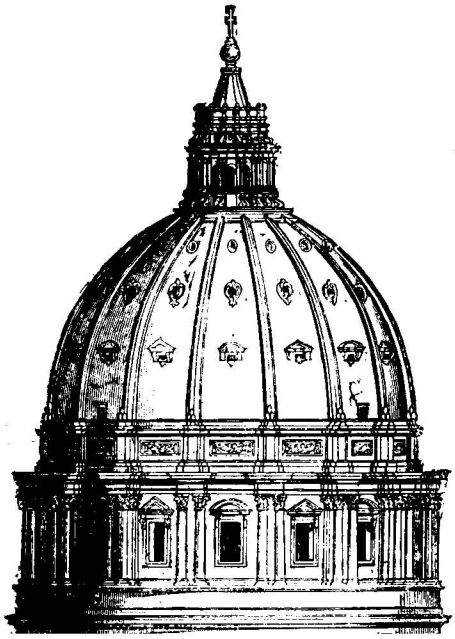
ISSUE BRIEF #6/2012



2012 Federal Cloud Review

BY DEBORAH COLLIER
Citizens Against Government Waste

CITIZENS AGAINST GOVERNMENT WASTE

1301 Pennsylvania Avenue, N.W.
Suite 1075
Washington, D.C. 20004

1-800-BE-ANGRY

www.cagw.org

CITIZENS AGAINST GOVERNMENT WASTE

Citizens Against Government Waste (CAGW) is a private, nonprofit, nonpartisan organization dedicated to educating the American public about waste, mismanagement, and inefficiency in the federal government.

CAGW was founded in 1984 by J. Peter Grace and nationally-syndicated columnist Jack Anderson to build support for implementation of the Grace Commission recommendations and other waste-cutting proposals. Since its inception, CAGW has been at the forefront of the fight for efficiency, economy, and accountability in government.

CAGW has more than one million members and supporters nationwide. Since 1986, CAGW and its members have helped save taxpayers more than $1 trillion.

CAGW publishes a newsletter, *Government WasteWatch,* and produces special reports, and monographs examining government waste and what citizens can do to stop it.

CAGW is classified as a Section 501(c)(3) organization under the Internal Revenue Code of 1954 and is recognized as a publicly-supported organization described in Section 509(a)(1) and 170(b)(A)(vi) of the code. Individuals, corporations, companies, associations, and foundations are eligible to support the work of CAGW through tax-deductible gifts.

1301 Pennsylvania Avenue, NW
Suite 1075
Washington, DC 20004
1-800-BE-ANGRY
www.cagw.org

EXECUTIVE SUMMARY

On December 1, 2010, the General Services Administration (GSA) announced that it would become the first federal agency to deploy a cloud-based email system (Email-as-a-Service or EaaS). GSA anticipated saving up to $15 million over five years with the new system.[1]

While GSA's Office of Inspector General has been unable to verify the expected savings due to inadequate cost analysis at the agency, it is the potential for savings such as these that has encouraged adoption of cloud computing strategies.[2] On December 9, 2010, the Obama Administration announced its 25 Point Implementation Plan to Reform Federal Information Technology Management (25 Point Plan),[3] encouraging federal agencies to quickly adopt cloud computing tools and consider "cloud-first" when making new information technology (IT) purchases in order to manage information in a cost-effective manner.

Federal spending on cloud computing is expected to total $11.2 billion between 2012 and 2017.[4] These cloud services include public, private and shared service models, ranging from EaaS and cloud-based web hosting to large scale Infrastructure-as-a-Service (IaaS). In the fall of 2011, Citizens Against Government Waste (CAGW) published issue briefs on cloud computing[5] and best practices for cloud procurement[6] to assist federal decision makers on cloud purchases.

While progress has been made in expanding cloud services, a July 11, 2012, Government Accountability Office (GAO) report indicated there are several roadblocks remaining in the path to full implementation and adoption.[7] Among these challenges are meeting federal security requirements, obtaining guidance on deployment, acquiring internal cloud knowledge and expertise, certifying and accrediting vendors, ensuring data portability and interoperability, overcoming cultural barriers, and procuring services on a consumption or on-demand basis. Addressing these concerns is critical for successful cloud adoption by federal agencies.

---

[1] Steve Hoffman, "GSA Becomes First Federal Agency to Move Email to the Cloud Agencywide," U.S. General Services Administration, GSA #10694, December 1, 2010, http://www.gsa.gov/portal/content/208417.

