TechAmerica FOUNDATION

Cloud First Buyer's Guide for Government

Commission on the Leadership Opportunity in
U.S. Deployment of the Cloud (CLOUD[2])

“The movement to the cloud is a one-way street.”

Vivek Kundra, Federal Chief Information Officer
Comments before the TechAmerica Foundation
CLOUD^2 Commission
July 7, 2011

Cloud First Buyer's Guide for Government

The U.S. Government is on the brink of a major shift to cloud computing. Like the private sector, the Government has realized that cloud computing can dramatically reduce IT costs while significantly improving performance and accelerating innovation. Based on case studies, The Brookings Institution determined that federal, state and local governments realized significant cost savings associated with various cloud computing migrations. It was estimated overall savings (from infrastructure, labor and energy costs to name a few areas) "generally average between 25 and 50 percent." [1]

Every major analyst firm believes that cloud computing will expand its share of the overall IT market, with Goldman Sachs going so far as to say that the shift to cloud services and solutions is "unstoppable."[2] Data center consolidation is an important driver for the adoption of cloud computing services and solutions in the public sector. The U.S. Federal Government alone has plans to eliminate 800 data centers by 2015, with 373 to be shut down by the end of 2012.[3]

To spur government agencies to take advantage of the benefits that cloud computing enables, the Obama Administration has issued a Cloud First policy. This Buyer's Guide is designed to assist government agencies as they evaluate and purchase cloud services and solutions in response to that policy. The main requirements of the Cloud First policy are excerpted below.[4]

- *Beginning immediately, the Federal Government will shift to a Cloud First strategy.*

- *When evaluating options for new IT deployments, the Office of Management and Budget (OMB) will require that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists.*

- *These new cloud implementations should be compatible with the secure, certified platforms currently provided in the private sector.*

- *Migrating these services will build capabilities and momentum in the Federal Government, encourage industry to more rapidly develop appropriate cloud solutions for government, and reduce operating costs.*

- *Each agency chief information officer (CIO) will be required to identify three "must move" services and create a project plan for migrating each of them to cloud solutions and retiring the associated legacy systems. Of the three, at least one of the services must fully migrate to a cloud solution within 12 months and the remaining two within 18 months.*

I. Agency Preparation

To comply with the Cloud First policy, Federal agencies must carefully evaluate cloud computing services and solutions to determine which ones meet their needs and then move to implement them where appropriate. Cloud First is an opportunity for government to build on the benefits that consumers and businesses have realized from cloud computing and to deploy new technologies with the goal of significantly improving the efficiency of governmental operations and the public services it offers. Although the shift to cloud computing raises new issues that must be considered, existing Federal government procurement practices are flexible enough to enable acquisition of the new capabilities. Listed below is a series of best practices for government agencies interested in adopting cloud computing.

1. Begin with a business case that defines requirements and performance objectives.

Government agencies should begin with a business case that outlines their requirements and performance objectives, not with a particular cloud model (public, private, hybrid or community). Defaulting to a particular cloud deployment or service model rather than using agency performance objectives to define the approach will result in missed opportunities to benefit from available cloud services.

In making the transition to the cloud, Federal agencies should first focus on workloads and cloud services and solutions that have already been widely deployed in the cloud in the private sector and government. Among those workloads, services and solutions immediately suitable for government adoption are (1) storage, computing, web hosting, and backup, which fall under the category of infrastructure as a service (IaaS); (2) database services, identity management services, security services, geospatial information systems and customized application in areas of IT management, which fall under the category of platform as a service (PaaS).; and (3) email, customer relationship management (CRM), collaboration, payment processing, and service centers, which fall under the category of software as a service (SaaS).[5] These workloads and services have already been successfully deployed in the cloud in both the private sector and government. After agencies have identified initial targets for transition to the cloud, they should explore the business and mission benefits of emerging cloud applications, such as enterprise applications and agency-specific mission support systems.

