Get Ready for the Inflection Point in U.S.
Federal Government Cloud Adoption

Published: 19 January 2016

Analyst(s): Rick Holgate, Neville Cannon

In response to the maturing cloud-based as-a-service market and their growing experience with commercial cloud service providers, federal government CIOs are poised to make a bigger push to the commercial cloud. This research helps CIOs move to a fully cloud-augmented environment within five years.

Impacts

- The demonstrated success of cloud-based applications (such as enterprise email) has increased the confidence and willingness of federal government CIOs to move a growing population of mission-critical applications to the cloud, which could lead to widespread, distributed, ad hoc cloud adoption.

- The significant effect of impending cloud migration on residual retained workload will require CIOs to accurately plan, estimate and monitor their changing on-premises infrastructure.

- The decision for most agencies to adopt a hybrid IT model — choosing cloud-native services for some fraction of their portfolio, while also maintaining an on-premises component for those most sensitive and mission-critical applications — will require federal CIOs to pay careful attention to architecture, management and acquisition.

Recommendations

- Federal CIOs will need to govern, and keep pace with, organizational expectations, and plan subsequent migrations with a rationalized approach and in a way that maximizes benefits and buy-in.

- Department CIOs must clearly communicate the limitations and risks of a data center consolidation mindset, shifting away from the physical-first model and rethinking it as an opportunity for service-hosting optimization.

- CIOs need to plan the acquisition of cloud services and retained, on-premises services with due diligence, risk awareness, and evolved roles and responsibilities to elude the trap of operating within legacy contract constraints and to reduce the dangers of cloud lock-in.
Strategic Planning Assumption

By 2018, increased security will displace cost savings and agility as the primary driver for government agencies to move to public cloud within their jurisdictions.

Analysis

Figure 1. Impacts and Top Recommendations for Federal CIOs

<table>
<thead>
<tr>
<th>Impacts</th>
<th>Top Recommendations</th>
</tr>
</thead>
</table>
| Widespread, decentralized, ad hoc (ungoverned) cloud adoption could occur. | - Actively govern, and keep pace with, departmental expectations.  
- Plan and prioritize migrations using a rational decision framework.  
- Adopt a common architecture to facilitate adoption and improve governance. |
| Cloud migration will have a significant effect on residual retained workloads. | - Plan accordingly for future on-premises footprints.  
- Evolve data center goals and shift to application-hosting optimization.  
- Address needed contractual and workforce adjustments. |
| Hybrid IT will likely be the most common model, but requires careful planning. | - Start using IaaS/PaaS services.  
- Evolve the acquisition of cloud and retained services in a coordinated manner.  
- Move with full awareness, build for flexibility and have an exit strategy. |

IaaS = infrastructure as a service; PaaS = platform as a service

Source: Gartner (January 2016)

The U.S. federal government has been given “cloud first” as a mandate since the early days of the Obama administration, when that mantra was a key element of the first federal CIO’s 25-point plan. Since then, the government — in the form of both CIOs and their mission/business counterparts — has gradually become more comfortable with cloud-based services. Although we have noted that the pace and progress of federal cloud adoption to be still in its infancy, there have also been signs of acceleration. Gartner estimates U.S. federal cloud spending will more than double over the next four years (see "Market Trends: U.S. Federal Cloud Market — Beyond the Hype"). Having taken nearly five years to lay the foundation for federal cloud adoption, we expect to see more visible and tangible progress and a greater level of federal cloud adoption (see Figure 2).
Several potential benefits ultimately motivate cloud migration, although the balance of benefits can be substantially different based on the type of cloud service under consideration. IaaS or PaaS, compared with SaaS, will not only incur distinct benefits (see Table 1), but will also involve different frameworks for assessing application readiness and different architectural requirements, and the markets will involve a different number and complexity of vendors. The ability to achieve some or all of the promised cloud benefits requires informed analysis of the cloud service model (IaaS/PaaS/SaaS) and the candidate applications.
Table 1. Cloud Migration Benefits and Considerations

