DON’T BE A BOX HUGGER
A REPORT BY THE CLOUD COMPUTING CAUCUS ADVISORY GROUP

“If everyone does it, cloud could be huge.”

Federal CIO Tony Scott,
at the Data Transparency Coalition’s
Financial Regulation Summit, March 25, 2015
Cloud computing represents a tremendous opportunity to dramatically transform how the Federal government manages, processes, and shares information. Federal agencies that effectively procure and deploy advanced cloud computing solutions will not only substantially lower costs as a result of greater operational efficiency, but they will finally possess the necessary computing power to solve our nation’s largest and most pressing challenges; speed the flow of information; and establish a clear path toward more agile and flexible Federal information system.

In short, cloud computing is all about better government.

That is why I co-founded the Congressional Cloud Computing Caucus, to foster awareness and understanding of cloud computing’s potential to save taxpayer dollars and improve government operations.

The Federal government invests approximately $80 billion annually on information technology. However, as the U.S. Government Accountability Office (GAO) noted when it placed “Improving the Management of IT Acquisitions and Operations” on the GAO High Risk List earlier this year, “…Federal IT investments too frequently fail or incur cost overruns and schedule slippages while contributing little to mission-related outcomes.” The bottom line is that the Federal government is running on systems that are disjointed and regrettably, often built on aging, outdated technology.

In Fiscal Year 2015, out of the $79 billion budgeted for Federal IT, taxpayers will spend $58 billion simply to maintain antiquated legacy systems, an astounding sum that amounts to 73 cents out of every Federal IT dollar invested. This imbalance between innovation and the status quo ultimately squanders our country’s most valuable Federal IT asset – its people – as valuable IT talent is forced to focus on managing daily tactical problems at the expense of developing and implementing comprehensive strategic improvements that would make government more efficient, more responsive, and more effective over time.

American taxpayers deserve more for their hard-earned dollar than yesterday’s technology tomorrow. They deserve value, and cloud technology is all about value – paying for computing power when you need it, rather than designing everything for maximum use or worst-case scenarios.

The Federal Information Technology Acquisition Reform Act (FITARA), which I co-authored, represents the first major overhaul of the laws governing Federal IT management in more than 20 years. Effectively implemented, FITARA will reduce waste and duplication in agency IT spending and generate better outcomes for the American people. A key component of FITARA is codifying and strengthening the Federal Data Center Consolidation Initiative, which will spur agencies to utilize commercial cloud computing solutions as they seek to eliminate costly and antiquated Federal data centers.
Of course, more work remains to be done. Washington needs to fundamentally change how government views, acquires, and employs technology.

Forecasters predict the global market for cloud computing will reach $270 billion by 2020. Yet, Federal spending on cloud services remains modest, with agencies expected to invest $2.05 billion in 2015. To accelerate Federal adoption of cloud technologies, agencies must overcome inertia and cultural resistance, while working with Congress to address any regulatory, educational, or bureaucratic hurdles that may exist. We must adapt to new models of doing business. And we must make it easier for commercial vendors to enter the Federal market by removing barriers to entry and unnecessary procedural hurdles.

The Cloud Computing Caucus Advisory Group’s expansive new report is a timely review of cloud computing’s utility, the institutional barriers that are slowing its adoption, and the steps that must be taken for the Federal government to finally reap the full benefits of this powerful new technology.

I commend the Cloud Computing Caucus Advisory Group’s important work in highlighting successful best practices and identifying challenges that are impeding agency efforts to fully embrace IT innovation. I look forward to continuing to lend my voice to the dialogue on this important conversation.

Sincerely,

Congressman Gerald E. Connolly (VA-11)
Founding Member of the Congressional Cloud Computing Caucus
Leadership, in the end, is the crucial differentiator between agencies that are embracing all that cloud has to offer and those that are sitting on the fence and hugging their boxes. The Cloud Computing Caucus Advisory Group set out to determine what sets the cloud pioneers apart from the fence sitters and box huggers by capturing the views of nearly two dozen of the most forward leaning Chief Information Officers (CIOs) and Chief Financial Officers (CFOs) in government. Their comments, supplemented by research and reports from the Office of Management and Budget, the Government Accountability Office, and industry analysts provide the most comprehensive picture of the progress made to date and the work still to be done as the Federal government lurches toward realizing the White House’s Cloud First vision.

Key Insights from Cloud Experts

The key to most government cloud installations is the Federal Risk and Authorization Management Program (FEDRAMP), a government-wide effort to standardize the assessment, authorization, and monitoring of commercial cloud products and services for government customers. The process can be expensive and time consuming, and we asked cloud experts to discuss what the long and winding road to certification means for Cloud Service Providers (CSPs) and agencies. We also asked about cloud security, why some hesitate to move data and applications to the cloud, and why others feel security is no longer a hurdle. We asked them about the return on investment they’ve experienced and about what distinguishes the pioneers from the fence sitters and box huggers. We asked cloud experts to outline the barriers surrounding cloud computing and asked agencies to grade their cloud migration efforts.

Here are some up-front observations:

- **Bean Counter Indifference**
  CIOs see the cloud as a business transformation opportunity, but the potential savings have failed thus far to capture the attention of Federal CFOs. Whether this is because CIOs are holding their savings close to the vest in hopes of reinvesting those funds to pay for other priorities, or because IT represents too small a slice of most agency budgets to command a

---

**FEDERAL IT SPENDING – BY THE NUMBERS**

According to President Obama’s 2016 budget request, Federal cloud spending will increase by only 2.3 percent in 2016, after growing 33 percent from 2014 to 2015.

