Transcending the Cloud

A Legal Guide to the Risks and Rewards of Cloud Computing

The Key Risks and Rewards for Federal Government Contractors

ReedSmith

reedsmith.com

Cloud Computing – The Key Risks and Rewards for Federal Government Contractors

Authors

Lorraine Mullings Campos, Partner – lcampos@reedsmith.com

Stephanie E. Giese, Associate – sgiese@reedsmith.com

Joelle E.K. Laszlo, Associate – jlaszlo@reedsmith.com

Whether or not you believe cloud computing represents a revolutionary change in the provision of software and data processing services, the cloud and its lexicon have become firm fixtures in corporate enterprise management and, more recently, in doing business with the federal government. As discussed further below, contractors should recognize the legal risks and rewards of both assisting federal agencies in implementing clouds, and in employing cloud service providers to perform federal government contracts.

President Obama's Federal Cloud Computing Initiative

With the release of President Obama's budget for fiscal year 2011,[1] cloud computing also became an essential aspect of the nation's information technology strategy.[2] In fact, the administration has had its eyes on the clouds for some time, and while the 2011 budget represents its strongest commitment toward cloud computing, efforts to implement the concept have been ongoing since at least the roll-out of the 2010 budget.[3]

Around that time, Federal Chief Information Officer ("CIO") Vivek Kundra, the CIO Council, and the Office of Management and Budget established the Federal Cloud Computing Initiative (the "Initiative") to develop a broad strategy and to begin to identify specific applications for cloud computing across the federal government. From the Initiative sprung cross-agency bodies, including the Cloud Computing Executive Steering Committee and the Cloud Computing Advisory Council, and individual agency-based committees like the General Services Administration's ("GSA") Cloud Computing Program Management Office ("CC PMO"). The analysis that follows considers the implementation of cloud computing at the individual agency level, since it is the most immediate, and ultimately the most likely, source of government contracting activity.

Though one of the ultimate goals of the Initiative is to determine whether clouds will provide an appropriate means for breaking down inter-agency data stovepipes, federal cloud computing encompasses four different deployment models, and in these preliminary stages of cloud development, agencies have been free to determine which model best serves their needs. The four models, as defined by the National Institute of Standards and Technology ("NIST"), include: (1) *private clouds*, for the use of a single agency; (2) *community clouds*, shared by multiple agencies; (3) *public clouds*, largely for the public's use and benefit; and (4) *hybrid clouds*, facilitating the sharing of data and utilities across two or more unique clouds of any type.[4] In the sections that follow, we analyze some of the specific legal issues that may arise in the course of government contracting, first in the context of a hybrid cloud, then in the context of a private cloud, and finally in the context of a public cloud. In addressing *hybrid* and *private* cloud computing below, we focus on the key issues contractors should be aware of when assisting federal agencies in implementing cloud computing. In addressing *public* cloud computing, we focus on the key issues that arise when a contractor uses cloud computing to perform its federal government contract.

Key Issues Impacting Contractors Assisting Federal Agencies in Implementing Cloud Computing

Legal Issues in Hybrid Cloud Contracting: GSA's Apps.gov

In September 2009, federal CIO Kundra announced GSA's Apps.gov, which he described as an "online storefront for federal agencies to quickly browse and purchase cloud-based IT services, for productivity, collaboration, and efficiency."[5] Spearheaded by the CC PMO, Apps.gov provides agency consumers four different kinds of cloud computing applications: (1) *business applications*, to facilitate process and analytical tasks; (2) *productivity applications*, to support individual and group functionality; (3) *cloud IT services*, for storing and enabling diverse access to data; and (4) *social media applications*, to enhance communication and collaboration.[6] Again following the NIST taxonomy, the capabilities embodied by the applications on Apps.gov may be delivered to agency customers in one of three methods: (1) *software as a service* ("SaaS"); (2) *platform as a service* ("PaaS"); or (3) *infrastructure as a service* ("IaaS").[7] Perhaps not surprisingly, the delivery method is closely tied to the model of cloud used to provide a particular capability,[8] and a company seeking to offer a particular cloud computing application through Apps.gov will face unique legal implications, based on the method and model involved.[9]

Legal Issues in Contracts Involving SaaS Applications

Business and productivity applications are considered SaaS applications on Apps.gov, and are currently offered mostly through private clouds (though this is an ideal area for the future development of community clouds). Any such application procured through the traditional contracting approach must be certified and accredited by the Federal Information Security Management Agency ("FISMA"). That Certification and Accreditation ("C&A") process, which is defined in the NIST Special Publication ("SP") 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,"[10] is not a prerequisite to being listed as a vendor of SaaS applications through Apps.gov.[11] However, contractors offering these services through Apps.gov must be prepared to work with agency contracting authorities to ensure the C&A process is completed before contract performance begins. Failure to do so may render the contract unenforceable.