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Cloud Services</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IaaS/PaaS</td>
</tr>
<tr>
<td>Flexibility in an on-demand model</td>
<td>x</td>
</tr>
<tr>
<td>Scalability or elasticity to accommodate changing demands</td>
<td>x</td>
</tr>
<tr>
<td>Shifting to an operating expenditure-only model and eliminating the</td>
<td>x</td>
</tr>
<tr>
<td>need for periodic capital expenditure infusions to remain technically</td>
<td></td>
</tr>
<tr>
<td>current and out of &quot;technical debt&quot;</td>
<td></td>
</tr>
<tr>
<td>Availability or redundancy that didn’t exist or was prohibitively</td>
<td>x</td>
</tr>
<tr>
<td>expensive to achieve reliably</td>
<td></td>
</tr>
<tr>
<td>Superior built-in security than what had been historically in place</td>
<td>x</td>
</tr>
<tr>
<td>on-premises</td>
<td></td>
</tr>
<tr>
<td>Improved and quantifiable service levels</td>
<td>x</td>
</tr>
<tr>
<td>Geographic diversity (proximity to users/customers)</td>
<td>x</td>
</tr>
<tr>
<td>Rapid access to cutting-edge technology and innovation</td>
<td>o</td>
</tr>
<tr>
<td>Better end-user experiences</td>
<td>o</td>
</tr>
<tr>
<td>(Incidental) cost savings/cost avoidance</td>
<td>o</td>
</tr>
</tbody>
</table>

o May deliver
x Will deliver

Source: Gartner (January 2016)

In some cases, the ability to achieve all these benefits was compromised based on federal agencies' risk aversion and desire for a fully single-tenant (agency-only, dedicated and private) cloud service, which inherently came at a higher cost and reduced cloudlike character. There are signs of recognition of the costs, both monetarily and in lost capability, in the market, with federal customers of dedicated services now looking to multitenant government community or commercial public cloud offerings.²

Cloud migration decisions — and the ease or difficulty of accomplishing the migration — are highly correlated with the sensitivity of the application or service (as measured by its FISMA/Federal Information Processing Standard [FIPS] categorization or impact level) and its mission criticality (see Figure 3).³ In general, agencies have moved most assertively with easy workloads (nonsensitive, public-facing websites and services being the most obvious candidates), and are now following up with more highly regulated and sensitive applications.

The middle tier — FISMA/FIPS Moderate — in Figure 3 is intentionally larger, because it represents the largest population of systems and applications in the federal government and, therefore, the largest opportunity for cloud migration. Nearly 60% of federal systems⁴ fall into this category.
The cost savings (or cost avoidance) for development and test instances are significant. Especially for such hardware, the cost of unused excess capacity can be prohibitive (or at least can be managed more efficiently by using an on-demand service). For many federal agencies, asset utilization is suboptimal, and average server utilization can be as low as 10% to 20%. Nonproduction development/test environments represent a substantial fraction of total on-premises workload, and eliminating the idle excess capacity (for a non-mission-critical purpose) can be a significant motivation for cloud adoption. Achieving maximum efficiency and economy will require a change in the mindset around buying and managing capacity.

Agencies with sensitive missions — law enforcement (Federal Bureau of Investigation [FBI], Drug Enforcement Administration [DEA], United States Marshals Service [USMS] and United States Secret Service [USSS]), intelligence (Office of the Director of National Intelligence [ODNI]), homeland security (Transportation Security Administration [TSA], Customs and Border Protection [CBP], and Immigration and Customs Enforcement [ICE]), defense (DoD) and citizen benefits (Veterans Affairs and Social Security Administration) — struggle most with moving mission-critical applications to the cloud, mainly due to a lack of confidence in entrusting a cloud provider with the availability, integrity and confidentiality of their systems and data, and with a proportionately larger share of FISMA/FIPS High systems and applications. Until cloud services can be authorized at that level under FedRAMP, CIOs of such agencies will largely remain cautious or measured adopters. Ultimately, they are expected to use a hybrid model, retaining their most sensitive and mission-critical systems and applications in-house.

Email represents an interesting paradox. Every agency would consider email mission-critical, but virtually every agency has migrated, or is in the process of migrating, to an EaaS model. Motivated by the increasing maturity of the email/collaboration-as-a-service market (and largely dominated by
two providers, Microsoft and Google), as well as increasing disenchantment with on-premises service providers, federal agencies have ultimately shown the collective will, either at the department level or piecemeal at the bureau level, to move decisively to a cloud service provider.