<table>
<thead>
<tr>
<th>Year</th>
<th>Total IT Spending</th>
<th>Cloud Spending</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY 2014</td>
<td>$81.8 billion</td>
<td>$1.54 billion</td>
</tr>
<tr>
<td>FY 2015</td>
<td>$84.2 billion</td>
<td>$2.053 billion</td>
</tr>
<tr>
<td>FY 2016</td>
<td>$86.4 billion</td>
<td>$2.101 billion *</td>
</tr>
</tbody>
</table>

---

2. Ibid.
Federal IT leaders know cloud computing offers a new way to store, process, and deliver data and IT services. But most of that is not cloud, but rather an attempt to move everything to the cloud. According to OMB, a provisioned IT service refers to a shared/cloud service that is (1) owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises and (2) consumed by the agency on an as-needed basis. OMB’s IT Dashboard shows 26 agencies investing $2.101 billion on cloud in 2016. But that may not comprise the full scope of federal cloud. Gartner Research predicts Federal cloud spending will reach $3.5 billion in this year, and IDC pegs the market at $3.4 billion. The administration must present an accurate picture for Congress and the market to have a clear understanding of where the government market is and how far it still has to go. Failure to do so will draw industry into the market with frothy and unrealistic expectations.

### Cloudy Forecast

Pinning down exactly what the government is spending on cloud services is difficult. OMB says it is seeking $7.34 billion for “cloud and other provisioned services” in the President’s 2016 budget request – 8.5 percent of the proposed $86.4 billion 2016 IT budget. But most of that is not cloud, but rather a generic commodity service, the low-hanging fruit in an otherwise complicated jumble of custom programs and applications. Moving beyond the low-hanging fruit is the most pressing challenge most agencies face today.

### Email First

Half of Federal agencies have moved email to the cloud, according to a recent MeriTalk study, and nearly one in five said they deliver more than 25 percent of their IT services fully or partially via cloud. Email is viewed as a generic commodity service, the low-hanging fruit in an otherwise complicated jumble of custom programs and applications. Moving beyond the low-hanging fruit is the most pressing challenge most agencies face today.

### Defense Is the 800-Pound Gorilla

The Department of Defense (DoD) will account for 37 percent of all the money Federal agencies will spend on cloud computing in the current fiscal year, or $772.9 million of a total $2.05 billion. By way of comparison, DoD accounts for 43 percent of all Federal IT spending, a comparable share of the overall budget.

Federal IT leaders know cloud computing offers a new way to store, processes, and deliver data and IT services. But cloud also demands that they fundamentally re-evaluate what they are currently doing and why, as well as what’s actually possible. All that self examination makes the process that much harder.

“Making the leap to cloud is like you’ve been flying a Douglas MD-80, but wanting it to turn it into a Boeing 777 mid-flight – you have to keep everything running while also making the necessary transformation from an application-centric model to a data-centric one,” said Dr. David A. Bray, CIO, Federal Communications Commission (FCC).

### Security

Data is currency. It’s an asset. Federal agencies represent most of the world’s largest repositories of data, ranging from employment, tax, and college spending statistics to agriculture, weather, surveillance data, and more.

Digital highways and the proliferation of video security and other sensors are now, or soon will be, expanding exponentially the volume of data they produce. Worse, databases have replicated themselves over and over, with agencies often maintaining duplicate data sets, using those copies for disparate purposes, indeed, 40 percent of Federal data assets are stored four or more times.

There are lots of reasons that’s not a good idea – data integrity and consistency are just two. But security trumps all. The more data is replicated, the more likely it is that one or another copy can be compromised.

Data is difficult enough to protect when it’s housed in Federal facilities, behind Federal firewalls and inside Federal servers. But in the cloud, data is in motion, and could pass through the hands of many people in unknown locations (in the absence of government security regimes). Anxiety about data stewardship and security throughout that journey is a pain point, and it’s holding agencies back.

Can FedRAMP certification be improved?

The Federal Information Security Management Act (FISMA) requires Federal agencies to develop, document, and implement information security policies, and the National Institute of Standards and Technology (NIST) is responsible for setting standards for implementation. For cloud applications, FedRAMP certifies that cloud products and services are FISMA compliant. Managed by the General Services Administration (GSA), FedRAMP provides a Good Housekeeping Seal of Approval for cloud security in the Federal market. The goal: “Certify once, use often,”

FedRAMP was conceived five years ago and launched in June 2012. Industry and agencies alike have chafed at both the standards and the cumbersome certification process. Maria Roat and Matt Goodrich, the founders in the FedRAMP PMO, are to be commended for their leadership in bringing this program to life. As the Director, Goodrich continues to show admirable, tireless dedication to advancing and improving the program. As of May 5, 2015, according to the FedRAMP ONRAMP, just 35 products are certified as FedRAMP compliant, with another 40 at one stage or another in the review process, and many, many more waiting to engage in certification.

Can FedRAMP certification be improved?

---


Insight into the FedRAMP Process

According to CSPs, the average cost to complete FedRAMP certification is between $4 million and $5 million. It can take up to 18 months to get through the process. In April 2014, 24 CSPs were awaiting certification, according to the FedRAMP ONRAMP. One year later, 16 of those same CSPs were still in the pipeline awaiting approval.

The submission typically can entail 1,000 pages of technical and legal documentation.

Hewlett-Packard holds the record for the fastest FedRAMP dash: just five months. HP was only able to move that fast because it was retreading stomped ground. “They had a previous ATO [Authority to Operate] they built for the government, so it wasn’t a unique service,” said FedRAMP Director Matt Goodrich. “They built their service on FISMA.”

There are three paths for CSPs to gain Authority to Operate (ATO) under FedRAMP:

• **Through the Joint Authorization Board**
  The JAB consists of CIOs from GSA, DoD, and the Department of Homeland Security (DHS). Vendors must first be assessed by an accredited Third Party Assessment Organization, or 3PAO. The JAB issues a provisional ATO, which allows a vendor to bring a product to market. But a customer agency must ultimately issue a final ATO. To date, there are 14 approved CSPs with 17 approved solutions using this method

• **Directly through a customer agency**
  Agencies may work directly with a CSP to issue an ATO. To date, there are 13 approved CSPs with 15 approved solutions using this method

• **CSP-supplied package**
  Just three CSPs have earned ATOs using this last approach. In this process, vendors use a 3PAO to submit a security assessment package to the FedRAMP PMO without going through the JAB

Each product has to be certified separately, but once one product or service is through, much of the documentation can be applied to subsequent products, provided the technology and approach is largely the same from one product to the other. Small businesses in particular find this burdensome and a barrier to entry.

