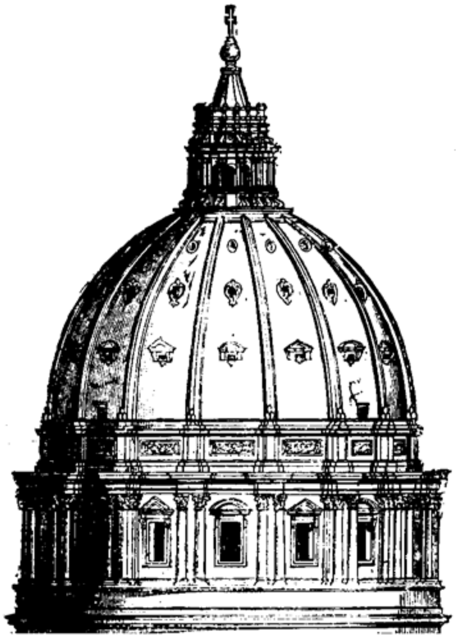
ISSUE BRIEF #1/2011



Cloud Computing 101: A Brief Introduction

BY DEBORAH COLLIER
TECHNOLOGY POLICY DIRECTOR

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 Waste Watch, 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

INTRODUCTION

In 2010, U.S. Chief Information Officer Vivek Kundra announced that the federal government needed to stop building large stove-piped information technology (IT) systems and instead use what he called "light technologies and shared solutions;" in other words, cloud computing. This concept is embraced in the Obama administration's Transforming Federal Information Technology Management Initiative, which includes a "Cloud First" directive as part of its 25-point plan. But what exactly is "cloud computing," and how can it benefit government agencies in this era of shrinking budgets?

According to the National Institute of Science and Technology (NIST), cloud computing delivers IT applications to users by enabling "ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources."[1] Popular examples include email, calendars, websites and employee portals. Cloud computing enables organizations and individuals to access information without concern about the server's physical location; promising cheaper, faster, easier, more flexible, and more effective IT. Most organizations already utilize some form of cloud computing, whether their users are synchronizing web-enabled smartphones through their email provider, or obtaining information over the Internet. Online shopping and banking are prime examples of how cloud computing has transformed the way in which companies interact with and provide online services to customers.

The progress of technology through the years has offered both increased computing capabilities and reduced costs. According to an October 6, 2009 Booz Allen Hamilton study, over a 13-year life cycle, the total cost of implementing and sustaining a cloud environment may be as much as two-thirds lower than maintaining a traditional IT data center.[2] In the past, IT infrastructure typically required high energy consumption and extensive amounts of maintenance and support. If additional computing power was required to support new applications, additional hardware would need to be purchased. In larger corporate environments, duplicate systems were built to provide a fall-back in the event of main server failure, frequently using identical equipment sitting idle except during data

[1] National Institute of Science and Technology draft definition of cloud computing, http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf.

[2] Alford, Ted and Morton, Gwen, "The Economics of Cloud Computing: Addressing the Benefits of Infrastructure in the Cloud," Booz|Allen|Hamilton, October 6, 2009, http://www.boozallen.com/media/file/Economics-of-Cloud-Computing.pdf.

transfer, which also required the same level of support and maintenance as the main server. The large number of servers required the construction of large data centers.[3] Within these data centers, the Booz Allen Hamilton study estimated an average server utilization rate of only 12 percent of available central processing unit (CPU) capacity. In a cloud scenario, the server utilization rate would increase to around 60 percent.[4]

In 1998, the federal government maintained 432 IT data centers. With the continued growth of IT processes and applications, the number of these data centers has grown to more than 2,000. As part of the government's move toward shared solutions, the administration plans to shutter 198 of these data centers by the end of 2011, and an additional 178 by the end of 2012.[5]