Mission-critical applications can and should soon follow that precedent. Agencies should explore opportunities for shifting as many applications as possible to achieve the greater availability, flexibility, scalability, security and economy offered by IaaS/PaaS cloud services than any on-premises model, provided they take appropriate steps to make informed decisions. Opportunities for SaaS cloud services — particularly beyond email and collaboration — also require informed decisions, including due diligence on small or emerging service providers.

**Impacts and Recommendations**

The demonstrated success of cloud-based applications (such as enterprise email) has increased the confidence and willingness of federal government CIOs to move a growing population of mission-critical applications to the cloud, which could lead to widespread, distributed, ad hoc cloud adoption.

With the lowered barriers to and increased comfort with cloud adoption — email migrations being the primary example — federal agencies have overcome a significant impediment to entrusting CSPs with mission-critical applications, which could lead to widespread, distributed, ad hoc cloud adoption if federal agencies aren’t able to govern, and keep pace with, departmental expectations. Anticipating and actively managing the impending wave of "shadow IT" or business unit (bureau/component) adoption of cloud — and leveraging the buying power and economies of the enterprise, achieving interoperability and synchronizing movements — will require active and deft governance (see "Better Adoption of Public, Community and Hybrid Cloud Opportunities Through Government Cross-Boundary Collaboration" and "Embracing and Creating Value From Shadow IT"). The authorities afforded to federal CIOs by the Federal Information Technology Acquisition Reform Act (FITARA) will also provide important tools to enable better governance. Maximizing the collective benefits should be a priority, motivated by interoperability, visibility and accessibility across the enterprise. Identify the agency’s early movers, and scale their efforts across the enterprise to avoid the proliferation of diverse, unintegrated and noninteroperable cloud services (especially SaaS) in the environment. Achieving a rational approach requires agility and responsiveness, lest impatient customers move forward autonomously.

Agency CIOs should use a decision framework for cloud migrations to examine the portfolio on an application-by-application basis and determine which should be migrated to the cloud, based on rational, consistent and well-understood criteria. The decision framework should reflect the organization’s values and beliefs, including, for example, risk appetite, compliance constraints, data sensitivity, mission criticality, application dependencies and business value to be derived. This framework should provide the organization with a set of criteria against which it can consistently evaluate applications and decisions, thus avoiding emotionally charged debates.5
FedRAMP has done a notable job of lowering the barriers of adoption and demystifying cloud services, just not at a sufficiently fast pace. With a throughput of only about 10 authorizations per year, it lacks the bandwidth to keep up with the level of supply and demand for cloud services and has increasingly relied on agency Authorizations to Operate (ATOs) for the bulk of the workload (and a reliance on cross-agency reciprocity), which may not be easily sustainable. Of note, FedRAMP has announced its "FedRAMP Forward" two-year set of priorities to improve throughput, increase standardization and encourage cross-agency collaboration.

FedRAMP is in the process of establishing a FISMA High set of controls for authorizations at that level (their release is expected in early 2016), which will first open up opportunities for Amazon Web Services (AWS) and Microsoft, who have eagerly been awaiting that opportunity, and other CSPs will follow in pursuit of the elusive set of mission-critical systems. Still, FedRAMP is projecting the image of a partner, not a gatekeeper.

CIOs should not feel constrained by the pace and throughput of FedRAMP to keep up with the supply and demand in the federal cloud market. Agency CIOs who have a high-demand service in mind should not wait for permission to pursue their own agency ATO (preferably in partnership with other like-minded agencies).

Rational organizational cloud adoption benefits from an architectural approach. Defining who should have access and to what providers and services, controlling access (and onboarding new users quickly) through the use of identity solutions, establishing privileges, implementing via technology policies to enforce this, and establishing an audit process and policy are important enabling and managing capabilities.

Recommendations:

- Reach out and actively govern cloud adoption across your organization. Gain visibility into impending cloud migrations, and be prepared to move quickly to govern and support or manage them. The increasing pace of growing and evolving expectations will require a similarly increased pace and responsiveness of governance.

- Identify enterprise opportunities and pursue them with a focus on maximizing benefits. Allow early adopters to lead the way, and have a plan for expanding their services to the enterprise.