[2] "Audit of GSA's Transition from Lotus Notes to the Cloud," Report Number A120131/O/F/F12004, Office of the Inspector General, U.S. General Services Administration, September 28, 2012, http://www.gsaig.gov/?LinkServID=1C91FE07-FF0A-7F2A-F5EC7659D924AE6D&showMeta=0&fileExt=.pdf.

[3] "25 Point Implementation Plan to Reform Federal Information Technology Management," U.S. Office of Management and Budget, December 9, 2010, https://cio.gov/wp-content/uploads/downloads/2012/09/25-Point-Implementation-Plan-to-Reform-Federal-IT.pdf.

[4] John K. Higgins, "Federal Cloud Adoption, Part 2: Raining Contracts," *E-Commerce Times,* May 16, 2012, http://www.ecommercetimes.com/story/75125.html.

[5] Deborah Collier, "Cloud Computing 101: A Brief Introduction," Citizens Against Government Waste, September 2011, http://www.cagw.org/assets/reports/issue-brief-2011-9.pdf.

[6] Deborah Collier, "Cloud Computing 201: Guidelines for Successful Cloud Investments," Citizens Against Government Waste, November 2011, http://www.cagw.org/assets/reports/cloud_computing_201.pdf.

[7] "Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned," U.S. Government Accountability Office, GAO-12-756, July 11, 2012, http://www.gao.gov/assets/600/592249.pdf.

This report reviews federal IT spending, obstacles to widespread cloud adoption, GSA's implementation of the federal risk and authorization management program (FedRAMP), cloud brokering and other new options for cloud purchasing and management, the stability and security of cloud services, and digital government strategy as it relates to cloud computing.

FEDERAL INFORMATION TECHNOLOGY SPENDING

In fiscal year (FY) 2011, there were approximately 7,200 IT investments at the federal level totaling at least $79 billion. In FY 2012, federal agencies spent nearly $74 billion on 6,814 IT investments.[8] These expenditures include software and hardware upgrades and improvements, upgrades to legacy IT systems, data migration to virtual servers, consolidation of data centers, provisioning telecommunications support, maintenance on existing systems, provisioning cybersecurity efforts, development and improvement of mobile apps, and migration efforts to cloud services.

In 2011 and 2012, GAO issued two reports identifying a number of duplicative services and systems that have the potential to save taxpayer dollars through either consolidation or elimination. The first report, "Opportunities to Reduce Potential Duplication in Government Programs, Save Tax Dollars, and Enhance Revenue," published on March 1, 2011, identified 34 agencies, offices, and initiatives that provide similar or identical services to the same populations, along with 47 programs that are either wasteful or inefficient.[9] On February 28, 2012, GAO issued its second report highlighting significant cases of duplication, overlap and lack of coordination between agencies and programs.[10] Senators Tom Coburn (R-Okla.)[11] and Jeff Sessions (R-Ala.)[12] estimate that the two GAO reports identify $400 billion annually in overlap and duplication.

One source of duplication identified by the two GAO reports is IT procurement. The March 2011 GAO report stated that the number of data centers had increased from 432 in 1998 to more than 2,000 in 2010.[13] In February 2010, Office of Management and Budget (OMB) and

---

[8] Federal IT Dashboard, November 13, 2012, http://www.itdashboard.gov.

[9] "Opportunities to Reduce Potential Duplication in Government Programs, Save Tax Dollars, and Enhance Revenue," U.S. Government Accountability Office, GAO-11-318SP, March 2011, http://www.gao.gov/assets/320/315920.pdf.

[10] "2012 Annual Report: Opportunities to Reduce Potential Duplication, Overlap and Fragmentation, Achieve Savings, and Enhance Revenue," U.S. Government Accountability Office, GAO-12-352SP, February 2012, http://www.gao.gov/assets/590/588818.pdf.

[11] Senator Tom Coburn, "Dr. Coburn Says GAO Report Exposes Widespread Waste and Duplication in Federal Budget," February 28, 2011, http://www.coburn.senate.gov/public/index.cfm/pressreleases?ContentRecord_id=9f71c934-b926-47ee-a6f8-662d5225517f.

[12] Senator Jeff Sessions, "GAO Finds More Than $400 Billion Spent Each Year On 1,500 Duplicative, Fragmented, Inefficient Programs," February 28, 2012, http://budget.senate.gov/republican/public/index.cfm/files/serve?File_id=5b942c34-d1e5-49de-be92-a85dad8aa191&SK=42ED5BBA6767481D74B2057AC359ACD4.