Tools and workshops are available from industry partners if help is needed in building a business case and IT roadmap, assessing cloud readiness, or optimizing and migrating a workload to the appropriate cloud model.

2. Map agency priorities.

Government agencies should have a clear understanding of the cloud attributes that are most important to them. Below is a list of cloud attributes to be considered; different agencies will place different weight on different attributes.

- **Automatic Upgrades and Patches**
  Some in-house IT deployments can carry high maintenance fees and necessitate expensive upgrades. Agencies concerned about upgrading and patching legacy software should seek cloud services and solutions in which systems are maintained cost-effectively, schedules and processes for upgrades are clear, and there is transparency around pricing for substantially new functionalities.

- **Collaboration**
  Agencies that want to work together across stovepipes should explore secure cloud collaboration tools and social networking applications that connect people and their underlying information within the context of relevant security requirements.

- **Compliance**
  Agencies should evaluate the cloud service provider's ability to fulfill the necessary compliance requirements, such as HIPAA.

- **Development**
  Many government agencies will want to develop their own customized PaaS and SaaS cloud applications instead of purchasing commercially available solutions. These agencies should make sure that their cloud service includes a robust development platform that accommodates multiple programming languages, industry standard frameworks and tools for access controls, logging, security, real-time transparency, and privacy.

- **Ease-of-Use**
  For agencies deploying cloud services to a population with diverse IT skills, ease-of-use will be essential. SaaS and PaaS cloud applications should demonstrate high utilization and satisfaction rates. Agency stakeholders should talk with their peers to confirm customer satisfaction with cloud services and conduct market research to determine best practices.

- **Energy Efficiencies**
  Overall energy savings from shifting to the cloud can be significant. In addition, using cloud services to meet government data center consolidation requirements will facilitate significant energy-efficiency savings and benefits.

- **Integration**
  End-to-end processes may require integration between cloud applications and in-house applications. Agencies should consider this integration up front.

- **Interoperability**
  Agencies should make sure that their cloud services support open standards that have already been widely accepted.

- **Mobility**
  If mobility is important to mission requirements, look for a comprehensive

mobile platform that can be quickly deployed across a variety of mobile devices and operating systems.

- **Portability**
  Clarify that the agency can extract and move its data in a commonly accepted standard format.

- **Price**
  For some agencies, price will be the overriding consideration. If this is the case, they should require documentation of the total price of the cloud services and solutions and insist on a predictable pricing structure. Current procurement law requires past performance assessments, which can be used to determine whether those estimates are supported by customer experience.

- **Scale**
  Scale is often a primary concern for broadly delivered government services with unpredictable demand spikes. If scale is vital, agencies should validate the performance and reliability of the cloud service at the maximum anticipated scale and ask about the real-time monitoring tools available for the cloud service.

- **Security**
  Because security is such a critical consideration, it is discussed separately (see Section 3 below).

- **Speed**
  Other agencies will find that rapid deployment is the primary goal. This is especially true when responding to disasters, government mandates, and performance requirements with tight deadlines. In order to ensure rapid deployment or agility, agencies should request demonstrations, implement pilots, and include mutually binding deployment deadlines in cloud service contracts.

- **Sustainability**
  Agencies may need the cloud service vendor to build and deploy new capabilities for future needs. They should evaluate the cloud provider's strategy, alignment with the agency's mission, future product roadmap, financial and corporate stability, and ability to address needs in a timely fashion.

- **Transparent Performance**
  Availability, reliability and performance are priorities for government IT deployments. Agencies concerned about performance should ask for real-time Web dashboards that show the status, availability, reliability and speed of cloud services. Examples of such dashboards can be found at www.cloudbuyersguide.org.

3. Understand the security requirements.

Security usually tops the list of government concerns about IT, including cloud computing. Cloud services are not inherently more or less secure than in-house IT implementations. In both cases, security depends on technology, policies, and practices. A robust implementation of cloud services is capable of meeting a variety of security requirements.