Legal Issues in Contracts Involving PaaS and IaaS Applications

PaaS and IaaS applications are not yet available through Apps.gov, though their release is reportedly imminent.[12] These applications will most likely be provided through private clouds in the foreseeable future, and will encompass solutions for data storage, hosting, and processing.

Unlike SaaS providers, IaaS providers will be awarded blanket purchase agreements under their GSA Federal Supply Schedule ("FSS") Schedule 70 contracts, which will implicate different contracting provisions in the Federal Acquisition Regulation ("FAR") from those governing contracts with SaaS providers.[13] In addition, IaaS providers reportedly will be required to meet the "moderate" security level under FISMA standards.[14] The original IaaS request for quotes ("RFQ") that was issued, and later withdrawn in fall 2009, required compliance with Appendices A and B of NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems."[15] Providers of IaaS capabilities under that RFQ were also held to a guarantee of at least 99.95 percent availability, and agency customers were entitled at any time to complete copies of their own data or the applications through which it was processed.[16] It remains to be seen whether these provisions will be carried into the revised RFQ, but potential providers of PaaS and IaaS capabilities are well advised to brace for stringent data security and access requirements.

Legal Issues Involving the Provision of Social Media Applications

A notable exception to the considerations above applies in the case of free social media applications, including open source, shareware, and freeware tools and services. Since these items are provided free of cost, GSA does not negotiate contracts for their inclusion on Apps.gov.[17] In order to be included as a provider of a social media application on Apps.gov, however, a vendor must agree to abide by a Terms of Service ("TOS") agreement that addresses the particular status and needs of federal government agencies.[18] Working in coordination with several other agencies, GSA developed a model "Federal friendly" TOS agreement[19] meant to serve as a baseline for discussions with individual agency consumers. Prospective providers of social media applications through Apps.gov should review the model TOS carefully, as well as any agency-specific additions or amendments to its terms, to ensure they are able to comply with its provisions.

Legal Issues in Private Cloud Contracting: Department of Defense ("DoD") Initiatives

Rapid Access Computing Environment ("RACE")

Unlike GSA, DoD is currently focused on developing private cloud environments where the data center is controlled by DoD rather than outsourced.[20] DoD expects this approach to achieve the cost savings typical of cloud computing and to address cybersecurity concerns.[21]

One example of a DoD private cloud is the Defense Information Systems Agency ("DISA") Rapid Access Computing Environment. RACE is an internal cloud computing service – a service controlled by DISA in its Defense Enterprise Computing Centers ("DECC") and operated behind DoD firewalls with the support of federal government contractors.[22] Similar to other clouding computing services, DoD users only pay for the amount of storage and processing power they need based on a monthly fee.[23] Within 24 hours of payment, users can begin using the RACE computing resources to develop and test their applications in their own Windows or Red Hat Linux operating environment.[24] When the application goes into production, the resources are returned to the DISA's cloud at one of DECC locations.[25] In the future, RACE may be extended to production of computing processes and applications.[26] In addition to cost savings, RACE offers the potential to standardize software applications across DoD agencies, making collaboration among the agencies easier.[27]

Transitioning Existing IT Systems to Cloud Computing Environments

Beyond supporting new cloud computing environments like RACE, government contractors are assisting DoD agencies with the transition of existing IT systems to cloud computing. For example, the U.S. Navy has awarded Lockheed Martin Corporation and Northrop Grumman Corporation Consolidated Afloat Networks and Enterprise Services ("CANES") contracts totaling $1.75 billion to upgrade existing shipboard and onshore Internet Protocol networks for command, control, communications, computers, intelligence, surveillance and reconnaissance ("C4ISR").[28] Under the CANES contracts, the companies will transition these Navy networks to cloud computing environments.[29]

