with a target of boosting server utilization from 30% to 60%)
- ◆ Faster system consolidation (already a government priority, but challenged by slow adoption)
- ◆ Near real-time scalability of storage and compute capabilities, so agencies can align their response to changing market or national need (whether scaling up or down)
- ◆ Higher productivity from IT staffs, who can now focus on higher skill-level tasks like developing applications instead of configuring servers
- ◆ Accelerated development, piloting and launching new applications in a controlled and replicable fashion, while providing a more open platform for sharing innovations across agencies

- ♦ A background bridge for IT systems undergoing technology refreshes, reducing potential impacts to users while keeping vital systems available
- ♦ A change in IT success metrics, from managing assets to delivering services
- ♦ A more balanced culture of risk and entrepreneurship closer to the norms of enterprise
- ♦ Better alignment of government's information infrastructure to its mobile workforce, along with a virtualized workplace no longer bound to a desk, facility or department
- ♦ A streamlined way to acquire cloud services on popular federal contracts, using pre-competed pricing from pre-certified vendors
- ♦ Improved procurement flexibility to align computing and storage assets with program needs
- ♦ Free-market pricing that promises a well-defined and commoditized service

To help address security concerns, GSA is working with the Office of Personnel Management (OPM) to develop a standard risk-management platform (FedRAMP) for cloud-based applications. FedRAMP creates a single Authorization to Operate (ATO) for a platform with infinite reuse capacity; it strips layers of process, reducing cost and complexity, while introducing a uniform security definition for continuous situational awareness (reducing the need for audits). By standardizing security services, FedRAMP should accelerate the traditional nine-month Certification & Authorization (C&A) security assessment process by pre-certifying vendors and the computing environment – reducing not just time-to-market for the service itself, but any applications that ride on it.

PREPARING FOR COMMON MIGRATION CHALLENGES

While agencies will see clear advantages by using the GSA BPA and FedRAMP for their cloud migration, there are four common change-management issues they should prepare to face:

1. Business process implications

Some processes require transformation to fit the new virtual environment; agencies must conduct “fit” analyses to prioritize those functions to migrate first, as well as determine resources to maintain legacy applications and data environments. Other processes will arise exclusively within the cloud; these opportunities will be difficult to foresee, as IT teams may still be working with a dedicated-infrastructure mindset.

Fortunately, both cloud and dedicated environments share the same user expectations for availability, confidentiality, and scalability, especially for Continuity of Operations (COOP); cloud will make it easier to achieve these expectations by providing a flatter and simpler data sharing platform that can be defined in advance as part of the agency's COOP plan, then rapidly scaled up when crises occur.

2. Cultural implications

As agency IT moves from being system administrators to service administrators, this will change the “checkbox” they're charged with, as the focus moves from system metrics to mission metrics; IT leadership will need to develop fair and accurate performance measures to share with stakeholders in a supportive team environment. IT staff may have issues with losing physical dominion over infrastructure; leadership will need to underscore that proximity is not the same as trust, and SLAs are a better way to maintain trust. Cloud migration also requires IT to plan for, deploy and support applications and data in a mixed infrastructure, with new quality-of-service challenges; IT will need to employ a higher level of development and support expertise, probably from external sources well versed and proven in the migration process.

IT leadership will also need to proactively dispel key myths about the cloud, to set the right expectations. One is that cloud is inherently less secure than dedicated infrastructure; in fact, the federal cloud's complexity and uniform security structure actually adds security. Another is that “cloud is always cheaper;” in fact, IT needs to conduct an apples-to-apples comparison to determine which legacy applications or storage should move to the cloud, and then, which cloud configuration best meets the agency's security, performance, and cost goals. In many cases, agencies will have to find a balance between security, performance

and cost, as not all may be practically achievable at the same time.

All these changes will require not just IT, but overall leadership to demonstrate a high level of commitment to migration. Maintaining this discipline in the face of everyday mission demands may be especially challenging; leadership should be prepared to support proactive change management across the entire organization, not just IT. Leadership will also need to integrate the change process with other socioeconomic goals, in some cases without any precedent from enterprise (as it would be unlikely for some purpose-built applications like social service, defense and pure science to arise in the market).

3. Scaling implications

Given the immediate benefits of migration and its alignment with Administration goals, IT leaders may want to focus on large-scale migrations with high visibility. But agencies without prior migration experience should actually start with small migrations, like relatively simple and non-critical functions, to build the experience and process needed to tackle key agency functions.

4. Security implications

Agency IT leaders should give special attention as well to their choice of cloud environment. Government applications require acceptable levels of risk associated with threats from adjacent or rogue commercial applications that can occur in public and community clouds. To maintain a proper security posture, agencies need a service provider such as Carpathia Hosting who can establish true physical separation between environments, as well as isolate and take down environments that could become compromised without impacting those that have not.