In assessing the security of cloud services, government agencies should rely on the same Federal Information Security Management Act (FISMA) authorizations that are required for in-house IT implementations. Today, security Assessment and Authorization (A&A) is performed on an agency-by-agency basis. The goal of the Federal Risk and Authorization Management Program (FedRAMP) is to provide a more comprehensive government security framework that will enable different government agencies to leverage the same security authorization, as the Federal government moves to an updated FISMA framework.

One of the differences between cloud and in-house IT implementations is the degree of control for who manages and controls the security processes. Agencies should focus on managing the agreements between the agency and provider to ensure that a consistent security posture is maintained independent of who is responsible for the various layers of the system.

4. Consider how the cloud service will be implemented by your agency.

Government agencies should choose those services that map to their business and mission needs and that they can readily share with other agencies with similar needs. In matching cloud services and mission objectives, Federal agencies should consider the following:

- Is the cloud service easy to configure? Government agencies should be able to configure solutions themselves and should not require deployment of complex IT processes. Changes by one agency should not affect the usage or configuration of the service for the other agencies using the shared service.

- Does the cloud service exist elsewhere within government and can that service be shared elsewhere within government?

- Does the cloud service provider enable portability of user data through an effective combination of documents, tools, and support for agreed-upon industry standards and best practices? If not, are there third-party solutions to provide access to the data in the cloud service? Government agencies should avoid vendor lock-in solutions that make it difficult for them to extract and move their data in translatable formats for use in other cloud platforms.

- Will the cloud service provider, the government agency, or third party integrate cloud applications with in-house applications where needed to ensure seamless end-to-end processes? Government agencies can clarify the technologies and standards used and perform testing to verify compliance and understand the differences with the stated standards.

5. Outline mission requirements in an RFP.
Requests for Proposals (RFPs) should focus on mission and business requirements and service performance guidelines rather than detailed technical specifications or an architectural approach. They should be flexible enough to allow vendors to craft a variety of cloud solutions to meet these requirements. Cloud computing technologies are rapidly evolving, and it is important to evaluate the track record of the cloud services and cloud vendors under consideration.

In addition to making sure that the RFP process considers attributes relevant to cloud services, it is important to streamline the RFP process to reflect the rapid deployment of cloud services. The topics and sections of the traditional RFP still largely apply, including background descriptions about the provider, client references, startup and ongoing cost models, and required certifications; however, other typical requirements such as key personnel requirements may not make sense for a self-service cloud application.

6. Take advantage of government-wide cloud initiatives.
In the Federal Government, much thought has gone into analyzing how agencies can use the cloud within the Federal security, technology, and acquisition context — from exploring centralized security authorizations like the proposed FedRAMP, GSA's Blanket Purchase Agreement (BPA) for IaaS, to evaluating National Institute of Standards and Technology (NIST) standards and guidance. By building on these efforts, agencies can meet mandated timetables and accelerate potential savings.

7. Look beyond technology hype claims to include people and process in decision making.
Cloud technology will not deliver the desired return on investment without addressing the people and process issues that are needed to manage effective systems.

8. Leverage a common service measurement framework to evaluate providers.
Once an agency has prioritized its requirements, the agency should use a data-driven approach to evaluate cloud offerings based on those requirements. Several efforts are underway to develop data-driven approaches to evaluate competing offerings based on measurable criteria like those mentioned above.[6]

9. Understand timing and triggers for considering cloud deployment.
The following kinds of IT activities may offer an opportunity to introduce a cloud solution that will drive significant savings:

- **Systems Scheduled to Replace Existing Computer Equipment**
  Agencies should identify their systems that require updates to computer equipment or that need to acquire new functionalities and then evaluate if the workloads running on those systems are candidates for moving to the cloud, potentially eliminating significant costs associated with the scheduled IT infrastructure improvements. Three factors contribute to the anticipated savings:

- First, the agency leverages the cloud provider's global economies of scale in computer equipment acquisition, pooled expert IT infrastructure staff, and investments in IT service management technology and operating procedures.