Legal Issues Associated with Cybersecurity

Whether discussing cloud computing in terms of networks like RACE, where it is inherent, or CANES, where it is being adopted, the same cybersecurity issues apply. Cybersecurity includes safeguarding systems from security breaches, maintaining system operations while a cyber attack is underway, and developing network self-healing capabilities to minimize the impact of cyber assaults. Secretary of Defense Robert Gates has stated the United States is "under cyberattack virtually all the time, every day," and cybersecurity is not a new issue for DoD.[30] Of course, some cyberattacks are more damaging to national security than others. In a series of cyberattacks attributed to the Chinese government, computer hackers recently stole several terabytes of technical specifications pertaining to the Pentagon's $300 billion F-35 Joint Strike Fighter development program, and to the Air Force's air traffic control system.[31]

Given these kinds of cyber threats, federal government contractors implementing cloud computing technologies for DoD should expect compliance requirements related to cybersecurity to continue to evolve. Today, DoD contractors must comply with the Defense Information Assurance Certification and Accreditation Process ("DIACAP") when such requirements are included in their contracts.[32] Federal contractors required to seek C&A under DIACAP should recognize that this can be a lengthy, expensive process.[33] In addition to DIACAP, DoD contractors can expect new regulations to be promulgated related to cybersecurity. For example, Federal Desktop Core Configuration ("FDCC") security setting requirements may be incorporated into the FAR to standardize the FDCC contract clauses federal agencies are already required to include in their IT contracts.[34] Because these kinds of requirements will continue to evolve, Federal government contractors should carefully analyze the cybersecurity specifications in their DoD contracts.

Key Issues Impacting Contractors Using Cloud Computing in the Performance of Federal Government Contracts

Public Cloud Services Employed by Federal Government Contractors

Federal government contractors already use public cloud computing services to carry out their contracts. For example, cloud service providers offer applications and computing power to enable federal contractors to manage and collaborate on government projects in real-time, as well as to automate business processes such as those for timekeeping and compliance with federal fiscal requirements, such as earned value management.[35] Government contractors using these services expect to achieve greater efficiencies through collaborative online

project management and increased visibility into project health.[36]

Government contractors are also hiring cloud service providers that offer "FAR compliant accounting platforms that can satisfy audit requirements of the Defense Contract Audit Agency ("DCAA")."[37] Here small and medium-sized government contractors expect to reduce the cost of compliance with federal government accounting regulations by avoiding the cost of implementing and maintaining such compliance systems in-house, and instead paying commercial cloud providers a less costly usage fee to store, accumulate, and report accounting data in compliance with the FAR.[38] These cloud service providers typically promise a government contractor a certain level of security, as well as 24-hour-a-day, on-demand access to data and applications stored in the cloud.

Cloud Service Providers as Federal Government Subcontractors

A government prime contractor may need to treat its cloud service provider like a government subcontractor when the services, such as those discussed above, are required to perform a federal government contract. This raises several legal issues that government prime contractors should consider carefully to avoid potential administrative, civil or criminal liability. As discussed further below, to mitigate the prime contractor's potential liability, the prime contractor, more often than not, will need to negotiate contract terms with the cloud service provider that the provider would typically not accept from its other commercial customers.

Legal Issues Arising from Government Information Assurance and Security Requirements

Depending on the federal government's view of the criticality or confidentiality of the data maintained by the cloud service provider, a government prime contractor may need to include in its contract with the cloud service provider certain federally mandated information assurance or security requirements. For example, the prime contactor and its cloud service provider may be required to comply with the DIACAP or the NIST C&A standards discussed above. Further, the prime contractor and the cloud provider may be required to allow government inspection of the privacy and security safeguards at their respective facilities, and to notify the government of any failure of those safeguards.[39] In addition, under certain circumstances, the government may require the prime contractor to maintain a continuity-of-operations plan in the event of a catastrophic failure of the primary information systems. In order to execute that plan, the prime contractor may need to contractually impose certain requirements on the cloud service provider. Thus, in order to comply with information assurance and security requirements pursuant to its contract with the government, the prime contractor may need to flow down these same requirements in its contract with the cloud service provider.