ADDRESSING UNIQUE FEDERAL ISSUES

Federal IT leaders should also plan for the following challenges unique to the mission, architecture and culture of federal agencies:

Expertise issues

Government tends to lag enterprise IT generally, so it's not surprising government is behind in cloud adoption as well. Further complicating this situation is a lack of understanding among many agencies of how to apply cloud technology in their operations. These factors compel agencies to rely on third parties, a difficulty for organizations accustomed to building their own solutions. Those that do may quickly see operational costs increase due to scale issues, as their agency may be too small to recover fixed costs.

Timing issues

Long project cycles can also force agencies to migrate in a non-integrated fashion, since they can't afford the risk of handling multiple major migrations at one time. Agencies should therefore prioritize which environments get moved to the cloud first, and when.

Compatibility issues

Not all applications and data environments run efficiently in a cloud, regardless of scale. Many agencies also have nationally sensitive missions where even controlled risk in a cloud environment is excessive. Not all cloud functions are in the GSA BPA; some have to be provided through other vehicles, dictating use of a traditional RFQ. Agency plans should therefore include external guidance in defining these other services, then identifying the right contract vehicle for acquisition.

TABLE 1: Decision Framework for Cloud Migration

SELECT	PROVISION	MANAGE
<ul style="list-style-type: none"> ◆ Identify which IT services to move and when › Identify sources of value for cloud migrations: efficiency, agility, innovation › Determine cloud readiness: security, market availability, government readiness, and technology lifecycle 	<ul style="list-style-type: none"> ◆ Aggregate demand at Department level where possible ◆ Ensure interoperability and integration with IT portfolio ◆ Contract effectively to ensure agency needs are met ◆ Realize value by repurposing or decommissioning legacy assets and redeploying freed resources 	<ul style="list-style-type: none"> ◆ Shift IT mindset from assets to services ◆ Build new skill sets as required ◆ Actively monitor SLAs to ensure compliance and continuous improvement ◆ Re-evaluate vendor and service models periodically to maximize benefits and minimize risks

Framework is flexible and can be adjusted to meet individual agency needs.
 Source: "Federal Cloud Computing Strategy," OMB, February 2011

Cultural issues

Many government computation requirements live on the contractor side – but smaller contractors often don't have the financial wherewithal to commit computing or storage assets without first winning the program bid. Agencies should therefore include cloud planning in their Requests for Proposal to ensure smaller, desirable contractors can fairly bid for projects, then rapidly scale once that program is awarded.

Contractors working on a commercial migration might be able to help the enterprise rationalize its staff as system administration requirements decline. But in government, rationalization mainly results in reassignment (due to civil service and union regulations). Agencies therefore should plan to reassign affected IT staff to mission-level concerns; doing so will help agencies realize more intellectual value from scarce and costly human assets.

Federal funding is also distinct from that of enterprise. As spending feuds in Congress intensify, an increasing reliance on patchwork Continuing Resolutions (CRs) prevents many programs from having the same forward visibility as a full-year budget. Worse still, CRs can delay funding flow to individual programs. Given the federal calendar's hard stop, the result is a shorter spending cycle, with a premium on the agency's ability to spin up or down computing and storage capabilities. Agencies can address this in their cloud migration business cases by highlighting the connection between program funding and promised outcomes (for which cloud is a better match than dedicated environments).

Contract issues

Cloud choices can't happen in a vacuum; decisions must be made in step with the agency's program priorities, in turn affecting acquisition timing. The choice of acquisition vehicle can also be influenced by related requirements for specific hardware or software features. In many cases, the cloud choice itself is driven by a system integrator overseeing the program, and impacted by their competitive situation and workplace culture.

The GSA BPA itself strictly defines service features and billing criteria, such as pay-per-use; while intended to create a commoditized service offering and easier acquisition process, it also limits the number of configuration options available. If an agency needs an option not available on the BPA, or achieve a different scaling

structure, they should explore other avenues for those features or pricing configurations

Multi-level partnering issues

While large contractors dominate most federal programs, those vendors depend on subcontractors to define and carry out major program elements. Cloud services are no different; today's large-scale integrator would prefer to focus on higher-value transition efforts like data migration, and leave infrastructure concerns to partners. Agencies should ensure each prime contractor has the right team in place to deliver any IaaS or SaaS components in their programs. A key criteria is if the subcontractor can team well with not just the program prime, but other subcontractors as well, including contractors on other programs impacted by leveraging cloud solutions.