- Second, the agency shifts to paying only for the computing services it needs. For example, the agency can access the computing power it needs to run everyday operations, later add more scale for high-volume spikes, and reduce resources when they are no longer needed (instead of leasing new computers to support peak operations and paying for unused computing power during lower-volume periods).

- Third, the agency can avoid the time and cost of infrastructure-specific security authorization and accreditation activities. Agencies can look to leverage security authorizations from other agencies with similar security needs or the proposed FedRAMP for cloud infrastructure, and focus time and resources on certifying the security of the agency's applications running on that infrastructure.

- **Planned New System Implementations and System Upgrades**
  New system implementations and major upgrades also typically trigger a need for new computing equipment. Agencies can realize significant savings by deploying these systems directly into an IaaS cloud environment where they can rent, instead of buy, the required new machines. They can also achieve significant savings by using SaaS and PaaS solutions that do not require any infrastructure investments and limit or eliminate software upgrade costs.

- **IT Infrastructure Requests for System Conversion, Testing, or Development**
  Acquiring development and testing environments in the cloud can reduce the cost of creating and maintaining these environments. The agency can provision servers (and incur costs) in the cloud only when needed instead of paying for unnecessary continuous capacity.

- **Pilot Projects and Investments in New Capabilities That Are Only Used Periodically**
  If an agency does not require or desire ownership, the cloud approach provides access to new or additional functionality with minimal costs. This access also applies to capabilities required only on an as-needed or trial basis. For example, in advance of the next fiscal year budgeting cycle, an agency might want to pilot software that automates budget formulation. The agency can acquire the access it needs for the pilot, expand its use of the software during the peak budget preparation season, and then scale back or eliminate the capability as desired.

- **Investment Requests to Develop Systems**
  For development needs, a cloud approach provides the ability to develop custom applications or capabilities without having to purchase infrastructure or development software. The agency can rent a development platform in the cloud, build the capability it needs, and migrate the application into steady-state operation. If agency-specific development environments are not commercially available, the IaaS cloud approach provides the ability to develop custom applications or capabilities without having to purchase infrastructure.

II. Best Practices

We have categorized best practices for government cloud services procurement across six different functions: (1) acquisitions managers, (2) program managers, (3) chief financial officers, (4) chief information officers/chief information security officers, (5) chief human capital officers and (6) agency leadership. There is some overlap across these functions, and we have tried to highlight issues that are especially relevant to each one.

1. Acquisition Manager

- **Evaluating RFPs**
  Ask for transparent prices in the form of subscription or pay-as-you-go pricing; verify that automatic upgrades appropriate to the service type provided are included; and confirm that the cloud service can accommodate scale to a level consistent with the agency's requirements.

- **Verifying Goals**
  Make sure that agency mission goals and security requirements have been fully addressed in the proposed contract.

- **Developing an Appropriate Statement of Work**
  Shift from defining deliverables to defining service level agreements (SLA) and their required outcomes (focus on measurable operating quality metrics, not inputs like number of labor hours). Require cloud service providers to include in their service price all upgrade and maintenance fees appropriate to the infrastructure, platform, or software service being procured.

- **Defining the Legal and Regulatory Requirements**
  Ask the cloud service provider to explain its information handling practices and disclose the performance and reliability of its services on its public Web sites. Verify that the cloud service provider does not claim any ownership right to government data and agrees to maintain it securely and use it only as the government customers instruct them to or to fulfill contractual or legal obligations.

- **Managing Services-Based Contracts**
  Make sure that subscription-based cloud service contracts that specify periodic payments in exchange for defined services do not raise any new contractual issues. Handle use-based cloud service contracts (i.e., based on frequency of usage) as managed service contracts with an overall obligation and periodic draw-downs.