[13] GAO-11-318SP, page 66.

the federal Chief Information Officer (CIO) announced the federal data center consolidation initiative, which is supposed to lead to the consolidation of 1,200 data centers by the end of 2015.[14] Not only will the consolidation effort improve efficiency, but GAO anticipates it will also reduce the cost of data center hardware, software purchases, maintenance, and center operations. The report also identified the use of enterprise architecture by federal agencies as an area that could use improvement, calling the agencies' efforts a "work in progress." The report included one example of success at the Department of the Interior, which used enterprise architecture to modernize its IT operations, and reduced expenditures by at least $80 million.[15]

The February 2012 GAO report stated that even though OMB issued guidance on how to report IT investments to agencies, this does not ensure that duplicative investments are identified or properly reported.[16] GAO reviewed IT investments at the Department of Defense (DOD), Department of Energy (DOE) and Department of Homeland Security (DHS) and found that of the 810 investments sampled, 37 were potentially duplicative, accounting for about $1.2 billion in IT spending for FY 2007 through FY 2012.[17] GAO recommended that agencies identify potential duplicative investments prior to making additional purchases by using adequate inventory controls and internal auditing tools.

On top of the duplication and overlap, there is little coordination of the IT acquisition process, with several divisions within a department or agency having the ability to perform their own contracting without consulting with any other divisions. For example, a July 15, 2011, article in Nextgov reported that the DHS Office of Inspector General found that, since 2010, individual divisions within the agency had purchased $3.2 billion of metal detectors, explosive detection systems and radiation detectors. According to the report, had the agency utilized a practice known as strategic sourcing, it could have better managed the purchase of this equipment and reduced costs.[18]

In addition to duplicative hardware and equipment purchases, the government buys unnecessary or excessive software licenses because of inadequate tracking of the IT software licenses that agencies currently own or use. Therefore, it is difficult for agencies to procure licenses and services on an on-demand or consumption basis.

---

[14] Federal Data Center Consolidation Initiative (FDCCI) Data Center Closings 2010-2013, November 19, 2012, https://explore.data.gov/Federal-Government-Finances-and-Employment/Federal-Data-Center-Consolidation-Initiative-FDCCI/jv3c-8kqr.

[15] GAO-11-318SP, page 64.

[16] GAO-12-352SP, page 133.

[17] Ibid., page 134.

[18] Aliya Sternstein, "DHS' Failure to Leverage Large Technology Buys Costs Billions in Lost Savings," *Nextgov Technology and the Business of Government,* 2011, http://www.nextgov.com/nextgov/ng_20110715_9845.php?oref=topnews.

As pointed out in a March 10, 2010, article in *CIO Magazine,* these purchases are often made using "seat licensing" or enterprise license agreements. Such seat licensing agreements require a thorough knowledge of software licenses and usage prior to contracting for additional software licenses or seats.[19] On July 19, 2011, GAO criticized government agencies' inventory management at federal data centers, noting that 15 federal agencies did not list all software assets in their reports.[20] This lack of information on software assets and usage impairs decision-making on both future software licensing needs and the procurement of software on an on-demand or consumption basis through the cloud.

On April 27, 2012, *Federal Computer Week* reported the results of an April 25, 2012, survey of 108 federal civilian and DOD personnel by MeriTalk Cloud Computing Exchange. The survey found that approximately $5.5 billion has been saved annually from the adoption of cloud computing tools.[21] The article also stated that, had there been broader adoption of cloud computing services by agencies, the federal government could have potentially saved $12 billion per year.[22] MeriTalk released a second survey targeting federal IT managers in September 2012, which indicated the managers anticipated savings of up to $16 billion annually through the use of cloud computing tools.[23] These figures are far greater than the $5 billion in annual savings estimated by former federal CIO Vivek Kundra when he first discussed the administration's cloud-first initiative.[24]

As one example of how modernizing IT can save money, on July 30, 2012, *Government Security News* reported that DHS had reduced its IT budget by $40 million for FY 2013, and expects further reductions in its FY 2014 budget request.[25] Savings like these come from a shift from stand-alone legacy systems to integrated public and private cloud computing solutions that can eventually incorporate mobile computing solutions such as Smartphones, laptops and other mobile devices, and potentially allow employees to participate in "bring your own device" programs (BYOD), which could further reduce the hardware cost burden to the federal government.

---

[19] Thomas Wailgum, "Enterprise Software Licensing: New Options, New Headaches," *CIO Magazine,* March 16, 2010, http://www.cio.com/article/580013/Enterprise_Software_Licensing_New_Options_New_Headaches.