- Pursue cloud migration opportunities predicated on a decision framework that embodies a rational analysis and a best fit for the agency environment, even if it has not already obtained a FedRAMP-compliant ATO.

- Adopt a common architectural framework to streamline the process for cloud adoption and improve the consistency of agencywide governance and visibility.
The significant effect of impending cloud migration on residual retained workload will require CIOs to accurately plan, estimate and monitor their changing on-premises infrastructure.

At the end of the rapid cloud adoption phase — in the "new normal" — the residual in-house workload will be radically different and substantially smaller. Agency CIOs need to plan accordingly.

As noted above, decisions on migration to cloud vs. in-house retention need to be made based on an informed analysis of the data in question, the service quality level requirements of end users of the cloud services under consideration and an unemotional analysis of risks (see "Clouds Are Secure: Are You Using Them Securely?" and "Take a Risk-Based Approach to Public Cloud IaaS"). In some cases, FISMA/FIPS categorizations by CIOs have been shown to be aspirational or illusory, so don't base your decisions on those alone. Objectively validate the categorizations first.

First migration efforts should focus on the "fat middle" of federal system portfolios — mission-critical systems that are accredited and authorized at the FISMA Moderate impact level. With the large number of cloud services accredited at that level, this is the richest set of opportunities. Applications need to be evaluated for their potential to be moved as-is or whether they require more fundamental rearchitecting or rebuilding from scratch (see "Decision Point for Selecting an Application’s Cloud Migration Strategy"). Consider what your migration journey will look like to best fit the organization's culture and needs: a "lift-and-shift" as-is; a move to cloud-enabled virtual automation; or an end-to-end, top-to-bottom DevOps transformation (see "Three Journeys Define Migrating a Data Center to Cloud Infrastructure as a Service").

Federal CIOs need to revisit their goals for data center consolidation. Slow progress on data center consolidation, at the same time as increasing cloud migration, should be seen as a warning sign. Although data center consolidation is now codified in law under FITARA, too many agencies interpret that priority too literally and focus on on-premises, physical data centers at the cost of huge investment, delayed availability and deferred benefits, all with the hope of becoming a better data center service provider. Agencies need to work with the Office of Management and Budget (OMB) to give up that vain hope and focus on optimizing the application hosting portfolio, with the understanding it's likely to be cloud-dominated over the long term.

CIOs, working with their acquisition counterparts, must also be prepared to displace entrenched and traditional integrators and service providers who may be masquerading as cloud providers, but may lack the scale or capability or commitment to truly become one. Disentangling their deep roots can be difficult and require a resolute approach. Rethinking, resizing and reshaping contractual relationships with in-house service providers cannot begin too soon, given the lead time that contract changes will require.

CIOs should not overlook the workforce implications — managing a predominantly cloud-based portfolio of services will require different skills than the in-house model (see "Key Skills Needed for Successful Deployment of Cloud Computing in Government"). If an inventory of workforce skills and positions does not reveal strong experience with managing service providers, and does not identify candidates for roles like "cloud architect" or "cloud service manager," begin efforts immediately to adjust and reshape the workforce. CIOs must also examine adjacent workforce limitations,
especially in the acquisition community, and work with their counterparts to address skill gaps or lack of familiarity or comfort.

Recommendations:

- Analyze the application portfolio for cloud migration potential, and prioritize efforts. CIOs should view their FISMA Moderate systems as the immediate targets of opportunity. Project residual retained workloads and their on-premises footprint.

- Communicate intentions clearly and often to governance bodies (departmental CIOs, CIO councils and the OMB). Revise and evolve goals from a focus on the data center footprint to optimized application hosting.

- Develop an acquisition strategy for the portfolio of service providers, beginning with an assessment of the effects of cloud migrations and mapping revised roles and responsibilities to contract vehicles. Be aware of — and prepare to communicate and manage — impacts on service provider workloads.

- Conduct human capital planning for the workforce of the (near) future, and begin urgently closing skill gaps through recruitment and/or retraining. Work with chief acquisition officers to close their workforce gaps.

The decision for most agencies to adopt a hybrid IT model — choosing cloud-native services for some fraction of their portfolio, maintaining an on-premises component for those most sensitive and mission-critical applications — will require federal CIOs to pay careful attention to architecture, management and acquisition.