2. Program Manager

- **Customer Success**
  Talk to peers in other government agencies and in the commercial sector who have successfully implemented cloud services similar in scope and

complexity to those being considered. Make sure that the cloud service is production-ready.

- **Budget**
  Talk with acquisition and budget teams about expected utilization and potential surge scenarios to ensure budget is appropriately developed and the contracts with service providers have enough flexibility to scale up or down based on utilization. Factor in the costs and resources needed to make the application or service cloud-ready.

- **Productivity**
  Ask for documented results about collaboration and operational efficiencies. Proven cloud service vendors should be able to provide this evidence.

- **Agency-Wide Information Sharing**
  Request collaboration tools that enable information and document sharing through filters and feeds with appropriate protections for proprietary information. Look for data and cloud integration tools that enable cloud information sharing with existing IT systems.

- **Mobility**
  If mobility is important to mission requirements, look for a comprehensive mobile platform that can be quickly deployed across a variety of mobile devices and operating systems.

- **Reusable**
  Determine if cloud services, including custom cloud applications and configurations, already acquired by the government would be reusable without having to be re-architected for mission requirements.

- **Pilots**
  Implement pilots to verify speed of deployment, ease-of-use, and performance. Cloud applications can be built, customized, and deployed quickly, so government agencies should not hesitate to ask for pilots to be deployed promptly depending on the deployment model.

3. Chief Financial Officer (CFO)

- **Price Transparency**
  Confirm that the prices are predictable, auditable, and transparent. Cloud subscription agreements should include all software, maintenance, and upgrade fees appropriate to the infrastructure, platform, or software service being procured so that it is easy to assess and forecast prices.

- **Cost Reduction and Avoidance**
  Ask for evidence that shows the cloud service will reduce the total life cycle costs, relative to in-house technologies. Request references to clarify the

ongoing cost of the service. Understand specific costs to make the application or service cloud-ready, not just the cost to purchase the cloud service.

- **Infrastructure**
  Verify that the cloud solution is production-ready, without extensive upfront IT infrastructure costs or requirements for third-party hardware, telecommunications capacity, network devices, or software. Understand what system requirements may require configuration or engineering changes to existing applications to make them cloud-ready.

- **Evaluating Cloud Service Contracts**
  The following are among the key areas that cloud service contracts should cover: security; reliability and availability; redundancy, backup, and restoration; disaster recovery and continuity of operations; maintenance; customer support; capacity planning and dynamic provisioning of resources; access and user administration; operating system and application administration; documentation; and technology refresh management.

4. Chief Information Officer/Chief Information Security Officer (CIO/CISO)

- **Security**
  CIOs and CISOs should work with the mission/business stakeholders to assess the potential risks in moving to cloud services. Based on that assessment, they should define their risk management plan and put controls in place that are appropriate for their determined risk profile. They should require an A&A commensurate with the sensitivity of the data being processed (low, moderate, high). They should also look for complementary industry security certifications and best practices and determine any identity management requirements.

- **IT Organization**
  Consider the impact of cloud services on the IT workforce. Some skills, such as patching legacy IT systems, may not be needed by the agency, while others, such as service management and contract management, will be in demand. As a result, career paths and reporting relationships may change.

- **Readiness and Migration Path**
  Understand what work must be done to enable the migration of the application or service to the cloud. Look for tools that enable integration of the cloud service with existing systems and processes.

- **Open Standards**
  Make sure the components support open industry standards that have already been widely accepted.

- **Automatic Upgrades**
  Verify the schedule, process, downtime, and costs associated with upgrades

related to security and functionality. The impact of upgrades for cloud services is generally less than with in-house IT implementations.

- **Reusable Services**
  Determine if cloud services, including custom cloud applications and configurations, that have already been acquired by the government would be reusable without having to be re-architected for mission requirements.