GSA acknowledges that the hurdles can be burdensome, but officials expect the time lag experienced to date to ease over time.

“It’s a maturing process to become certified and we’re learning along with the entire community,” GSA Acting CIO David Shive told the Cloud Computing Caucus Advisory Group in March. “It’s safe to assume there will be some refinements and optimization. We hear from industry that they understand the process and it can be difficult and time consuming. But anything worth doing typically takes a fair amount of effort. There is value in securing the Federal enterprise in line with certain standards. It’s a burden, but a burden worth doing. Our goal is to lessen that burden on the bureaucracy side. But the basic blocking and tackling of running scans and making sure your stuff is validated is important.”

Adding to the confusion: There's no clear requirement that Federal agencies must use FedRAMP-certified CSP offerings. OMB initially established a June 4, 2014, deadline for CSPs to achieve FedRAMP certification, but the date came and passed without fanfare. OMB failed to enforce the deadline.

Meanwhile, it's clear that FedRAMP is not going to be sufficient for all agencies. Some customer agencies, particularly in DoD, will require additional certifications and testing. Inspectors general at 19 agencies last year evaluated the government's cloud computing efforts and concluded that FedRAMP was unable to meet basic security standards and that service-level agreements between agencies and commercial cloud providers needed to improve.11

Standards keep changing. Having to constantly revamp an agency's infrastructure to adhere to new security regulations is burdensome for all.

"Industry says, 'Tell us what to do once so we don't have to keep changing it.' But if they really want that, then we need to set a high security baseline," Goodrich told an audience of mostly industry representatives in April. FedRAMP has thus far approved products and services only at the FISMA low and moderate levels. A draft FedRAMP standard for meeting FISMA high requirements was circulated in early 2015 for comments, and will be revised and recirculated in summer 2015.

The new FedRAMP high standards were created for health care, financial data, and law enforcement, where personally identifying information and privacy issues become a significant concern. They do not address National Security System (NSS) or classified levels of security.

Five agencies – DoD, Department of Justice, DHS, Veterans Affairs, and Health and Human Services (HHS) – represent 75 percent of the market for FedRAMP high solutions.

It may ultimately make more sense to simplify matters, so that instead of a series of confusing government standards, commercial and government users alike can settle on a single set of requirements for privacy and personally identifying information.

"What we want to do is really have a thoughtful dialogue around those security controls that we think are needed at the high baseline," Goodrich said at a MeriTalk cloud computing event in January.11

Regardless of what standards GSA settles on, the Pentagon will still expect a higher standard for classified national security systems. As DoD CIO Terry Halvorsen explained at a Cloud Computing Caucus Advisory Group meeting in February: FedRAMP is a "great starting point." But it is not the answer to all of DoD's security requirements.

Still, vendors agree that FedRAMP provides a baseline that all customer agencies can understand. GSA should be applauded for its commitment to transparency through its website, frequent public appearances, and the FedRAMP OnRAMP – www.fedramponramp.com. This dialogue is expanding understanding across the marketplace. Separately, the new FedRAMP Forward industry advocacy group provides an excellent vehicle for industry to provide input on the process.

The tension between security requirements and the speed with which products and services can be certified is natural and unavoidable. For good reasons, Kathy Conrad, deputy associate administrator of GSA's Office of Citizen Service and Innovative Technologies – and owner of the FedRAMP Program Management Office at GSA – says "FedRAMP doesn't want to sacrifice the rigor of their requirements and security simply to speed up solutions through the pipeline." In short, FedRAMP leadership believes its process not only improves security but has changed the conversation. Some 41 percent of Federal IT professionals say they are more likely to consider and select hybrid, community, or public cloud solutions because of FedRAMP certification.14

"The barrier to the cloud used to be security, security, security," said one long-time Federal CIO. "FedRAMP is tearing that barrier down."

GSA has unveiled a two-year plan intended to improve the program. The plan lays out 6-, 12-, 18-, and 24-month incremental initiatives to expand understanding, promote adoption, and speed the approval process. The 12-page plan also seeks to incorporate industry standards and to enhance the way those standards are integrated into the certification process.14 FedRAMP assessment overlays will be created to make it easier for agencies, 3PAOs and CSPs to demonstrate compliance with additional requirements and initiatives, such as Trusted Internet Connections (TIC) and Continuous Diagnostics and Mitigation (CDM).

That's a heavy lift. The FedRAMP Program Management Office is clearly working overtime to develop standards and improve efficiency, but is under resourced for the challenge. Considering all that is riding on the program, additional investment in staff and support could pay dividends in speeding the approval process and increasing the number of FedRAMP-approved products and services available to government customers.


Separation Anxiety: Letting Data Go

Box huggers are afraid to let go. They want hands-on control of their servers and data. Some accuse them of clinging not just to their boxes, but to status quo. Change is hard.

Security, integration, portability, and a lack of trust in commercial CSPs are the most cited factors holding those managers back:

- 58 percent of Federal IT professionals say cloud/legacy system integration is a barrier to further migration
- 57 percent cite the inability to move data from existing legacy systems to the cloud
- 54 percent cite concerns with regaining control of data once it is in the cloud

Further, 32 percent insist their data cannot be moved to the cloud due to security or data sovereignty issues. And 23 percent said that they were still not comfortable passing sensitive Federal data even to FedRAMP-certified CSPs.

CIOs say a little paranoia is justified.