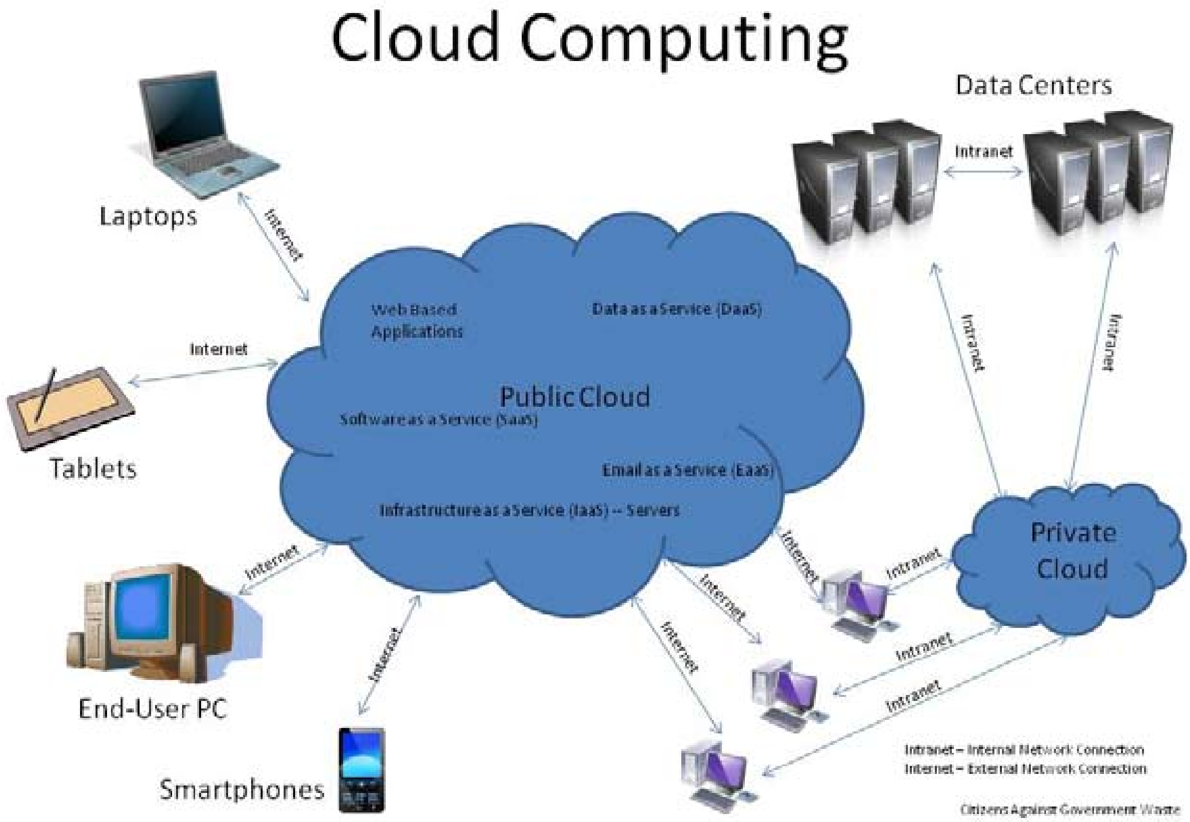
Cloud computing vendors offer technology options that can be economically scaled and priced to meet the needs of all types of customers. These offerings typically include the availability of web-based applications; servers that can host multiple tenants; software development with a support structure in place to assist the developer; a self-service user environment for system and application management; Internet Protocol (IP) Networks that connect end users to "the cloud" and the components of the cloud to each other; and, pricing agreements that scale technology costs with their cloud services volume and revenues.[6]

[3] Dorf, Michael, "Cloud Computing vs. Virtualization," LearnComputer.com, April 23, 2010, http://www.learncomputer.com/cloud-computing-vs-virtualization/.

[4] Alford, Ted and Morton, Gwen.

[5] Zients, Jeffrey, "Shutting Down Duplicative Data Centers," The White House, July 20, 2011, http://www.whitehouse.gov/blog/2011/07/20/shutting-down-duplicative-data-centers.

[6] Gens, Frank, "Defining 'Cloud Services' and 'Cloud Computing'," IDC eXchange Blog, September 23, 2008, http://blogs.idc.com/ie/?p=190.



Citizens Against Government Waste
July 2011

When considering cloud computing options, good network connectivity is essential. Once the network is in place, the choices of how to create a cloud environment vary, but most fall into four different categories: private cloud, community cloud, public cloud, or hybrid cloud.[7] Among the best known public cloud services are Amazon, Bing, Google, Yahoo, and others. However, these public clouds may not offer all of the security protections required by cloud users. A private cloud is one built for a specific customer – either in the corporate sector or government – with greater security protection for the customer's data. A community cloud allows several clients to share the same cloud to perform similar functions such as human resources or email. A hybrid cloud is a combination of two or more of the other three cloud infrastructure options.