5. Chief Human Capital Officer (CHCO)

- **Training**
  The CHCO should coordinate with the CAO to ensure adequate and appropriate training is provided for the acquisition workforce within the agency to understand and effectively acquire cloud services and solutions.

- **Workforce**
  The CHCO should coordinate with the CIO to ensure that the IT workforce is prepared for the shift from internal management and operations of in-house systems to provisioning and deploying cloud capabilities for the agency. This preparation should include both hiring people with new skills and training those already in the agency workforce.

6. Agency Leadership (Assistant Secretary, COO)

- **Mission Support**
  Understand the impact that migrating services to the cloud will have on agency mission and effectiveness. Be prepared to address mission improvements or projected mission improvements in external forums, such as Congressional hearings and interagency meetings. Own the decision to move services to the cloud.

- **Budget**
  Seek information and justification on budgetary impacts of the move to cloud solutions. Understand the total cost of migrating solutions to the cloud, including agency and contractor time to make existing applications cloud ready. Ask for clarification on the budget and pricing implications of surges and the costs to move from one provider to another.

- **Customer Success**
  Talk to your peers in other government agencies that have successfully implemented cloud services to learn from their experiences. Anticipate challenges and prepare agency executive leadership for risks and successes.

III. Frequently Asked Questions

Do Federal Acquisition Regulation (FAR) rules allow government agencies to purchase cloud services?
Yes. The FAR pertains to cloud computing just as it does to any other government procurement. It should not be an impediment to the purchase of cloud services.

What about capital expenditures versus operational expenditures (CapEx versus OpEx)?
The budgeting process should aim to minimize CapEx and focus investment on the value of the cloud service itself. CapEx should be part of the discussion leading up to the RFI and RFP so that there are no surprises.

What about small-business set-asides? Are all of the cloud providers large companies?
Small businesses have an important role to play in the delivery of cloud services to the Government. Because they can be nimble, they are in the vanguard of the effort to deliver cloud services to the Government. Moreover, they will play an active role in the customization of cloud applications to meet specific government needs.

What's the difference between contracting for cloud computing and managed services?
The cloud payment model is very similar to the managed services payment model. Subscription-based cloud service contracts that require an agency to pay a specified amount in exchange for defined services should not raise any new contractual issues. Use-based cloud service contracts that require payment depending on usage are best handled as a managed service contract in which payment is based on an overall obligation and a periodic drawdown based on how much the service is used.

Is there an OMB 300 short form for cloud services?
Not yet, but it would be a good idea. OMB is in the process of updating the OMB 300 form. Just as cloud services accelerate the delivery of government computing services, the OMB 300 update should help streamline the procurement process for these services.

What impact will cloud computing have on government IT jobs?
It will shift the focus to higher-value-added activity and away from commodity operations, like patching and upgrades. Because cloud computing will accelerate development and deployment of IT services, it will also allow agencies to focus more on innovation. As a result, it will enable IT departments to play a more strategic role within their agencies.

IV. Acknowledgements

TechAmerica Foundation gratefully acknowledges the contributions of the Commissioners, their colleagues and staff to the successful completion of this "Buyer's Guide." The "Buyer's Guide" is the product of a concerted effort by the Commission to improve and facilitate the U.S. Government's adoption of cloud computing.