“There isn’t one primary barrier, but there are complex technical barriers. The data is in someone’s computer storage room, so there will always be security concerns,” said one senior Federal IT executive. “Your private cloud can sit two rows away from the public cloud. There’s always a fear factor. You have to be hyper vigilant.”

Why is data security still such a significant concern for agencies?

Thoughts from Pioneers on Cloud Security

Many CIOs are in the midst of a crash course in cloud – trying to understand and explain the range of deployment models and implications of moving data and applications. FCC’s Bray recommends that all agencies should challenge their staffs to justify on-premise storage and solutions versus moving to the cloud.

“We each should examine why we want to have an on-premise solution versus other cloud-based alternatives,” he said.

Halvorsen has spoken persuasively at numerous public events on the need to move non-sensitive data

---

16 Ibid.
to commercial clouds. For him, it's a simple matter of conserving resources. Like many agencies, the Pentagon engages in frequent debates over what it can move to a commercial cloud and what it must fully control. It's likely, Halvorsen said at DoD's Cloud Industry Days in January, that the amount of truly sensitive DoD data "is a much smaller portion of our data than we think it is."

Pioneers buy into cloud because they understand that fact better than others. They understand that CSPs are providing inexpensive storage solutions, and they've overcome the long-standing institutional belief that you if you can't touch it, it's not real.

Other agencies remain skeptical and anxious. Data governance – determining what data belongs where – is a slow, painstaking process.

"Security has and will continue to be a major concern for all [data] regardless of its location," said Pamela Dyson, CIO at the U.S. Securities and Exchange Commission.

That concern applies to the debate over applications as well.

Some 44 percent of respondents in a recent MeriTalk report said they remain "uncomfortable" or "very uncomfortable" turning IT services and applications over to cloud providers.17

"It's all about the mission and where we can most effectively move our information so it best fits our cause," said Tom Michelli, Deputy CIO, U.S. Coast Guard. "We constantly ask ourselves, 'Does it make sense to move it here and when?'"

The key to overcoming obstacles can be as simple as putting cloud solutions to the test.

"We've moved into adoption more aggressively because we've gotten more comfortable with the security we've achieved," said Rick Holgate, CIO, Bureau of Alcohol, Tobacco, Firearms, and Explosives.

Michael Valivullah, CTO at the Department of Agriculture's National Agricultural Statistics Service, plans to move 70 percent of his agency's data into the cloud by 2020. "I think FedRAMP has been moving in the right direction and making good progress," he said. "Federal agencies are feeling more comfortable with the security controls in the FedRAMP assessment list. Therefore, I expect more agencies to adopt cloud sooner than later."

CHAPTER 3
Understanding ROI

Cloud has many appeals, including the promise that it can cut costs, but determining an ROI for cloud is difficult. A recent report by the Congressional Research Service warns that in "at least some cases...costs associated with cloud computing may outweigh potential financial benefits."

"Although most observers appear to believe that cloud computing can offer substantial economic benefits, attempts to project the cost advantages vary widely, with cloud services estimated to cost anywhere from 10% to 250% as much as local IT, but with most estimates projecting savings of at least 50%. The large variation appears to reflect uncertainties arising not only from imperfect understanding of the economics of cloud computing in general, but also from variations in need and circumstance among potential users and uses," the CRS report said.18

Officials say they've noted the problem, but leave solving it to their customer agencies.

"We do not have a blanket approach to identify the savings. We rely on the agencies to articulate their savings," a White House official said. "Each agency has different ways they're moving to the cloud, so there are different ways they measure their success."

All that fuzzy math plays into the hands of the box huggers and their desire to stick with conventional approaches. If you can't prove the savings, there's no reason to bother with all the extra work and risk.

But what have cloud pioneers learned about savings and ROI?

Case Studies on ROI

Pioneers are adamant – cloud computing represents an unparalleled opportunity to save money and increase IT efficiency. Case in point: Moving its Consumer Help Desk to the ServiceNow cloud saved time and money at FCC compared to conventional options.

"When we looked at previous 'gold standards' in public service, they cited $3.2 million and 18-24 months of development for an on-premise solution," Bray said. "By opting for a Software-as-a-Service solution, we spent only $450,000 and had it done in less than six months. Cloud services provide increased scalability, flexibility, agility, and increased resiliency."

The SEC experienced the same speed-to-market phenomenon.

"Cloud computing allowed us to quickly capitalize on some business needs that otherwise would have taken longer to implement," Dyson said. "It has also allowed us to leverage common functions and applications that have eliminated the need for the SEC to build or purchase something specifically for our use."


ATF used Microsoft to move email to cloud, eliminating frustrating outages at the agency. "We've had no downtime in email in 18 months," Holgate said. "It's beyond anything we could have achieved on prem." What was the return on investment? "It's hard to quantify as it's an immeasurable monetary benefit."

The Labor Department also saw cloud email as a simple configuration change within its infrastructure, and instantly saw benefits in terms of enhanced service.

"We saw 400 times as much storage in cloud email in terms of mailbox size for the same cost, along with collaboration benefits," said Dawn Leaf, Labor's CIO.

Pioneers consistently cited non-monetary rewards – improved service and capabilities – as justifying cloud investments, regardless of whether or not they captured expense savings.

"There's a 'soft benefit,' even if we're just breaking even," said Richard McKinney, CIO, Department of Transportation. "We're able to add more features, while increasing transparency with customers."

Environmental Protection Agency (EPA) CIO Ann Dunkin echoed that comment.

"When we first started considering our email cloud migration, we anticipated recouping the implantation costs within two to three years and realizing cost savings afterwards," she said. "However, we are now looking at expanding the capabilities of our tool well beyond the email and collaboration capabilities initially purchased to provide application hosting and development. We will be thinking of ROI in terms of increased capability and usability."

Still, finding a way to quantify cloud's soft benefits is important.