Legal Issues Arising from Government Business Practice Requirements

The prime contractor also may need to flow down to the cloud service provider certain government compliance requirements related to business practices in its prime contract. For example, during certain DCAA audits, the government will evaluate the adequacy of the prime contractor's systems, policies, procedures and internal controls related to the performance of its government contracts.[40] If the cloud service provider is operating an internal control system for the prime contractor, such as storing, accumulating and reporting the prime contractor's accounting data in compliance with the FAR, the prime contractor must ensure the cloud service provider is contractually bound to comply with the federal government requirements applicable to the prime contractor, as well as the prime contractor's policies and procedures. If providing cloud-based services for processing the prime contractor's accounting data, the cloud service provider may also be required to comply with the federal government's Cost Principles and Cost Accounting Standards.[41] If the prime contractor does not require the cloud service provider to comply with federal government requirements applicable to the prime contractor, the prime contractor may suffer the consequences of failing a government audit.

Additionally, prime contractors are required to comply with certain document retention requirements under the FAR.[42] A prime contractor should ensure that its cloud service provider's retention policies do not conflict with the FAR requirements, because, among other reasons, the prime contractor needs its data maintained in accordance with the FAR and readily available in the event of a government audit. The case study below provides an illustration of some of this and other potential legal risks, as well as the rewards, of employing a cloud service provider in performing a federal government contract.

Case Study: The Risks and Rewards of a U.S. Federal Government Contractor Employing a Cloud Service Provider to Perform a Federal Government Contract

By way of illustrating the importance of addressing the specific legal implications that arise in the context of government contracts whose performance involves the use of cloud computing, we offer the following hypothetical situation: a Small Business Administration-certified 8(a) staffing company, SB, teams with a joint venture partner, JV, to compete for, and ultimately win, a three-year U.S. Army contract for the provision of medical personnel at various military hospitals and clinics across the country. While SB and JV have performed similar contracts in the past to provide health research and practitioner staff to civilian government agencies, the Army contract represents a new foray into military contracting for both partners. While both partners are aware that the Defense Contracting Audit Agency ("DCAA") will audit the contractors' accounting systems for compliance with the Federal accounting regulations, including the Federal Cost Accounting Standards which are applicable to the joint venture under this contract, neither partner is sure of what is required to comply with those regulations, or how their current systems measure up.

The Rewards of Cloud Computing

Because the Army contract represents an entirely new line of business for SB and JV, and one they are not sure they will continue after completion of the contract, neither is quite ready to assume the expense and complexity involved in adopting new accounting systems that comply with Federal accounting regulations. Thus, SB and JV decide to outsource all of the accounting tasks associated with the Army contract to a mid-sized firm, MF, that has recently announced a new cloud-based accounting service that complies with the FAR ("Federal Acquisition Regulation"). The terms of the Army contract do not prohibit this kind of subcontracting, but the contract also does not explicitly specify terms & conditions related to data retention under the FAR that should be flowed down to such a contractor. Further, the prime contractor fails to flow down these FAR requirements to the cloud computing service provider.

The Risks of Cloud Computing

The contract, to all outside observers, is successfully performed by SB and JV. In fact, all is well, until just under two years after the contract is completed and final payment has been made. At this point, a woman who worked as a dental hygienist under the contract alleges that irregularities in the electronic timecard system employed by SB and JV led it knowingly to submit false invoices to the Army, and thereby violate the False Claims Act. The Government intervenes and DCAA immediately initiates an audit of the completed contract. Unfortunately, though DCAA found MF's accounting system complied with Federal accounting regulations during performance of the contract, MF failed to maintain the accounting data for the period of time required by the FAR after the contract was completed. Many of the records no longer available include accounting data from the Army contract, the production of which DCAA now demands. Thus, the prime contractor no longer has the accounting data it was required to maintain under the FAR to support costs it billed to the Army. As a result, the prime contractor will have greater difficulty refuting the alleged false claim to the Army.

Mitigating the Risk

This scenario demonstrates the importance of structuring the prime contractor-subcontractor relationship in light of the Federal government's right to audit the performance of a contract. This is particularly true where the prime contractor decides to subcontract the task of managing data essential to the contract's performance (and therefore relevant to any potential audit). When the subcontractor provides its services through cloud computing, even if the prime-subcontractor agreement mandates near-constant availability of the data, the prime contractor must take care to ensure that the particular requirements for data maintenance imposed by the FAR are flowed down to the subcontractor. As added protection, the prime contractor may also seek a contract clause providing that the subcontractor will indemnify the prime contractor for liability that arises in the event that the subcontractor fails to maintain the data as specified in the prime-subcontractor arrangement. From the subcontractor's perspective, it is equally important to understand the terms of the arrangement, particularly the responsibility it imposes on the subcontractor to provide a certain level of data and services, and exactly what that level is. A cloud computing subcontractor who agrees to indemnify the prime contractor in the event that essential data is lost or inaccessible may choose to build the cost of this provision, or the cost of undertaking insurance for such a contingency, into its price to the prime contractor.