Although some agencies — Recovery Accountability and Transparency Board (RATB), Consumer Financial Protection Bureau (CFPB), GSA’s 18F and Commerce’s International Trade Administration (ITA) — were, are or will be cloud-only, that model will likely be atypical. Most agencies will retain a hybrid model for the foreseeable future, choosing cloud-native services for some fraction of their portfolio and maintaining an on-premises component for those most sensitive and mission-critical applications. Defining and achieving their end state requires careful attention. Agencies will end up with more than one IaaS/PaaS provider and multiple SaaS providers. Hybrid IT is the state in which IT becomes the broker of these cloud services to the business, establishing governance, security and management for cloud consumption. Management becomes extremely critical for IaaS and PaaS. To reach scale and achieve the benefits that organizations seek, agency CIOs must evaluate new management processes and tools. Agencies will benefit the most from cloud-native tooling, with the understanding that they can manage the cloud vastly more efficiently and in a far more automated manner than they can achieve with management of traditional on-premises infrastructure (see "A Comprehensive List of Management Requirements for Organizations Using Public Cloud Services," "Selecting an Approach for Managing Public Cloud Services" and "How to Budget, Track and Reduce Public Cloud Spending").

Concentrating solely on the hybrid IT model may shortchange organizational opportunities. Gartner advocates not focusing on hybrid IT (as an infrastructure exercise), but rather bimodal IT, recognizing the transformative opportunities available for IT overall, not just operational efficiencies.
CIOs need to find usable, flexible and economical contract vehicles. GSA vehicles for cloud services are in the process of being updated and refreshed, IaaS has expired and EaaS has gone largely unused. Governmentwide Acquisition Contracts (GWACs) have arisen (for example, the Department of the Interior cloud vehicle) to compete with the GSA. A more competitive, relevant and usable set of GSA vehicles would improve the overall availability of cloud services in the federal space. The recent award of a GSA Salesforce BPA is a step in the right direction.

Federal CIOs should also recognize the dominant "pure" cloud market leaders for IaaS and PaaS: AWS and Microsoft (see, for example, "Magic Quadrant for Cloud Infrastructure as a Service, Worldwide"). Unmatched, to date, in scale and in their ability (and willingness) to meet government requirements, they recognize their dominant position, increasing the potential for lock-in on Azure or enticing customers with AWS-unique application services. The SaaS market is larger and more diverse. Although email and collaboration are dominated by Microsoft and Google, other SaaS CSPs vary widely in scale, long-term viability and government readiness.

The cloud market evolves rapidly. In particular, more than a small number of CSPs serve the federal cloud market, especially if a hybrid environment is the goal (see "Government (Federal) Context: 'Magic Quadrant for Cloud Infrastructure as a Service, Worldwide'"), and the players change frequently. For reasons of diversity, competition, flexibility and viability, a multi-CSP-vendor environment should be the default. Agency CIOs need to enter with open eyes and architect their cloud services with maximum flexibility, where it makes sense. If agencies are enticed by a SaaS provider, they need to be prepared for a long-term commitment, as the costs to exit may be prohibitive. In any case, understand the nature and implications of the commitment, and plan for an exit before you commit (see "Devising a Cloud Exit Strategy: Proper Planning Prevents Poor Performance").

Lastly, agency CIOs should begin mapping out changes in roles, relationships and responsibilities among their current service providers and their CSPs, and begin efforts to codify the changes contractually. Starting early will allow for lead time to acclimate affected parties to the coming changes and implement contractual modifications or new contracts entirely.

Recommendations:

- Start using IaaS/PaaS services, establish contracts, learn the providers' services and build a management strategy.
- Evolve the acquisition of cloud services and retained, on-premises services in a coordinated manner, with an integrated environment using a best-fit set of management tools as the objective.
- Move to the market leaders that are the best fit organizationally, but do so with full awareness; build for flexibility; and have an exit strategy.
- Map changes in roles, relationships and responsibilities among (cloud and other) service providers, and begin efforts to codify the changes contractually.
Evidence

1 The GSA has in many ways been on the leading edge of, and a catalyst for, cloud adoption: providing contract vehicles to ease access to IaaS and EaaS; establishing and evolving FedRAMP as a common approach to security for cloud services; and, through its support of the Federal CIO Council, publishing best practices for cloud acquisition. Most recently, with the stand-up of 18F, the GSA has shown the power of a cloud-native development team. Moreover, GSA has engaged in "eating their own dog food," setting the example by adopting all the flavors of cloud services it has espoused (IaaS, PaaS and SaaS), including EaaS. FedRAMP's publication of its draft FISMA High baseline signals its intention to address the most sensitive workloads. For civilian agencies, the GSA has been a significant catalyst and accelerator.