"Every business needs to do their own budget and ROI for the cloud," said Halvorsen at the February meeting of the Cloud Computing Caucus Advisory Group. "They need to constantly ask, 'Am I mission-effective?' and 'Am I saving money?'" 19

A standard methodology that any agency could use to calculate the value of improved service along with any other savings that might be had could go a long way toward helping agencies project savings and justify upgrades. It would also avoid duplication of effort and enhance the consistency of data.

---

CHAPTER 4

Cloud Pioneers: Racing to the Cloud

While box huggers are deliberating, pioneers are innovating.

The Department of the Treasury, National Aeronautics and Space Administration (NASA), DoD, DHS, GSA, and the National Oceanic and Atmospheric Administration all are widely recognized as cloud computing pioneers because they have consistently looked for new ways to leverage the cloud to advance their missions, save money, and improve the delivery of service.

As pioneers, they give other agencies positive role models and demonstrate that government can be on the forefront of change, despite its reputation to the contrary.

Treasury became the first cabinet-level agency to have its website fully hosted in a public cloud in 2010.20 The department leveraged Amazon's EC2 cloud service to host the site and associated data applications.21 Hardly surprisingly, NASA was among the first to boldly go.

“We were so early that we came up with our own words for the cloud and its add-ons,” said Tom Soderstrom, CTO at NASA’s Jet Propulsion Laboratory. “We just tried to do something new and experiment. The powerful thing about the cloud is the speed to market. Start with what can improve collaboration so more people become familiar with the model.”

What makes a pioneer? Have other agencies followed their lead?

Common Traits of Cloud Pioneers

Pioneers share three traits:

- Leadership that understands how the cloud can further their mission
- Defined requirements and goals for their solution
- Direction and support from both the CIO and CFO, enabling them to enable culture change

“Successful agencies using cloud are mixed in their size and budget. But they [all] have leadership support to make the change to the cloud,” the White House official said.

---


Most agencies have moved some applications to the cloud, even if they remain in the initial stages. This low-hanging fruit consists of:

- Email
- Web hosting
- Customer Relations Management systems
- Logistics
- Procurement applications

NASA has moved nearly 160 applications across three cloud deployment models – public, private, and hybrid – to date. Soderstrom urges agencies to ask first whether it makes sense to migrate legacy applications or if it might be wiser to start fresh.

More intensive migrations include:

- Document tracking
- Security storage
- Geospatial services
- Records management

Those who dive headfirst into the cloud acknowledge they do so with their own share of anxiety. But they go in with a forward-thinking frame of mind.

“We started with collaboration tools that were just internal facing,” said GSA’s Shive. “We got our user population familiar with the tool and made them feel that there is no difference between operating this on the cloud or internal GSA servers. Once they felt comfortable with the use of the tool and the security, they knew that where it was hosted didn’t matter. They didn’t have to hug their servers.”

Pioneer CIOs say their success hinged on the teams they were able to assemble across their organizations. It wasn’t just IT people.

“Our success is due to how innovation is enabled by three communities that don’t interact often: the CIO; the acquisition, procurement, and contract people; and the legal team,” said Soderstrom. “We went face to face over to visit cloud vendors so our legal people could talk to CSPs’ legal people. All entities working together is the key to innovation. All three communities are vital.”

---


No department or agency spends more on IT than the DoD. So it should be no surprise that DoD leads Federal agencies in cloud investment, too. What may be surprising is that DoD is also among the Federal government’s cloud pioneers. Where box huggers may be intimidated by cloud computing, DoD is matter-of-fact: its appetite for data is insatiable, and cloud is just another data distribution technology.

Defense endured bumps along the way. By its own admission, it couldn’t implement cloud infrastructure as quickly as it wanted because of its own stringent and constantly evolving security requirements.24

That hurdle still remains, but DoD continues to move forward. Its 2015 cloud investment is expected to reach nearly $773 million, accounting for 37 percent of all Federal cloud spending.25

DoD cloud requirements continue to change. For DoD, FedRAMP is a starting point, not the answer. That’s why the Pentagon talks about “FedRAMP Plus,” which represents a secondary level of scrutiny. The Pentagon’s concerns about data and security are substantially greater than most agencies because lives and national security can be on the line. But Halvorsen has also acknowledged that DoD puts plenty of data under lock down that could safely live in FedRAMP-compliant commercial clouds.

“I think [relatively sensitive data] is a much smaller portion of our data than we think it is,” Halvorsen said at a February meeting of the Cloud Computing Caucus Advisory Group.

The Pentagon says it wants to go commercial. But will it? The key, Halvorsen has said, is to differentiate between the kinds of data, so that the appropriate level of security is applied to each.

What do the Pentagon’s future cloud plans look like? Will it be satisfied with commercial cloud?

DoD’s Additional Requirements

The Pentagon still lives in a “FedRAMP Plus” world where extra security standards are a must, but it is making slow, deliberate steps toward commercial cloud. Last year the Pentagon gave defense agencies more authority to purchase cloud services from commercial vendors rather than using the Defense Information Systems Agency (DISA) as its sole broker. The DoD Security Requirement Guide defined three tiers of data sensitivity:

• 1 and 2: Commercial cloud. Used for systems that are fully public or discoverable through FOIA requests. Does not require physical separation or access to DoD networks


25 www.ITdashboard.gov Fiscal Year 2015 cloud spending
• 3 and 4: Virtual cloud with a secure connection to DoD networks. This is for business systems that support operations in DoD.

• Data 5 and 6: Private cloud for national security systems that must exist in a physically separate environment not connected to a virtually accessible cloud.

The guidance helps CSPs understand what they can expect. But DoD continues to move slowly forward, and it has one pilot program underway to test higher-security level 4 data in a secure, commercial cloud.

While FedRAMP Plus represents the Pentagon's current approach to security, DoD does not see it as proprietary.