Vendors offer cloud services such as Email as a Service (EaaS); Software as a Service (SaaS); Infrastructure as a Service (Iaas); and Data as a Service (DaaS). The services offered are usually accessible through the Internet, require minimal technology skills, and are obtained by a user self-service request through a browser. Vendors also typically provide web Application Programming Interfaces (API) and other shared resources. All of these services can be customized and may offer a usage-based pricing structure.[8]

[7] National Institute of Science and Technology draft definition of cloud computing.

[8] Ibid.

Cloud Computing 101: A Brief Introduction

The "Cloud First" policy in the administration's Transforming IT Initiative suggests that agencies make cloud computing the default option whenever possible. Each federal agency has been directed to identify at least three "must-move" services and shift them to the cloud by mid-2012, a transition that is supposed to engender efficiencies in government IT systems, save money while providing better services to the public, and maintain mission critical systems.[9] As part of this shift in the way the government utilizes IT services, agency chief information officers (CIO) must be vigilant about security in order to protect the privacy of personal identifying information maintained by their agencies, as well as their essential missions.

This efficiency model was highlighted during an April 27, 2011 panel discussion of the Transforming IT Initiative held at the White House.[10] As part of the Cloud First directive, 15 agencies have identified 950,000 mailboxes and more than 100 email systems that they would be able to move to the cloud. As a follow-up, on May 11, 2011, the General Services Administration (GSA) asked for bids by vendors to provide services for GSA's EaaS cloud offerings, designed to increase the speed of agency adoption, deployment and implementation of cloud technology.

The Department of Energy has already transitioned 5,000 email and calendar applications to cloud computing and is projecting between $1.5 and $2 million in savings over the next two years. The U.S. Department of Agriculture (USDA) is working to move approximately 120,000 employee email accounts to a new cloud-based solution, and plans are in the works to scale back the department's data centers from the existing 43 to seven. USDA officials expect to close 10 of these data centers by the end of 2011, and plan to consolidate more than 20 document and correspondence systems into a single agency-wide cloud solution. Hundreds of human resource and financial management systems will also be combined into the cloud in the future.

Critical to the federal government's move toward cloud computing is the simultaneous adoption of superior procurement practices and the implementation of high-level security protections. However, the federal government has a less than stellar history of IT cost overruns and mediocre procurement practices. For example, on July 15, 2011, it was revealed that the Department of Homeland Security mismanaged the purchase of $3.2 billion worth of metal detectors, explosive detection systems and radiation detectors by failing to use appropriate strategic procurement practices.[11] This is just one

[9] "The New Technology Paradigm," Fortune, Special Advertising Section, 2011, June 13, 2011, www.fortune.com/adsections.

[10] "White House Forum on Transforming Federal Information Technology (IT) Management," 57 min, 47 secs, The White House, April 27, 2011, http://www.whitehouse.gov/photos-and-video/video/2011/04/27/white-house-forum-transforming-federal-information-technology-it-m.

[11] Sternstein, Aliya, "DHS' failure to leverage large technology buys costs billions in lost savings," Nextgov.com, July 15, 2011, http://www.nextgov.com/nextgov/ng_20110715_9845.php?oref=topnews.

example of mismanaged, compartmentalized procurement practices within the federal government that waste billions of taxpayer dollars.

In addition to procurement problems, telling examples of the consequences of inadequate security for sensitive information include the Internal Revenue Service's failure to notify the 36 percent of taxpayers whose personal identifying information was "inadvertently" released during fiscal years 2009 and 2010,[12] and the May 3, 2006 IT data breach at the Department of Veterans Affairs (VA), when an employee's laptop containing the personal identifying information of 26.5 million veterans was stolen, which ultimately cost the VA $20 million in a class action suit.[13] This was the largest data security breach in the federal government's history and the second largest security breach in the nation, and it highlights the importance of building and maintaining a thoroughly buttoned-up IT system that will protect all stored information.

