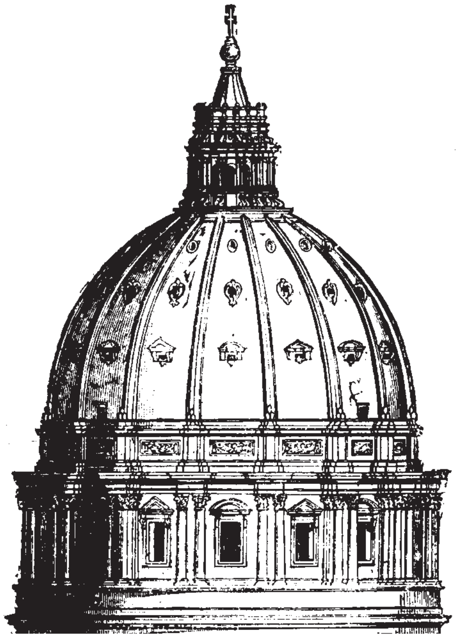
ISSUE BRIEF #2/2011



Cloud Computing 201:
Guidelines for Successful Cloud Investments

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

EXECUTIVE SUMMARY

The federal government spent $78.8 billion on information technology (IT) in calendar year 2011. In December 2010, the Obama administration issued its 25-point plan for Transforming Federal Information Technology Management, which included a requirement that agencies move three IT services to the cloud, as part of a new "Cloud First" policy.

The federal government, as well as state and local governments, should carefully consider how and when to engage in any IT procurement. The total cost of ownership, integrity of the data, security of the solution, and viability of the transition are of critical importance to the success of any project. Greater efficiency and cost savings can be achieved, but there are also risks in transitioning IT solutions to new tools and methods. Agencies should be proactive in order to avoid unnecessary costs and should maintain constant contact and cooordination with service providers and contractors.

"Cloud Computing 201," Citizens Against Government Waste's (CAGW) second issue brief on the cloud, provides an overview and guidelines for acquiring IT solutions, including using the cloud as a tool for savings. Procurement teams in agencies must keep in mind that the cloud is simply a computing tool and should not be the basis for an overall IT strategy. In addition, mandating the use of any particular technology may not provide the appropriate results.

CAGW's recommendations are intended to help agencies at all levels of government improve the management of their IT budgets. The 11 proposals include full consideration of the agency's mission; an assessment of current inventory of equipment and applications; interagency collaboration; strategic technology and contract development; data protection and portability; security and privacy; protective contracting vehicle clauses; backup solutions; effective program management; and user consultation and training.

Using these guidelines as well as other resources listed in this report, agency chief information officers will be able to establish a commonsense approach to plan and develop an IT procurement strategy that offers the opportunity to include cloud computing tools as well as any other new technology that may become available in the future.

Cloud computing, as part of a federal agency's information technology (IT) strategy, can help an agency maximize its investments by shifting the appropriate amount of data, applications and email to a cloud-based solution.[1] Currently, federal agencies have been told to move various IT services to the cloud as part of the Obama administration's 25-point plan for Transforming Federal Information Technology Management.[2]

The federal government spent $78.8 billion in calendar year 2011 on IT,[3] and the myriad problems in existing systems raise red flags with regard to all investments, particularly "new" solutions such as the cloud. Successful IT acquisition and implementation requires close coordination among contracting officers, agency chief information offers (CIOs) and information security officers (ISOs). The procurement "team" in each agency should always be aware that the cloud is simply a computing tool and should not be the basis for an overall IT strategy.[4]

Critical to any IT investment is the total cost of ownership (TCO) for the solution under consideration, including maintenance, support, training, integration and utility expenses. The TCO is designed to find the lifetime costs of acquiring, operating, and changing the acquired system. An analysis of the TCO often shows there can be a large difference between a product's price and its long-term costs.[5] When applied to purchasing IT solutions, particularly cloud solutions, the TCO includes the initial purchase price of the solution plus the additional costs of operation. Consideration of the TCO will help enterprise managers determine the direct and indirect costs of a product or system. A September 14, 2011 study compiled by TriComB2B and the University of Dayton School of Business Administration cited TCO as a key component in the decision-making process by senior executives, with 56 percent of respondents indicating that TCO had been calculated into the decision-making process at least 60 percent of the time.[6]

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

[2] Kundra, Vivek, "25 Point Implementation Plan to Reform Federal Information Technology Management," December 9, 2010, http://www.cio.gov/documents/25-Point-Implementation-Plan-to-Reform-Federal%20IT.pdf.

[3] Federal IT Dashboard Portfolio Report, accessed November 3, 2011, http://www.itdashboard.gov/portfolios.