Stephen Alexander, *Ciena*
Amy Alving, *SAIC*
Jerry Archer, *Cloud Security Alliance*
Veena Avula, *Informatica*
Gregg Bailey, *Deloitte LLP*
JP Balakrishnan, *Infosys*
Ashok Balasubramanian, *Syntel*
Greg Baroni, *Attain, LLC*
Kia Behnia, *BMC Software*
Marc Benioff, *Salesforce.com* (Co-Chair)
Jeff Bergeron, *HP*
Heather Blersch, *General Dynamics*
Peter Bogdonoff, *AgilePath*
Mark Bohannon, *Red Hat, Inc.*
Bob Bonham, *SAS*
Emerson Brooks, *SRA International*
Paul Brubaker, *Synteractive*
Evan Burfield, *Synteractive*
Dan Burton, *Salesforce.com*
Teresa H. Carlson, *Amazon*
Michael Capellas, *VCE* (Co-Chair)
Pam Carpenter, *Adobe*
D. Zachary Champ, *TechAmerica Foundation*
Alan Chow, *Teradata*
Keith Collins, *SAS*
Nick Combs, *EMC*
Lance Crosby, *SoftLayer Technologies*
Peter D. Csathy, *Sorenson Media, Inc.*
Alan Davidson, *Google, Inc.*
William Davies, *Research In Motion, Limited*
Michael Donovan, *HP*
David Dudas, *Sorenson Media, Inc.*
Carolyn Eichler, *CSC*
Danielle Estrada, *Accenture*
Steve Estrada, *OpenConnect*
Sarah Falvey, *Google, Inc.*
Adam Famularo, *CA Technologies*
Gregory Gardner, *NetApp*
Andrew Gastwirth, *Attain, LLC*
Greg Gianforte, *RightNow Technologies*
Keith Glennan, *Northrop Grumman*
Diana L. Gowen, *Qwest Government Services, Inc.*
Eric Green, *CSC*
Melvin Greer, *Lockheed Martin*
Justin Greis, *Ernst & Young*
Elizabeth Grossman, *Microsoft*
Dan Guerra, *International Computerware, Inc.*
Randy Hahn, *Verizon Business*
Phil Harris, *VCE*
Phil Horvitz, *URS-Apptis*

Mel Hurley, *Wyle Information Systems*
Paul Hurley, *Securicon*
Michael Isman, *Booz Allen Hamilton*
Richard W. Johnson, *Lockheed Martin*
Wolfgang Kandek, *Qualys*
Daniel Kent, *Cisco*
Kirk Kern, *NetApp*
Jennifer Kerber, *TechAmerica Foundation*
Christie Kestler, *Savvis*
Mandeep Khera, *Cenzic, Inc.*
Jeff Koch, *IBM*
David Laliberte, *Research In Motion, Limited*
Jeff Lawton, *Grant Thornton*
Barry Leffew, *Adobe*
Curtis Levinson, *Qwest Government Services, Inc.*
Robin Lineberger, *Deloitte LLP*
Mare Lucas, *GCE*
Albert Lulushi, *L-3 Communications*
John Mallery, *MIT* (Academic Co-Chair)
Brad Maltz, *International Computerware, Inc.*
Chris Mankle, *ACS – a Xerox Company*
Ben Marglin, *Booz Allen Hamilton*
Eric Marks, *AgilePath Corporation*
Atul Mathur, *IMC, Inc.*
Timothy Matlack, *Delta Solutions and Technologies*
Daniel Matthews, *Information Innovators, Inc.*
Steve McCummings, *Cisco*
Nick Mehta, *LiveOffice*
PG Menon, *Brocade Communications, Inc.*
Randi Meyers, *TechAmerica Foundation*
Nick Mistry, *eGlobalTech*
Lew Moorman, *Rackspace Hosting, Inc.*
James Morin, *Ciena*
Gregg Mossburg, *CGI Federal*
Sergio Muniz, *MEI Technologies, Inc.*
Ray Muslimani, *GCE*
Vishy Narayan, *Infosys*
Michael R. Nelson, *Georgetown* (Academic Co-Chair)
Thomson Nguy, *Amazon*
Jeff Nick, *EMC*
Jim O'Hara, *LiveOffice*
Tom Parker, *Securicon*
Kevin Paschuck, *RightNow Technologies*
Steven Perkins, *Grant Thornton*
William Perlowitz, *URS-Apptis*
Brendan Peter, *CA Technologies*
Edward M.L. Peters, *OpenConnect*
Arnie Phatak, *Syntel*
Sterling Phillips, *GTSI Corp.*
John Pientka, *CGI Federal*