[20] "Data Center Consolidation: Agencies Need to Complete Inventories and Plans to Achieve Expected Savings," U.S. Government Accountability Office, GAO-11-565, July 19, 2011, http://www.gao.gov/new.items/d11565.pdf.

[21] "Cloudy with a Chance of Savings Study," MeriTalk Cloud Computing Exchange (CCX), April 25, 2012, http://www.meritalk.com/ccx/chanceofsavings.

[22] Camille Tuutti, "Cloud Could Squeeze Even More Savings, Says Survey," *Federal Computer Week,* April 27, 2012, http://fcw.com/articles/2012/04/27/meritalk-survey-cloud-computer-savings.aspx?sc_lang=en.

[23] Joseph Marks, "Feds Predict $16.6 Billion in Cloud Savings, Triple OMB's Estimates," Nextgov, September 18, 2012, http://www.nextgov.com/cloud-computing/2012/09/feds-predict-166-billion-cloud-savings-triple-ombs-estimates/58193/?oref=ng-channelriver.

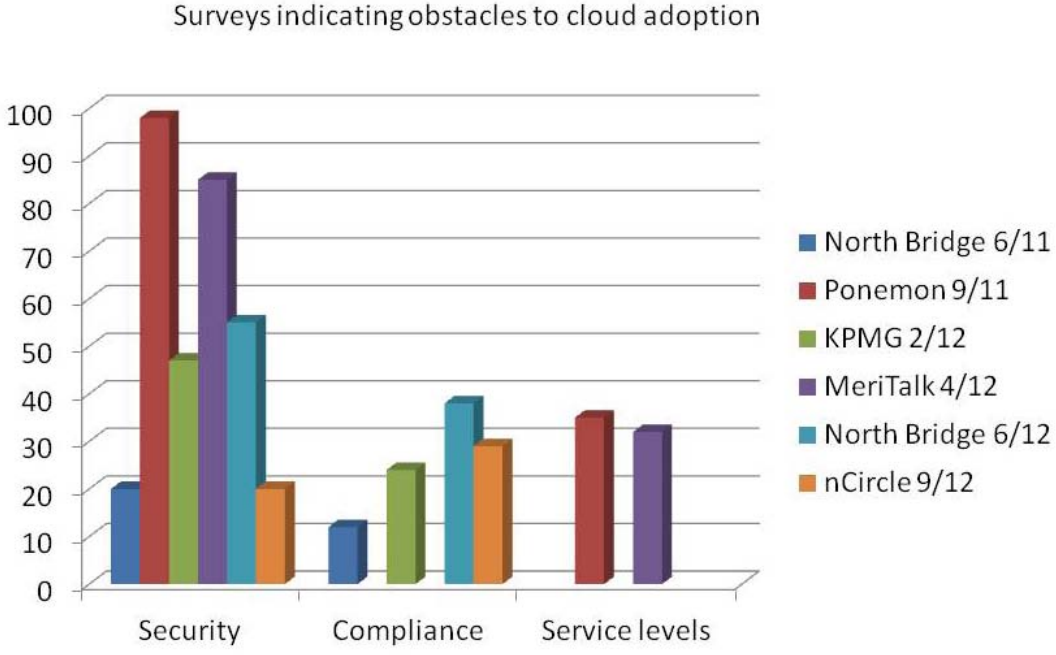
[24] Elizabeth Montalbano, "Government CIOs Doubt Cloud Savings," *Information Week,* May 26, 2011, http://www.informationweek.com/government/cloud-saas/government-cios-doubt-cloud-savings/229700072.

[25] Stephanie Sullivan, "IT Spending at DHS: High Technology Meets Budget Realities," *Government Security News,* July 30, 2012, http://www.gsnmagazine.com/node/26893?c=access_control_identification.

OBSTACLES TO ADOPTION OF CLOUD COMPUTING

As part of the Obama administration's "cloud-first" strategy for IT procurement, federal agencies are moving various services, including email, legacy software, archival services, public website hosting and infrastructure services to a cloud environment. The cloud-first strategy directed federal agencies to identify at least three IT services that could be moved to the cloud by February 2011 with implementation of at least one cloud service by December 2011 and three services by June 2012.

While agency officials are aware of the financial benefits to moving services to the cloud, several surveys over the past two years have indicated that obstacles to cloud adoption remain. These include security concerns, compliance with regulations, IT governance, problems with service level agreements, and interoperability, with the highest number of respondents listing security in the cloud as their top concern.