[4] Gray, Patrick, "The Cloud isn't a strategy," TechRepublic, October 12, 2011, http://www.techrepublic.com/blog/tech-manager/the-cloud-isnt-a-strategy/6838?tag=nl.e019.

[5] Schmidt, Marty J., "Total Cost of Ownership (TCO)," Encyclopedia of Business Terms and Methods, ISBN 978-1-929500-10-9, Copyright © 2011, revised September 4, 2011, http://www.solutionmatrix.com/total-cost-of-ownership.html.

[6] "The Considered Purchase Decision: What Matters, What Doesn't, And What It Means For B2B Marketing and Sales," research report compiled by TriComB2B in partnership with the University of Dayton School of Business Administration, September 14, 2011, http://tricomb2b.com/sites/default/files/TriComB2B-UD_Research_Report.pdf.

When planning to transition IT to cloud computing, agency officials must include measures to ensure the integrity of the data, the security of the solution, and the viability of the transition. Security in the cloud starts with the contract vehicle and continues through to the end product. An August 21, 2011 *New York Times* article reflects the current concerns of federal IT professionals with respect to moving to cloud-based infrastructure, most notably the security of the data and information security.[7] According to the article, "surveys of chief information officers of federal agencies, conducted by various research companies, show an elevated degree of concern about security when asked about cloud computing." This concern was heightened by attacks from abroad on government systems and contractors in the spring and summer of 2011.

An October 3, 2011 Government Accountability Office (GAO) report highlighted the need for federal agency IT systems to become more secure. In reviewing the Federal Information Security Management Act (FISMA) compliance of 24 federal agencies, GAO found that reports of security incidents at federal agencies increased by 650 percent from fiscal year 2006 to fiscal year 2010. According to the report, these agencies have hundreds of outstanding recommendations to improve the security of their IT data and infrastructures.[8] These findings suggest that agencies should fix outstanding problems in existing systems before moving to the newest "solution," i.e., the cloud. As federal agencies transition more services to the cloud, the need for improvements to security to meet FISMA requirements increase.

As with any new venture, there are concerns about the risks (access, data privacy, security, portability, and liability), involved in migrating to cloud computing. Instead of running away from the risks involved with cloud computing, government agencies must work directly with cloud computing providers to address these issues and meet them head-on. It is far better to be proactive and resolve these issues than to wait until problems arise in the later stages of the procurement process. An October 2010 report from the Center for Technology Innovation at the Brookings Institute has suggested the following six tenets for information security: confidentiality, integrity, availability, accountability, assurance, and resilience.[9]

[7] 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?_r=1&pagewanted=all.

[8] "Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements," Government Accountability Office report GAO-12-137, October 2011, http://www.gao.gov/new.items/d12137.pdf.

[9] Friedman, Allen A. and West, Darrell M., "Privacy and Security in Cloud Computing," Center for Technology Innovation at Brookings, Issues in Technology Innovation, Number 3, October 2010, http://www.brookings.edu/~/media/Files/rc/papers/2010/1026_cloud_computing_friedman_west/1026_cloud_computing_friedman_west.pdf.

Agency officials must also consider the usability of the system and how moving technology forward will affect the end-user, whether it is the federal employee or a taxpayer seeking assistance from the agency. User input into the development of agency technology solutions, as well as user training, is critical when moving IT systems to a new architecture. Using a commonsense approach to planning, contracting, and development, federal agencies can transition their IT systems to cloud solutions, while also taking into consideration TCO, privacy, security, interoperability and portability.

CAGW has developed the following recommendations to help ensure successful implementation of a cloud computing solution in government agencies:

■ **Agency Mission:**

As part of the administration's IT initiative, each agency of the federal government is required to identify three IT services that must move to a cloud environment, and of the three, one operation must be moved within 12 months, and the other two operations within 18 months.[10] An overall evaluation of the agency's mission, as well as a review of issues relating to privacy and data security, will help in the planning process and assist in determining the type of cloud solution the agency should use. The agency can then choose to seek out either a public, private, community or hybrid cloud solution that will provide the best services to meet its needs while at the same time reducing TCO. It should be noted, however, that mandating the use of any particular technology may not provide the appropriate results.

■ **Current Inventory and Applications:**

Assessing both the level of inventory under a CIO's control and the extent and results of prior agency IT investments will help to determine whether and how a particular system can evolve into a cloud-based solution. A July 19, 2011 GAO report criticized government agencies' inventory management of data centers, noting that 14 agencies did not provide a complete listing of data centers and 15 agencies did not list all of their software assets.[11] According to the report, many state governments have undertaken data center consolidation efforts and have encountered similar challenges to those reported by federal agencies. CIOs should maintain an inventory of current technology solutions and equipment within their agency and determine what works well and what doesn't.