"If we get FedRAMP Plus right, that ought to become no longer just our own 'plus' requirement, we could have a national standard that is not just for the government, but that applies to everybody," Halvorsen said at DoD's Cloud Industry Day in January. "It would say, 'Okay, if you've got this type of medical data, this is the level of protection it needs.' Commercial, government, academic, anyplace, we ought to have that that level of protection so that it's not overprotected and it's not overpriced. I think we can get a national dialogue started, and I think this group of people here can actually do that."

While DoD is figuring out the data security piece of its cloud puzzle, things get sticky when it comes to data access, Halvorsen has said at a Cloud Computing Caucus Advisory Group meeting. When data is compromised, he said, DoD will want to reach back and touch every place that its data might have been — meaning deep into the recesses of commercial cloud data centers and also across transmission lines. This question remains unanswered: Will CSPs be comfortable, or even capable, of guaranteeing that access, especially when reaching back means accessing not only CSP equipment, but also that of partners and affiliates?

Jack Wilmer, Deputy CTO at DISA, told MeriTalk's Data Center Exchange in March: "It's not that we don't trust commercial CSPs, it's that we want an extra layer of defense in case there is a compromise."

The Pentagon hasn't taken a lead in Federal cloud computing just because of its spending. The agency's role in figuring out thorny data security and access issues with CSPs have made it a leader because it is effectively paving the way for those who follow.

Congress credited DoD for its cloud efforts in a joint statement accompanying the 2015 National Defense Authorization Act, but also said the Pentagon can do more.

“We believe that the Department of Defense has made significant strides in consolidating its data center infrastructure, by maturing its process for evaluating data centers as well as finding opportunities to leverage commercial cloud computing capabilities,” the statement read. “However, as both savings and efficiencies from data center consolidation reach a point of diminishing returns, we believe that DoD can continue to make further progress by also integrating efforts to assess the applications that run on this infrastructure to determine which require dedicated servers and which can potentially be migrated to virtualized or cloud environments.”

Congress directed Halvorsen to identify software applications that DoD can move to the cloud and provide an estimate “of the cloud computing workload needs of DoD, time phased across the future years’ defense plan.” The goal: To inform DoD’s cloud computing needs under the Joint Information Environment initiative and determine how they "might be satisfied by government owned and operated or commercial cloud computing solutions."

Congress also suggested that DoD assess the need to establish cloud service Working Capital Funds to enable its transition to cloud-based solutions.

---


CHAPTER 6

Overcoming Obstacles

Data management and stewardship. Security. Integration. Migration. Portability. Public or private cloud? Which CSP? Can the cloud be trusted? Who's responsible if this idea fails? What happens if there’s a data breach?

The challenges posed by cloud migration go beyond the technical and financial, they go right to culture and psychology.

Box huggers aren’t clutching their servers just because they love them. They fear loss of control and getting blamed for failure. They are comfortable doing things a certain way, and uncomfortable with change.

“Anytime you have an upgrade or migration, you’ll always have hurdles,” said Transportation CIO McKinney. “I don’t think cloud brings its own technical hurdles. When people haven’t done their homework, they’re surprised about how bare bones the cloud is to start. You have to architect in a way that keeps your options open down the road.”

What can box huggers do to make their cloud migration easier? What changes would make cloud migrations easier for all agencies?

Learn About Overcoming Obstacles

Looking at the cloud as a pure technology change is a mistake, said Bray. “We need to both think long term and act more like startups by fundamentally changing the model of how we interact as a public service,” he said.

To overcome obstacles, agencies must untangle:

- Data security concerns
- Internal procurement issues
- Budget issues and who has responsibility for IT spending
- The psychology of the status quo

But box huggers and pioneers alike would benefit from a streamlined, more mature procurement process – at all levels.

CIOs want to buy cloud services as if they are a utility, like electricity, because they are buying computing capacity that can increase or decrease with demand. Indeed, they may get there eventually. But before they can, systems and processes need to be re-engineered and configured to make that possible. That’s why cloud veterans note that there may not be any savings initially, and first-year costs can actually spike. Savings come only over time.

CIOs also have concerns about CSP solutions.

---

More than half (53%) of Federal IT leaders say concerns about being locked into a contract hold their agency back from cloud adoption.

---

The biggest hurdle for moving applications to the cloud stems from lack of maturity in the cloud service provider offerings,” said EPA CIO Dunkin. “For example, the Federal sector currently requires IPv6 adoption and certain security protections for Federal data. The majority of CSPs have been slow in adoption of these requirements because there is little public/commercial demand for them. Therefore, investing in these types of requirements does not necessarily produce the profit margin CSPs might prefer.”

The average Federal cloud contract is 3.6 years. Agencies worry that they’re trading the handcuffs that tie them to their data centers for another pair that ties them to a cloud vendor. More than half of agencies say concerns about being locked into a contract is holding them back from cloud adoption. Agencies also worry about migrating data if they want to make a clean break from one CSP in the future in favor of another. More than three-quarters (78 percent) of Federal IT leaders have worked with a cloud consultant outside their agency, seeking outside advice, and the majority of those said it was very helpful.32

Tailoring procurement to an agency’s specific needs is also a concern. While Blanket Purchase Agreements (BPAs) may work for some, agencies express the desire to pick and choose their cloud additions on a pay-as-you-go basis. They want contracts that enable innovation, rather than binding them into unnecessary obligations.

“Their vendors working with government should provide us with six- or 12-month agreements,” Bray said. “Cloud services that auto-renew are problematic for government to procure. It would be nice for agencies to have the ability to procure Software-as-a-Service via a mechanism similar to the GSA Schedule.”

Agencies also must be better prepared to migrate data and applications to the cloud when they begin their move to the cloud. Almost two-thirds of agencies are not completing a workload analysis to define the data, service, or workload to migrate, and 69 percent are not developing a cost model.33 That lack of preparedness leaves agencies prone to mistakes.