It is vital that purchasers and users of cloud technology understand and address the risks associated with lax security practices and build protective infrastructure before rushing headlong into the new technology. Mistakes can be costly, and data security should be foremost in the minds of agency CIOs and senior IT officials as technology advances.

Among the top threats to cloud computing are abuse and nefarious use of cloud computing, insecure interfaces and APIs, malicious insiders, shared technology issues, data loss or leakage, account or service hijacking, and other unknown risk profiles.[14] These threats should lead government IT professionals to move cautiously toward the cloud computing environment. The Pentagon's announcement in July, 2011 that one of its contractors had suffered a data breach in March containing 24,000 confidential files[15] is a prime example of the increasing threats to the IT infrastructure from abroad. According to *The New York Times*, surveys of agency CIOs indicate that they have an elevated degree of concern about security in a cloud computing environment.[16]

[12] "Some Taxpayers Were Not Appropriately Notified When Their Personally Identifiable Information Was Inadvertently Disclosed," Treasury Inspector General for Tax Administration, May 24, 2011, Reference Number: 2011-40-054, http://www.treasury.gov/tigta/auditreports/2011reports/201140054fr.pdf.

[13] Yen, Hope, "VA agrees to pay $20 million to veterans in 2006 data breach, Lawsuit alleged privacy invasion," Associated Press, January 28, 2009, http://articles.boston.com/2009-01-28/news/29254594_1_data-theft-veterans-groups-va-inspector.

[14] "Top Threats to Cloud Computing V1.0," prepared by the Cloud Security Alliance, March 2010, http://www.cloudsecurityalliance.org/topthreats.

[15] Lynn, William J. III, Deputy Secretary of Defense, "Remarks on the Department of Defense Cyber Security," July 14, 2011, http://www.defense.gov/speeches.aspx?speechid=1593.

[16] Collins Walsh, Sean, "Federal Push for 'Cloud' Technology Faces Skepticism," The New York Times, August 21, 2011, http://www.nytimes.com/2011/08/22/technology/federal-push-for-cloud-technology-faces-skepticism.html?scp=1&sq=&st=nyt.

Cloud computing can save money for taxpayers, but only if it offers the features and performance that users really need to meet their agency mission, as well as adequate guarantees for security and data privacy. Unfortunately, the reality is that many early cloud implementations - typically those that offer email and a few barebones web applications - have only rudimentary features and often suffer from poor performance. Even worse, they have serious gaps in security and data privacy.

For example, the delays, cost overruns, and security and data privacy problems encountered by Computer Sciences Corporation's (CSC's) implementation of Google Apps for Government with the city of Los Angeles[17] illustrate the pitfalls of cloud implementation. After contracting to provide a city-wide e-mail solution for $7.25 million, CSC promised that the new e-mail system would be in place by June 30, 2010. However, full implementation of the system was delayed due to data security concerns raised by the Los Angeles Police Department. The city was then forced to continue to maintain licenses for both the new and old e-mail programs for several months beyond the expected implementation date.[18] According to an April 19, 2011 article in the *Los Angeles Times,* even for non-LAPD employees, the CSC contract still did not meet all of the security requirements, preventing nearly half of the city's workers from moving to the new system. [19]

However, security concerns are not a reason to abandon cloud computing. With the potential cost savings and gains in IT flexibility, the proper approach is for government agencies and procurement officers to become better educated about the true strengths and weaknesses of the current generation of cloud solutions. They must become more demanding and choosier customers who understand what the vendors are offering and how those offerings meet the mission critical needs of their agency before they buy. In Cloud Computing 201, CAGW will provide a checklist for cloud procurement.

[17] Vijayan, Jaikumar, "L.A. may sue over delays in Google Apps project, report says," *NetworkWorld*, April 15, 2011, http://www.networkworld.com/news/2011/041511-la-may-sue-over-delays.html.

[18] Sarno, David, "Google misses deadline for L.A. city e-mail system," *Los Angeles Times*, July 24, 2010, http://articles.latimes.com/2010/jul/24/business/la-fi-google-la-20100724.

[19] Sarno, David, "Google facing hurdles in bid to provide email service to governments," *Los Angeles Times*, April 19, 2011, http://articles.latimes.com/2011/apr/14/business/la-fi-google-email-20110414.