North Bridge Venture Partners, June 22, 2011, 2011 Future Cloud Computing Survey, http://northbridge.com/2011-cloud-gallery

Ponemon Institute Study, September 5, 2011, http://safegov.org/media/23573/ponemon_survey_raw_results.pdf

KPMG Global Study of Government Cloud Adoption, February 29, 2012, http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPablications/Documents/exploring-cloud.pdf

Meritalk Cloudy with a Chance of Savings, April 25, 2012, http://www.meritalk.com/pdfs/ccxappsvscash/MeriTalk_CCX_Brainstorm_Press_Release_042512_FINALpdf

North Bridge Venture Partners, June 20, 2012 Future Cloud Computing Survey, http://northbridge.com/2012-future-cloud-computing-survey-exposes-hottest-treds-cloud-adoption

nCircle, September 7, 2012, http://www.ncircle.com/index.php?s=resources_surveys_Security-Compliance-2012

The concerns of federal IT users in adopting cloud strategies are further evidenced in a July 11, 2012, GAO report entitled "Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned."[26] GAO issued the report as a follow-up to the administration's

[26] "Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned," GAO Report No. GAO-12-756, July 11, 2012, http://www.gao.gov/assets/600/592249.pdf.

cloud-first initiative. While GAO found that agencies have made progress in implementing cloud computing, it also detailed challenges for agencies trying to meet the deadlines for the cloud-first policy. Of the 20 plans submitted to date to OMB, every agency cloud program, except the Department of the Treasury's Document Management and Freedom of Information Act Case Management program, were missing key elements including estimated costs and plans for retiring or repurposing existing legacy systems.

Among the other problems reported by GAO were meeting federal security requirements; obtaining guidance for cloud procurement and deployment; acquiring knowledge and expertise in cloud computing; certifying and accrediting vendors; ensuring data portability and interoperability; overcoming cultural barriers; and, procuring services on a consumption or on-demand basis.

FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM (FEDRAMP)

One of the top challenges cited in the surveys and GAO reports as an obstacle to cloud adoption is the need for government agencies to meet the security requirements of the Federal Information Security Management Act. This concern is one of the driving forces behind the development of the Federal Risk and Authorization Management Program (FedRAMP).

FedRAMP is managed by GSA under a December 11, 2011, OMB memorandum to streamline the security certification process of cloud computing purchases.[27] GSA uses a framework for FedRAMP that has been co-developed by cloud and cybersecurity experts at GSA, National Institutes of Standards and Technology (NIST), DHS, DOD, the National Security Agency (NSA), OMB, federal CIOs and private industry. FedRAMP is expected to streamline the security certification process for government agency purchases of cloud computing tools and services.

According to a December 8, 2011, article in *Politico*, federal agencies will be required to use FedRAMP to certify that vendors meet the government's minimum security standards for cloud services instead of wasting time and taxpayer dollars creating their own separate processes for approval.[28] Cloud service providers also are permitted to apply directly to the FedRAMP program for authorization to operate in the federal environment.

But even with a standardized security certification process, there are questions as to whether FedRAMP will meet the needs of all federal agencies. A January 19, 2012, *Government Computer News* article suggested that reliance on FedRAMP standards may not be sufficient for agencies requiring more robust security levels, such as DOD, NSA and DHS, even though they were involved in developing

[27] Steven VanRoekel, Federal Chief Information Officer, "Security Authorization of Information Systems in Cloud Computing Environments: Memorandum for Chief Information Officers," Office of Management and Budget, December 11, 2011, http://www.cio.gov/fedrampmemo.pdf.

[28] David Saleh Rauf, "W.H. Pushes Cloud Rollout," *Politico,* December 8, 2011, http://www.politico.com/news/stories/1211/70135.html.

the standards.[29] While FedRAMP creates a baseline of minimum standards for security, continuous monitoring, and independent verification and validation of implementation, it is up to each federal agency to determine which additional requirements are necessary to meet its mission needs.