“We need to transform the role of the CIO, their visibility and inter-executive governance over IT spending,” said the White House official. “We’re looking at pain points between CIOs and CFOs.” OMB is expected to clear up some ambiguities that remain about some of the law’s particulars.

Dell Ushers NRC to its Private Cloud

The Nuclear Regulatory Commission (NRC) knew it wanted to reduce its data center footprint, and it launched a cloud migration that allowed it to shutter two data centers. Dell Services Federal Government built and installed an on-premise, Federally compliant private cloud for the NRC. The result? The NRC has moved 450 applications to its new cloud.

“Everything that they had that could go in the cloud is in the cloud,” said Edward Rice, Dell Services Federal Government customer executive.

Dell concluded the project in February 2015.

NRC’s data consolidation effort will cut costs dramatically by reducing operations and maintenance costs. The change will also improve IT efficiency, including reducing down time, because all the applications have been consolidated.

While larger agencies may be more comfortable with public clouds, smaller agencies often feel more at home in a private cloud, said Rice. So do agencies that handle sensitive materials. The NRC is responsible for regulating nuclear power and materials, as well as inspecting nuclear facilities and licensing, so data security represents a major concern for the agency and a private cloud represents an opportunity to save money while protecting critical data and networks.

“An on-premise private cloud allows NRC to manage its own destiny,” he said. And it relieves any anxiety associated with moving to a public cloud.

As cloud computing becomes more mature—and agencies become more comfortable with the technology—Dell believes that hybrid clouds are likely to become a favored cloud deployment model, even among agencies that remain concerned about data security.

---


CHAPTER 7

Grading on a Curve

Clearly DoD, FCC, Commerce, DHS, NASA, NRC, and HHS are pioneers. But most agencies are not nearly so advanced. They lack the resources, experience, leadership, or vision to move ahead more quickly.

The Cloud Computing Caucus Advisory Group asked CIOs and CFOs to grade the progress of their agency’s cloud migration. The answers are revealing: While nearly half of respondents gave their agency a seven (out of 10) when grading their cloud progress, roughly one in three gave their agency a three or less. Agencies were free to use any criteria in their self assessment, and many CIOs believe they have much more to achieve.

“I expect cloud adoption to increase day by day,” said Agriculture’s Valivullah. “Cloud vendors are being flexible to meet the needs of the government. It is a mutually beneficial relationship. Cloud use will only grow.”

Yet it begs the question – are agencies willing to take the leap of faith and commit to the cloud or not?

Valivullah says they are.

“I think cloud use has reached an inflection point in the Federal government,” he said. “I have not met any naysayers to Federal cloud use lately.”

In the end, the biggest driver may be budgets. Will maintaining the status quo become too expensive?

As noted in this paper’s foreword, in 2015, Federal IT spending is expected to reach $79 billion, but spending on legacy systems will still reach $58 billion, according to the GAO’s High Risk List, or nearly 73 cents of every dollar.34

Cloud promises to automate processes, reduce overhead, and streamline operations – and it’s beginning to deliver. When NASA sent the Mars Rover Curiosity to the red planet in 2012, it relied on a cloud infrastructure. “It was 100 times more cost effective with 100 times more data delivered,” Soderstrom said.


Federal agencies in 2015 spent 69 percent of their IT budgets on legacy systems, an expense that many identify as hindering efforts to spend resources on cloud computing.
GSA Overcomes Silos by Moving to the Cloud

Last year, GSA began a five-year project to modernize the Integrated Award Environment (IAE), the eGov suite that manages the government-wide systems for those who award, administer, or receive Federal financial assistance (i.e., grants, loans), contracts, and intergovernmental transactions.

The Common Services program will allow the agency to implement an IAE Platform-as-a-Service (PaaS) capability, which will be used to combine 10 legacy applications onto a single public cloud platform. The Common Services Platform is developed using industry-leading CSPs such as AWS, Docker, Chef, etc.

"We need a modernized environment that will support IAE's new agile development process, continuous integration, and a strong collaboration between our development and operations teams," said Navin Vembar, IAE's Director of Technology Development. "The common services platform will satisfy those requirements."

Munjeet Singh, Vice President, Cloud & Adaptive Architecture at Booz Allen Hamilton, said GSA will boost efficiency and save money in part by retiring the systems that powered the 10 applications that had operated independent of each other.

"Retiring of hardware is a great advantage experienced quickly, but down the road, there will be more efficiency and government reuse they haven't been able to realize yet," said Singh. "We're driving toward a nirvana of PaaS."

Raj Boopathy, Booz Allen Hamilton's Program Manager for the Common Services program, said the PaaS project, orchestrated by Booz Allen Hamilton, will also allow the GSA to share data more quickly and easily. The 10 applications that the IAE relies on were historically siloed, but after the PaaS project is complete users will only have to log on one time in one place to get access to the data from all 10 applications.

"The single pane of glass provides an integrated user experience for the developers to provision their application environment and also enables public users to access the information across the entire environment in a common landing page through Single Sign On," said Boopathy. "The Common Services Platform provides the capabilities to make the integrated user experience possible."

The Common Services program is a significant step forward in GSA's efforts to increase transparency and efficiency and save money in part by retiring the systems that powered the 10 applications that had operated independent of each other.

Successful cloud implementation allows for continuous innovation and updates without any major infrastructure changes. By the time Booz Allen Hamilton completes the five-year project, Singh said, the Common Services Platform will be just as current as it is today.

CHAPTER 8

Conclusion: Chessboards, Rice, and Exponential Growth

GAO's review last September indicated that agencies allocated just two percent of their IT budgets for cloud services in 2014, up from one percent in 2012.35

While a one percentage point increase appears miniscule, it shows a doubling of cloud spending in two years, which could be a sign of rapid growth to come.