[10] "Cloud First Buyer's Guide for Government," Commission on the Leadership Opportunity in U.S. Deployment of the Cloud (CLOUD^2), Tech America Foundation, July 2011, www.techamericafoundation.org/cloud2.

[11] "Data Center Consolidation: Agencies Need to Complete Inventories and Plans to Achieve Expected Savings," Government Accountability Office, Report No. GAO-11-565, July 19, 2011, http://www.gao.gov/new.items/d11565.pdf.

■ **Interagency Collaboration:**

When agencies share similar or collaborative missions, they should work together to evaluate their technology needs and plans to move to a cloud computing environment. This coordination is vital for agencies managing large databases such as the Department of Defense and Department of Veterans Affairs' electronic health records systems, where interoperability among systems is critical to patient care.[12] Most agencies have similar IT requirements in certain departments, such as human resources and procurement. By collaborating and sharing resources, agencies may be able to save additional money by placing similar functions into a community cloud environment that would provide flexibility and meet essential functional needs.

■ **Strategic Technology Development:**

Once the overall scope of technology needs are determined based on the agency's mission, the CIO should devise a technology strategy with a primary focus on the most appropriate solutions that will assist the agency in meeting its goals, with minimal compartmentalization. Agencies should also not be constrained to one particular method of computing. Using cloud computing may not be the best or only answer to meeting the overall IT strategy for an agency. A pragmatic assessment should be used in which all options are evaluated based on cost, functionality, maintenance and ease of use. The solution could include a combination of cloud and on-premises technology, or only the cloud or on-premises technology.

■ **Contract Development:**

While keeping an eye on the cost-effectiveness of any cloud computing solution, agency CIOs must work directly with contracting officers and program managers in developing contracts that ensure the product purchased meets business requirements and supports the agency's mission. Building these requirements into the contract vehicle at the beginning of the process is important. When making final decisions on the contract, agency CIOs and contract officers must keep in mind that the best solution may not be the cheapest solution in the short-term. If an agency must rebid a contract after the failure of the first solution, it is not cost-effective at all.

■ **Data Protection and Portability:**

When developing contracts for IT services, particularly in the cloud computing environment, these services must maintain portability of data.[13] According to an August 24, 2011 Computing Technology

[12] "Electronic Health Records: DOD and VA Interoperability Efforts Are Ongoing; Program Office Needs to Implement Recommended Improvements," Government Accountability Office, GAO-10-332, January 28, 2010, http://www.gao.gov/new.items/d10332.pdf.

[13] "Portability," BusinessDictionary.com, http://www.businessdictionary.com/definition/portability.html, Viewed November 2, 2011.

Industry Association survey of cloud trends, one in five companies are moving some or all of their outsourced cloud systems back on-premise. One of the reasons cited by survey respondents was difficulty integrating on-premise systems with systems in the cloud.[14] The integrity of the data must be maintained if the cloud services provider is unable to complete the contract, the contract expires, the IT needs of the agency change, or for any other reason. The customer should not be "locked in" to one cloud provider after the original provisions of contract.[15] By implementing portability for both data and code at the start of the configuration process, any necessary switching costs would be reduced.

■ **Security and Privacy:**

Security and data privacy protections should be built into all federal IT solutions from the start of the contracting process, not as an afterthought. Security of the system should be foremost in the mind of the CIO when planning to move to a cloud computing solution. The CIO must ensure that the data being moved to the cloud is secure from outside intrusion; the contractor has a full and robust security program in place at the time of purchase; and, employees at the agency are fully versed in the latest security measures they can take to ensure the privacy of taxpayers and the security of the data that supports the agency's mission. When creating a plan for the cloud computing architecture, agencies should consider all types of cloud and on-premises solutions, and choose the best mix and best architectures to meet the agency's needs, depending on the sensitivity of the information.

■ **Protective Contracting Vehicle Clauses:**

Many cloud service providers offer advertising opportunities to third party entities through the use of key word searches of emails and other materials. However, when engaging in business with federal agencies this is not always appropriate, even though permissible through the provider's terms of use agreements. Agency heads should determine what information and data cloud provider employees should have access to, if any, and whether the provider's terms of use agreements should apply or be amended with respect to information gathered by the government. These decisions should be built into the contracts negotiated with service providers and supersede the provider's normal terms of use agreements. In addition, third party entities should be specifically prohibited from any access to government owned data stored or accessed on a cloud service provider's infrastructure. Contracts should also be clear that taxpayer/government data is not an asset to be sold in the event a cloud provider goes bankrupt.[16]

[14] Torode, Christina, "Taking business back from cloud service providers," IT Knowledge Exchange, September 22, 2011, http://itknowledgeexchange.techtarget.com/total-cio/taking-business-back-from-cloud-service-providers/?track=NL-964&ad=848383&asrc=EM_NLN_14967643&uid=9163909.