Chris Poelker, *FalconStor Software*
Sanjay Poonen, *SAP AG*
John Potter, *AT&T Business Solutions*
Braden Preston, *Harris Corporation*
Branko Primetica, *eGlobalTech*
Todd Ramsey, *IBM*
Jim Reavis, *Cloud Security Alliance*
Dan Reed, *Microsoft* (Vice-Chair)
Kurt Roemer, *Citrix*
Margaret Rooney-McMillen, *AT&T Business Solutions*
Jim Rottsolk, *Microsoft*
Glenn Schoonover, *Qualys*
David M. Shacochis, *Savvis*
Jim Sheaffer, *CSC* (Vice-Chair)
Suresh Shenoy, *IMC, Inc.*
Steve Sieke, *Serco North America*
Duke Skarda, *SoftLayer Technologies*
James Slaughter, *SRA International*
Juan Carlos Soto, *Informatica Corporation*
David Smith, *Citrix*
Kirk Smith, *L-3 Communications*
Monica Smith, *Teradata Corporation*
Melissa Smolensky, *Rackspace Hosting, Inc.*
Emily Stampiglia, *VCE*
Wyatt Starnes, *Harris Corporation*
Ken Stephens, *ACS – a Xerox Company*
Dave Stevens, *Brocade Communications, Inc.*
Grady Summers, *Ernst & Young*
Jim Sweeney, *GTSI Corp.*
Franco Tao, *Information Innovators Inc.*
Scott Turicchi, *j2 Global Communications, Inc.*
Stanley Tyliszczak, *General Dynamics*
Leif Ulstrup, *CSC*
Michael Van Chau, *MEI Technologies, Inc.*
Jacqueline Vanacek, *SAP AG*
Herb VanHook, *BMC Software*
David Vennergrund, *Delta Solutions and Technologies*
David Wagoner, *SAIC*
Bob Wambach, *VCE*
Bryan Ward, *Serco North America*
Steven Warner, *Northrop Grumman*
John Weinschenk, *Cenzic Inc.*
Teresa Weipert, *Accenture*
James White, *Wyle Information Systems*
Jim Whitehurst, *Red Hat, Inc.*
Christopher E. Wilson, *TechAmerica Foundation*
Bernie Wu, *FalconStor Software*
Susan Zeleniak, *Verizon Business*
Hemi Zucker, *j2 Global Comm*

Special thanks to Deloitte LLP for their assistance in producing the graphics for the Buyer's Guide.

V. Endnotes

[1] Darrell West, *Saving Money Through Cloud Computing* (Brookings Institution, May 2010).

[2] Goldman Sachs, SaaS Survey, February 2010.

[3]For further information, please see http://www.whitehouse.gov/the-press-office/2011/07/20/white-house-announces-plans-shut-down-hundreds-duplicative-data-centers-).

[4] Excerpted from the *25 Point Implementation Plan to Reform Federal Information Technology Management*, Vivek Kundra, U.S. Chief Information Officer, December 9, 2010, The White House, pp. 6 – 7.

[5] See NIST the current draft definitions of IaaS, SaaS, and PaaS for further information, available at http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf.

[6] Examples of such initiatives include the Carnegie Mellon University Cloud Services Measurement Initiative Consortium (CSMIC), the Distributed Management Task Force's (DMTF) Cloud Management Working Group, and the Cloud Security Alliance, among others.

Launched in 1981, TechAmerica Foundation is a 501(c)(3) non-profit affiliate of TechAmerica. It disseminates award-winning industry, policy, and market research covering topics such as U.S. competitiveness in a global economy, innovation in government, government IT forecasts, technology employment and international trade indicators, and other areas of national interest.

TechAmerica
FOUNDATION

601 Pennsylvania Avenue, NW
North Building, Suite 600
Washington, DC 20004
202.682.9110 (T)
202.682.9111 (F)
TechAmericaFoundation.org