Consider the parable of the Chinese emperor, the inventor of the game of chess and the rice. The emperor was so pleased with the game that he told the inventor to name his reward. The inventor asked only for rice in return. "Rice," asked the emperor? How much? The inventor asked for just one grain of rice in exchange for the first square of the chessboard, two grains for the second, four for the third. The emperor thought it a trifling amount. But by the time he had paid off on just the third row of the chessboard, the emperor's stockpiles were gone and the inventor was rich. By the end, the emperor is in debtor's prison and the inventor is living in the palace.

Measuring the growth of Federal cloud computing isn't as easy as counting grains of rice. According to the White House FY 2016 budget request, the Federal government will spend 8.5 percent, or $7.34 billion, of its IT budget on provisioned services, such as cloud – the question, does provisioned services include telecommunications spend? The FY 2016 budget request numbers run counter to the cloud spending projection on OMB's IT Dashboard – which pegs projected spending at $2.1 billion. What's more, the $2.101 billion for cloud programs in 2016 represents a mere 2.3 percent increase over the $2.053 billion in 2015 cloud spending. OMB's data suggests that Federal cloud spending may have plateaued following substantial growth in 2014.

Strong leadership, bold changes, and increased transparency are all essential to continued cloud adoption. Here are three keys to accelerate the adoption of cloud technologies:

1. Tell the Truth

   • For OMB, that means setting real goals and deadlines and then exercising its authority to enforce those deadlines. Allowing the June 4, 2014, deadline for FedRAMP compliance to slip was a mistake that set back the FedRAMP program and introduced confusion to the marketplace – in both the buyer and supplier communities

   • Increase transparency. Suggesting that 8.5 percent of Federal IT spending will go toward “cloud and other provisioned services,” when actual cloud spending is barely a quarter of that, is obfuscation, not transparency. Nobody wins by wallpapering over the cracks – nothing is gained by creating inflated expectations, followed hard by disappointment. Define the spend. Break out cloud from “provisioned” services. Report real progress

Market Share

**Q1 2014**

- **Amazon AWS** $1 billion
- **Salesforce** $0.1 billion
- **Google** $0.2 billion
- **IBM** $0.2 billion
- **Microsoft** $0.3 billion

**Q1 2015**

- **Amazon AWS** $1.5 billion (growth: +49%)
- **Salesforce** $0.3 billion (growth: +34%)
- **Google** $0.3 billion (growth: +74%)
- **IBM** $0.4 billion (growth: +56%)
- **Microsoft** $0.6 billion (growth: +96%)

Source: Synergy Research Group

---

**2. Change the Game**

- **Accelerate FedRAMP.** Its job is too important and too big for the program as it’s designed now. FedRAMP staffing is insufficient to the task, and delays will continue unless the office gains more resources – people and funding. It is startling that 17 of the 25 CSPs who were awaiting FedRAMP certification one year ago remain in the pipeline. At the same time, new approaches should be explored to expedite certification and adoption.

- **Streamline acquisition and budgeting.** Agencies need financial tools to manage the leap from legacy to cloud technologies. Implementing a revolving capital fund for cloud investment within GSA could provide resources for agencies to migrate more rapidly to cloud services. The CDM revolving capital fund provides a clear established precedent. The concept allows agencies to escape the tyranny of annual budgets, by providing cash for the upfront costs associated with migrating an application. Congress also has established a precedent, suggesting that DoD assess the need to establish a working capital fund to enable its transition to cloud-based solutions.

- **Provide incentives and reward success.** Agencies that embrace cloud and can demonstrate real savings as a result should be rewarded for their efforts by allowing them to keep the savings and reinvest them to tackle other IT modernization projects.

- **Speed the certification process.** The three paths CSPs may follow to gain Authority to Operate are not seen as equal. Vendors see the Joint Authorization Board as the gold standard for certification, because it carries the imprimatur of DoD, DHS, and GSA. But this job is too large to be given to three CIOs laboring at it on a part-time basis. Alternative paths must be developed, seen, and treated as equal.

- **Encourage and nurture public-private collaboration to exchange best practices and ignite innovation and progress.**

---

**3. Think Bigger**

- **Data is ballooning, and the pace of growth is accelerating.** The power of data analytics is yet to be tapped. Much of the low-hanging cloud migration fruit – email, collaboration technologies, and content management systems – has already been plucked. But enormous opportunities remain. Agencies now must be open to re-inventing processes, adopting new technologies, and serious soul-searching about how and where cloud solutions can help save money, speed development, improve services, and increase mission effectiveness. The real promise of cloud is in re-inventing processes to find better, more efficient, agile, and cost-effective ways to deliver services and accomplish goals. Cloud computing will make the unimaginable possible. But only if agencies are willing to open their minds and imaginations to the possibilities – and boldly take their computing needs to the cloud.

- **Vivek Kundra’s “Cloud First” vision must be renewed and reinvigorated.** As the new Federal CIO, Tony Scott has a unique opportunity to reinforce and revitalize the Federal cloud transition. Any time agencies invest in new IT infrastructure or re-compete existing systems, the presumption should be that cloud is the first option. Agencies should be required to justify themselves when they choose not to use a cloud solution. Enforcing a Cloud First policy must be the new normal.

So, peel your fingers off that box – the future isn’t in your data center. It’s in the cloud.
CHAPTER 9

Epilogue

On hurdles:

“Cloud is going to take some middlemen out of the picture. You have to think of HR consequences for those resisting the cloud. Their jobs don’t go away, but become more important.”

– Tom Soderstrom, NASA JPL

On change:

“We have an obligation to force our workforce to grow instead of atrophy. Cloud enables them to learn more and new skills so they can later shift to different work.”

– Ann Dunkin, CIO, EPA

On strategy:

“Be very deliberate about killing off the stuff that’s not going to survive the move to the cloud. We’re great at launching new things but getting rid of the old stuff is part and parcel of that journey.”

– Tony Scott, Federal CIO, at the Data Transparency Coalition’s Financial Regulation Summit