[15] Friedman, Allen A. and West, Darrell M.

[16] Ibid.

■ **Backup Solutions:**

One of the benefits of cloud computing is the ability to store information remotely, without concern about physical location. Agency CIOs should include a redundant backup system in the cloud computing architecture in order to eliminate business downtime, minimize data loss, and provide for data segmentation. Cloud computing relies on a full-time Internet connection, in some cases over large distances on public networks. If any part of these networks goes down, the cloud user is "out of business." There should be a fallback plan to allow the agency to continue to operate in the event of network or cloud service provider service disruption or failure.

■ **Effective Program Management:**

One of the key issues surrounding technology cost overruns has been the lack of project management leadership. By incorporating an effective program management system into new IT development, agency CIOs can better monitor the cycle of accountability for new systems. The Department of Veterans Affairs uses the Program Management Accountability System, which ties projects to established milestones in order to inject accountability into the procurement process.[17] The Office of Management and Budget (OMB) has also provided guidelines through TechStats to help agencies through the process and enhance their ability to evaluate the progress of IT development. However, management accountability systems are not enough. Agency CIOs must also assign a knowledgeable program manager to the task who is invested in the new system and can encourage and motivate contractors to move forward on the contract milestones so that the project remains on time and on budget.

■ **User Consultation and Training:**

Ultimately, it is the end user who will be most impacted by IT procurement. It is vital that this user be included in decision-making throughout the process. Agency CIOs should consult with users to obtain information about what they like and don't like about their current applications, what they believe will improve their workflow, and what they expect from any new IT system. Agency CIOs should also inform the user of agency expectations for results in moving certain infrastructures to cloud computing services. End user buy-in must also incorporate training in security procedures and best practices in the cloud computing environment.

Using these guidelines as well as other resources available from organizations such as the TechAmerica Foundation, SafeGov.org, Computer & Communications Industry Association, the Brookings Institute and other industry experts, agency CIOs have the ability to create an IT procurement strategy that offers the opportunity to include cloud computing and any other new technology that becomes

[17] "VA Expands Evaluation of Technology Project," U.S. Department of Veterans Affairs, February 23, 2010, http://www1.va.gov/opa/pressrel/pressrelease.cfm?id=1855.

available in the future with minimal user disruption and higher security capabilities. Above all else, thoughtful planning and preparation are key to the successful deployment of any IT system.

GLOSSARY OF TERMS AND DEFINITIONS

Cloud Computing—A model or style of computing enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.[18] The essential characteristics of cloud computing are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. For additional information, see CAGW's report "Cloud Computing 101: A Basic Introduction."

Community Cloud—The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premise.[19]

Email as a Service (EaaS)—While not included in the NIST definition of cloud computing, EaaS is a term for a Software as a Service (SaaS) model for cloud computing, which offers the consumer the capability of using and storing e-mail messaging services in a cloud environment. It may be managed by the organization or by a third party and may exist on premise or off premise.

Federal Information Security Management Act (FISMA)—Enacted in 2002 as title III of the E-Government Act (P.L. 107-347) FISMA provides a framework for information and data security for federal agencies. FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and

[18] Mell, Peter and Grance, Timothy, "The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology," September 2011, p. 2, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[19] Mell, Peter and Grance, Timothy, "The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology," September 2011, p. 3, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.[20]

Federal Risk and Authorization Management Program (FedRAMP)—A program developed by the federal government to provide a standard approach to assessing and authorizing cloud computing services and products. FedRAMP allows joint authorizations and continuous security monitoring services for government and commercial cloud computing systems intended for multi-agency use.[21]

Hybrid Cloud—The cloud infrastructure is composed of two or more clouds (private, community, or public) that remain unique entities, but which are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).[22]

Infrastructure as a Service (IaaS)—A service model for cloud computing, IaaS is the capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).[23]

Platform as a Service (PaaS)—A service model for cloud computing, PaaS is the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.[24]

[20] "FISMA Detailed Overview," National Institute of Standards and Technology, Computer Security Division, Computer Security Resource Center, http://csrc.nist.gov/groups/SMA/fisma/overview.html. October 21, 2011.

[21] "Federal Risk and Authorization Management Program (FedRAMP)," CIO.gov, November 2, 2011, http://www.cio.gov/pages.cfm/page/Federal-Risk-and-Authorization-Management-Program-FedRAMP.

[22] Mell and Grance.

[23] Ibid.

[24] Ibid.

Private Cloud—The cloud infrastructure is provisioned for exclusive use by a single organization comprising of multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.[25]

Public Cloud—The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.[26]

Software as a Service (SaaS)—A service model for cloud computing, SaaS is the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.[27]

[25] Ibid.

[26] Ibid.

[27] Ibid.