GSA has begun accepting applications from vendors for FedRAMP security approvals.[30] According to a June 7, 2012 article in *Government Computer News*, the agency plans to have three cloud providers accredited under FedRAMP by the end of 2012.[31]

CLOUD BROKERING AND OTHER NEW PROCUREMENT PROCESSES

According to NIST, a cloud broker manages the use, performance and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers offering either a simple or stable interface between customers and providers, even when providers change.[32] On June 26, 2012, the DOD announced it would set up its own cloud brokerage services. In a memorandum to DOD leadership, CIO Teri Takai determined that the Defense Information Systems Agency (DISA) would act as DOD's cloud broker for cloud computing purchases.[33] On July 6, 2012, GSA followed DOD's announcement with a solicitation for a request for information (RFI) on cloud brokering to learn more about "how government could leverage the key characteristics and advantages of cloud computing to save money and increase IT efficiencies."[34]

Several other federal agencies have begun to seek information on additional business processes from the private sector. For example, with its current contract for cloud based web hosting services expiring at the end of 2012, the Department of the Treasury issued an RFI on July 3, 2012, to learn more about new technologies and services now available in the cloud computing marketplace.[35] The current contract was set for 12 months with a one-year extension to set up web hosting services and web site redesign with Amazon Web Services. Based on the information received by July 16, 2012, it

---

[29] Rutrell Yasin, "Could Agencies' Individual Needs Break FedRAMP?" *Government Computer News,* January 19, 2012, http://gcn.com/articles/2012/01/19/fedramp-cloud-agencies-security.aspx.

[30] John K. Higgins, "Feds Spark Boomlet for Risk Assessment Vendors," *Tech News World,* July 3, 2012, http://www.technewsworld.com/story/75538.html.

[31] Rutrell Yasin, "FedRAMP Aims to Authorize 3 Cloud Providers by Year's End," *Government Computer News,* June 7, 2012, http://gcn.com/articles/2012/06/07/fedramp-authorize-cloud-service-providers.aspx.

[32] Lee Badger and Tim Grance, "Standards Acceleration to Jumpstart Adoption of Cloud Computing (SAJACC)," National Institute of Standards and Technology, May 20, 2010, http://csrc.nist.gov/groups/SNS/cloud-computing/documents/forumworkshop-may2010/nist_cloud_computing_forum-badger_grance.pdf.

[33] David Stegon, "DISA to be DOD Cloud Services Broker," *Fed Scoop,* July 11, 2012, http://fedscoop.com/disa-to-be-dod-cloud-services-broker/.

[34] "Federal Acquisition Services Cloud Brokerage Request for Information," General Services Administration, July 17, 2012, Solicitation Number: QTA00AH12BRI0002, ITS Office of Acquisition Operations (QTA), https://www.fbo.gov/index?s=opportunity&mode=form&id=0e4bbe369331309722bb4f6429c5f80a&tab=core&_cview=0.

[35] "Public Cloud Webhosting Services," Department of the Treasury, July 3, 2012, Solicitation Number: 732012, Internal Revenue Service (IRS), National Office Procurement (OS: A:P), https://www.fbo.gov/index?s=opportunity&mode=form&id=1553ada859e30065fe3768994ea58ca7&tab=core&_cview=0.

is anticipated that Treasury will submit a Request for Proposal (RFP) for various cloud computing services that will include new technologies discovered through the RFI process.

During an August 2, 2012, GSA industry day, federal agency officials were asked about the challenges agencies face using existing procurement methods to purchase cloud services. Among the challenges mentioned at the forum were service level agreements; security; the use of a funding model not ideal for procuring cloud services; vendor lock-in; portability and standardization.[36] It is apparent from these responses that agencies are seeking simplified cloud services procurement mechanisms to better enable them to achieve the expected savings. One of the methods currently being considered to address these challenges is using cloud brokers who would act as intermediaries between agencies and cloud services providers.

An August 12, 2012, article in *Forbes* magazine on GSA's industry day reported that several federal and state agencies are reviewing cloud brokering as a procurement option, including DHS and the Department of Health and Human Services (HHS).[37] According to an August 13, 2012, *Government Computer News* article, NASA's Jet Propulsion Laboratory is also looking at the option of using a cloud broker with the caveat that it would have to provide added value to cloud computing offerings.[38]

Just as FedRAMP was established to streamline the security certification process for cloud vendors, the use of new, innovative methods to manage and simplify the procurement of cloud services will improve the ability of federal agencies to create overall successful cloud computing strategy.

SECURITY AND STABILITY IN CLOUD COMPUTING

Cloud computing must protect the security and stability of agency IT systems, along with all data and personal information. This was of particular importance following the July 2012 storms that swept through the Mid-Atlantic, shutting down power in the region and affecting operations at a cloud vendor's data storage facility. Although no federal systems were affected, the storm became a prime example of the importance of developing redundant back-up systems and implementation plans should a primary system be disabled for a period of time.

In an October 25, 2011, speech at the Churchill Club in Palo Alto, California, federal CIO Steve VanRoekel cited security as a key component of the administration's new shared-first initiative,

[36] "GSA Cloud Brokerage Industry Day" PowerPoint presentation, Federal Business Opportunities, August 2, 2012, https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=3bfb1810a6e8ac05bd58a528786688f6&_cview=0.