In the past year, the DoD has also made significant progress in increasing its comfort with the cloud, publishing its way forward, its commercial cloud acquisition guidance, its cloud security requirements guide and its best practices guide — going a long way to demystify the cloud and establish a common understanding of the tools and access at its disposal. The Defense Information Systems Agency (DISA) has been designated as "DoD’s FedRAMP" to authorize cloud service providers measured against the DoD’s heightened security requirements.

The GAO and the CIGIE both recently assessed the federal progress on cloud adoption. GAO noted the focus on service improvement (instead of cost savings), and CIGIE noted the immature, ad hoc, decentralized approach during the experimental or learning phase with initial cloud adoption. These are opportunities for growing federal maturity. The GSA, for example, is looking to update and...
modernize its cloud vehicles; meanwhile, 18F is on the verge of offering its own "cloud.gov" Platform-as-a-service.

In other signs of notable progress, the Department of Justice (DOJ) recently adopted Box as a departmentwide SaaS information-sharing platform, and the Federal Aviation Administration (FAA) awarded an enterprise cloud agreement to provide access to Microsoft and AWS. These both represent a conscious, enterprise-level decision to shift to the cloud in a rational way that achieves economies of scale.

The DoD recognized the easy workloads (public-facing Web presences) as a logical and uncontroversial step. Agencies with public-facing missions (GSA, U.S. Department of Agriculture [USDA] and Department of the Interior, for example) have found moving mission-related applications less daunting. And some of the newer agencies (RATB and CFPB) have been built on a pure-cloud foundation, again made easier because of their public-facing mission. The ITA (within the Department of Commerce) has announced its intent to adopt a 100% cloud-as-a-service model for its globally distributed workforce.

More-progressive agencies (including CBP and Citizenship and Immigration Services [USCIS] within the Department of Homeland Security [DHS]) have experimented with cloud-based development and test environments as an economical, agile alternative for uses that are neither mission-critical nor contain sensitive information.

For email (especially in the DHS and DOJ), bureaus are rapidly defecting to commercial cloud service providers. Even the DoD is looking hard at Office 365 as an enterprise offering, following the DoD CIO’s stated intention for a commercial email service, and with the Air Force and the Defense Logistics Agency having already announced their move. In particular, some bureaus with sensitive missions (TSA and Federal Emergency Management Agency [FEMA] within DHS, and the Department of Energy) are examining the government community cloud offering of Office 365 as sufficient for its requirements, foreshadowing what may be the ultimate demise of the Dedicated/International Traffic in Arms Regulations (ITAR) offering. The USDA and FAA are already contemplating a shift off the Dedicated/ITAR model, which would leave the DOJ and DoD as its only remaining federal customers of the premium service.

The analysis in this research is based on primary and secondary research. Gartner analysts conduct daily interactions with federal agencies, as well as the technology providers in this market. Various links to sources are embedded throughout this research.

2 For example, both the USDA and FAA are revisiting their decision to adopt Microsoft Office 365 Dedicated/ITAR and considering migration to the Government Community Cloud offering, based on more favorable pricing and greater currency of features and functionality.

3 Generally, one might expect the mission criticality of a system — or the degree to which it supports mission-essential functions — to be highly correlated to its FISMA/FIPS impact level, but that is not categorically true.

For examples of such frameworks, see "Decision Point for Selecting an Application's Cloud Migration Strategy," "Take a Risk-Based Approach to Public Cloud IaaS," "Devise an Effective Cloud Computing Strategy by Answering Five Key Questions" and "Government Cloud Benefit Realization Starts With Business Alignment."

See "An Emerging IT Role: The Cloud Architect."