In some agencies, small integrators dominate, as their skill-sets and institutional experience make them a better fit (and help meet set-aside requirements). For these firms, it's important to choose the right cloud service provider, as the program's value (and risk) rides on the reliability of that cloud service. The subcontractor also must be trusted to handle direct agency support, as small integrators often don't have resources to do this on their own.

Sensitivity issues

While sophisticated and government-grade, the GSA BPA's security standards are intended for routine needs. But what happens when an agency needs to combine a secure private storage cloud (say, for patient care data) with a mobile app housed in a community cloud? Such hybrid environments aren't unusual, but also aren't anticipated by the GSA BPA or an existing security definition. In the absence of FedRAMP, and with the need for zero-fail security, agencies should plan purpose-built solutions that can ensure inherent security for applications that reach beyond their private cloud.

PARTNERING FOR MIGRATION SUCCESS

For these reasons, agencies should partner with established, expert and proven services providers who can ensure their cloud migration, implementation, and operations and maintenance fulfill their promises. Key skill-sets and assets include:

- ♦ Professional services that go beyond technical proficiency, as well as pre-package elements of the ATO process to help speed time-to-market
- ♦ A “government-friendly” partner with a proven track-record; this should include familiarity with the agency’s mission, as well as understanding mission differentiators like data formats, security requirements, acquisition rules, and cultures
- ♦ An ability to work seamlessly with other integrators, as well as plug-into existing programs (or frame new ones) with minimal start-up efforts
- ♦ An appropriate infrastructure with true physical isolation, from hardened facilities to data vaults and environmental services; Katrina and Fukushima Dai-Ichi are just two examples why worst-case survivability matters to contractors as well
- ♦ A Defense-in-Depth approach that includes physical and logical access and policy controls; an environment that supports not just cloud services, but colocation and managed service requirements; and security that goes beyond regulatory or mandated standards, to industry best-of-class procedures
- ♦ Multiple facility fail-over provisions that supports the agency’s COOP plan across jurisdictions, regions, and missions
- ♦ Continuous monitoring, including operational and security staffing that’s 24x7x365 – as threats don’t keep a schedule
- ♦ Compliance for mandates like HIPAA, FISMA, PCI DSS, and DIACAP, so there’s no question of coverage for any application or data environment within that infrastructure

LINKS FOR FURTHER READING

Details on the GSA BPA are available at:

<http://www.gsa.gov/portal/content/190333> and [https://info.apps.gov/sites/default/files/Cloud IT Services - customer presentation v4.1.ppt](https://info.apps.gov/sites/default/files/Cloud%20IT%20Services%20-%20customer%20presentation%20v4.1.ppt)

FedRAMP information is available at:

<http://info.apps.gov/content/federal-risk-and-authorization-management-program-fedramp>

Details on the Cloud First initiative are available from the Federal CIO at:

<http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf> and [www.info.apps.gov/sites/default/files/Cloud Computing Strategy 0.ppt](http://www.info.apps.gov/sites/default/files/Cloud%20Computing%20Strategy%200.ppt)

Several federal cloud computing case studies of interest:

- ♦ VA uses SaaS to speed education claims processing for its veterans:
<http://www.federalnewsradio.com/?sid=2255355&nid=35>
- ♦ NASA turns to IaaS to replace up to \$1.5B in enterprise data center services for high-compute applications:
<http://www.cio.gov/pages.cfm/page/State-of-Public-Sector-Cloud-Computing--Enterprise-Data-Center-Strategy>
- ♦ DOE employs IaaS to help visualize complex ion collider data in 3D:
http://www.anl.gov/Media_Center/News/2009/news090402.html
- ♦ Army harnesses cloud services to improve the recruiting experience:
<http://www.publicsectorinstitute.net/OnTheFrontLines/Cloud/Army.lsp>

Carpathia Hosting is a leading provider of managed hosting services, delivering secure, reliable and compliant IT infrastructure and management for some of the world's most demanding enterprises and federal agencies. Founded in 2003, Carpathia is a growing, profitable business run by a seasoned management team with deep experience in delivering enterprise hosting solutions including colocation, managed services and cloud computing. Carpathia's suite of services is designed for organizations seeking scalable, secure, robust and enterprise-grade hosting solutions that can be quickly provisioned or tailored to meet unique requirements. Backed by its E3 Promise, Carpathia consistently delivers an experience that exceeds customers' expectations. Carpathia qualifies as a small business. Contact Carpathia at 1.888.200.9494, or visit www.carpathia.com for more information. References to other products are made to show compatibility. All companies and/or products mentioned in this document are registered or trademarked by their respective organizations. The inclusion of third party products does not infer endorsement by these parties, unless otherwise noted.