[37] Kevin L. Jackson,, "Cloud Management Broker: The Next Wave In Cloud Computing," *Forbes,* August 12, 2012, http://www.forbes.com/sites/kevinjackson/2012/08/12/cloud-management-broker-the-next-wave-in-cloud-computing/.

[38] Rutrell Yasin, "Cloud Brokerages Get Popular, But Are They Ready for Prime Time?" *Government Computer News,* August 13, 2012, http://gcn.com/Articles/2012/08/13/NJVC-Gravitant-Cloud-Brokerage-Prime-Time.aspx?Page=1.

aimed at eliminating waste and duplication in federal IT spending.[39] In his announcement, he discussed how technologies like cloud, mobile, web platforms and servers have matured to the point at which they play a key role in transforming every aspect of government. But as services increasingly move online, there must be increased vigilance against new threats that evolve daily. VanRoekel stated, "Consolidating data centers, shutting down legacy systems, and moving to the cloud all offer opportunities to enhance our cyber security posture. The private sector is already taking advantage of recent advances in cloud technology to make their systems even more secure. Going forward, we must build on top of a sound foundation of cyber security to ensure Americans and our government is safe."

Other methods to improve security and stability include selecting the appropriate programs and applications to be placed in a public cloud, such as public facing websites, application development and testing, online product catalogs and product documentation; evaluating existing security and increasing IT security when necessary; identifying and using the right third-party auditing services to determine whether the services being provided are giving the agency the best value; adding authentication layers; determining the effect of additional security on integration; placing security at the forefront of service level agreements; insisting on a transparent security process; streamlining logging and monitoring; adding encryption; and spreading risk with multiple, redundant cloud service providers.[40]

CLOUD COMPUTING AND THE DIGITAL GOVERNMENT STRATEGY

The administration's 25 Point Plan focuses on cloud computing, shared services, modular approaches for IT development and acquisition, and IT program management.[41] On May 23, 2012, the White House announced the administration's digital government strategy, which integrates the components of the 25 Point plan to provide digital information to citizens using current technologies such as Smartphones, tablets and other mobile devices, as well as building on the relationship between device and resources to create web strategies and virtual client desktops.[42]

A 2012 special report from *Government Computer News* discussed the administration's digital government strategy, which advances client virtualization as a necessary step for agencies migrating to cloud computing. According to the report, client virtualization centralizes control

[39] Steven VanRoekel, Federal Chief Information Officer, Speech at the Palo Alto Research Center, Churchill Club, Palo Alto, California, October 25, 2011, http://www.whitehouse.gov/sites/default/files/svr_parc_speech_final_0.pdf.

[40] Nari Kannan, "10 Ways to Ease Public Cloud Security Concerns," *CIO Magazine,* August 13, 2012, http://www.cio.com/article/713524/10_Ways_to_Ease_Public_Cloud_Security_Concerns.

[41] "25 Point Implementation Plan to Reform Federal Information Technology Management," U.S. Office of Management and Budget, December 9, 2010, https://cio.gov/wp-content/uploads/downloads/2012/09/25-Point-Implementation-Plan-to-Reform-Federal-IT.pdf.

[42] "Digital Government: Building a 21st Century Platform to Better Serve the American People," Office of Management and Budget, The White House, May 23, 2012, http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government-strategy.pdf.

of client operations away from local branch offices into a single centralized control system, which would allow agencies to monitor and maintain IT systems remotely.[43] Among agencies considering client virtualization as part of their overall cloud strategy are DOE and the National Nuclear Security Administration as part of a secure hybrid community cloud; DHS and HHS, which have already undergone client virtualization pilot programs; and the U.S. Census Bureau and DISA. Agencies are finding that the total cost of ownership for virtual client infrastructure is less expensive due to reduced costs for managing PCs, including PC replacement, support, and software distribution.[44]

The administration's digital government strategy also promotes the use of mobile computing, which relies on cloud computing services to access and store information. The strategy proposes that federal employees bring their own devices (BYOD) to work for use on agency networks. These devices can include Smartphones, tablets and laptops owned by the employee but used to access work-related information. BYOD is intended to create an environment in which employees use devices with which they are most comfortable, while saving taxpayer dollars by reducing equipment costs.

However, challenges remain to the BYOD program. As noted in an August 22, 2012, *Government Computer News* article, there are legal, reimbursement and security issues that must be addressed in order to make the information on these types of devices secure and under control by the government. Because the government does not own the devices, and many employees may have used them for some time, the data stored on them could already be compromised.[45]

A June 22, 2012, article in Nextgov provided a vision for BYOD in the federal workplace from the perspective of Department of Veterans Affairs (VA) CIO Roger Baker. Baker predicted that in five to six years, the VA would no longer furnish employees with a government-owned computer, relying instead on employees to provide their own devices to access agency information on the network.[46] Cloud computing enables and supports the concept of BYOD by placing information in cloud storage solutions and using IaaS models to provide greater access to information by individuals using devices with which they are most comfortable. However, it also means that there will be more mobile platforms being used in the federal workplace including Apple's iOS, Android OS, Blackberry, Windows, and whatever else may be developed.

According to Nextgov, in October 2011, VA initiated a pilot program testing the use of mobile devices by issuing 1,000 government-owned iPads. During the pilot program, VA found that using BYOD requires additional security measures to protect mission-critical information. Although the pilot was limited to iPads,

[43] "GCN Special Report: Modern Client Computing Relies on Centralized Management Control," *Government Computer News,* Special Report, 2012, http://gcn.com/microsites/2012/snapshot-client-computing/01-client-management-central-control.aspx.

[44] Ibid.

[45] Rutrell Yasin, "As BYOD Gains Fed Acceptance, Assume Devices Been Hacked, Protect the Data," *Government Computer News,* August 22, 2012, http://gcn.com/Articles/2012/08/22/BYOD-CIO-panel-technology-legal-issues.aspx?Page=2.

[46] Bob Brewin, "Agency-owned PCs Could Soon Be Relics of a Bygone Era," Nextgov, June 22, 2012, http://www.nextgov.com/cio-briefing/2012/06/agency-owned-pcs-could-soon-be-relics-bygone-era/56408/.

employees may also bring other devices using different operating systems into the information ecosystem. This necessitates new requirements for mobile apps developed by federal agencies as part of the digital government strategy. However, as noted in a September 25, 2012, issue brief published by CAGW, the government continues to develop mobile apps for use on a limited number of mobile platforms.[47]

For example, on August 9, 2012, the Census Bureau released a mobile app for public use to obtain information on 16 economic indicators. However, this mobile app is available only on Android devices, with a separate app for Apple iOS expected to be developed at a later date. The government currently has no plans to develop a similar app for Windows or Blackberry devices.[48] Many mobile apps developed by the federal government unfortunately will work on only one type of mobile device.

While industry leaders are in favor of the digital government strategy, they remain cautious, citing concerns about interagency cooperation and collaboration, as well as legislative, regulatory, budgetary, procurement and authority issues.[49] For the administration's digital government strategy to be effective, agency CIOs must not only consider the current state of technology, but also plan ahead for future developments and innovations by developing applications in a platform-neutral manner.

CONCLUSION

Cloud computing is no longer in its infancy. It is a maturing and robust tool used by both the private sector and federal government to save money while using technology more efficiently. The federal government currently spends between $70 and $80 billion annually on IT. As FedRAMP continues to gear up and accept applications and certifies additional vendors to supply the federal government with cloud computing services, there will be a greater shift toward using these IT tools. With new interest in cloud brokerage, there should be additional methods for federal agencies to shop for cloud services.

Federal IT will continue to transform, as agency CIOs find more ways to use cloud computing and enhance new technologies. Along with continued security concerns, federal IT managers will face new challenges to cloud computing, including the desire of employees to bring their own mobile devices, such as tablets, notebooks and Smartphones into the workplace; the need to create a higher standard for inventory management; and, avoiding the creation of duplicative systems.

Much work still needs to be done in order to assure federal IT professionals that the information they will be storing remotely in the cloud will be secure. Finally, the appropriate budget tools must be used to obtain the greatest savings possible from the cloud.

---

[47] Deborah Collier and Aaron Swensen, "Government Mobile Apps Proliferate," Citizens Against Government Waste Issue Brief No. 4, September 25, 2012, http://www.cagw.org/assets/issue-brief-2012-10-mobile-apps-web.pdf.

[48] Adam Mazmanian, "Census Debuts New Economic Indicators App," *The National Journal,* August 9, 2012, http://www.nationaljournal.com/tech/census-debuts-new-economic-indicator-app-20120809.

[49] Camille Tuutti, "Industry Members Laud Digital Government Strategy," *Federal Computer Week,* August 17, 2012, http://fcw.com/articles/2012/08/17/act-iac-industry-response-digital-government.aspx.