What You Should Do

Like other technology-related developments of the past hundred years, cloud computing poses benefits and risks for Federal government contractors. But failing to recognize the unique legal implications of cloud computing presented by each Federal contracting opportunity, and to carry on with business as usual, could expose a contractor to potentially significant liability. Federal government contractors should work with legal counsel to identify and mitigate those risks, including starting early in the contracting process with the negotiation of terms and conditions of the prime contract and any related subcontracts. By mitigating those risks, a Federal government contractor paves the way for using the cloud to revolutionize how it does business with the Federal government.

— Biographies of Authors —

Lorraine Mullings Campos, Partner – Washington D.C. +1 202 414 9386 lcampos@reedsmith.com

Lorraine's practice focuses on assisting clients with a variety of issues related to government contracts, government ethics, campaign finance, and lobbying laws. She has particular experience in counseling clients regarding Federal Supply Schedules, creating company ethics and compliance programs related to doing business with the Federal government, conducting internal investigations, drafting and negotiating government contracts and subcontracts, and facilitating government contract compliance training. She also counsels clients on bid protest matters, federal grant programs, federal audits, and the application of the Federal Acquisition Regulation ("FAR") and individual agency supplement procurement regulations.

Stephanie E. Giese, Associate – Washington D.C. +1 202 414 9246 sgiese@reedsmith.com

Stephanie counsels clients in matters involving federal government contracts and international trade. With regard to her federal government contracts practice, she advises high-technology clients in government and commercial contract transactions, federal grants and related litigation. Her experience includes advising federal government contractors on matters which involve claims, cost recovery and accounting, contract and subcontract administration, and rights in technical data. Stephanie advises clients regarding virtually every principal defense and civilian agency, the Department of Defense (DoD) (including all three Departments and the Defense Contract Audit Agency (DCAA)), the Intelligence Community, Department of Justice (DoJ), General Services Administration (GSA), National Aeronautics and Space Administration (NASA), National Institutes of Health (NIH), Department of Transportation (DoT), Department of Homeland Security (DHS), Department of Energy (DoE) and the Environmental Protection Agency (EPA). With regard to international trade, Stephanie's practice includes resolving export control, sanction and embargo issues subject to the jurisdiction of the U.S. Departments of Commerce, State and Treasury. In particular, she advises high-technology clients regarding obtaining export authorization and developing export control compliance programs. She also conducts internal investigations and prepares voluntary disclosures on behalf of clients.

Joelle E.K. Laszlo, Associate – Washington D.C. +1 202 414 9212 jlaszlo@reedsmith.com

Joelle is an associate in the Global Regulatory Enforcement group in the Washington, D.C. office.

— CLOUD COMPUTING TASK FORCE LEADERS—

Joseph I. Rosenbaum
Partner and Chair, Advertising Technology & Media Law Group
jrosenbaum@reedsmith.com
+1 212 702 1303

Joe is a member of Reed Smith's global Advertising Technology & Media Law practice, and has more than 30 years of international experience across a wide range of sophisticated and complex commercial transactions, in industries including advertising, entertainment and media, financial services, travel-related services, technology and many more. Joe specializes in the law and policy arising at the intersection of technology and online and behavioral advertising, social media, entertainment, finance, e-commerce, information security and digital rights, online gaming, promotions, privacy and data protection, among others. Joe's experience includes virtual worlds, mobile marketing, digital payments and PCI compliance, digital broadcasting, co-branded credit and gift cards, loyalty rewards programs, branded entertainment, online product placement and endorsements, user-generated content, buzz, word-of-mouth and viral marketing, licensing, software development and outsourcing. Joe lectures and writes extensively and, among others, has authored a book on outsourcing (*Outsourcing Agreements Line by Line*; Aspatore Publishing, 2004) and a seminal law journal article on privacy ("Privacy on the Internet: Whose Information Is It Anyway?"; *Jurimetrics Law Journal*, 1998). Joe's work has been cited by appellate courts, law reviews and journals, industry and trade periodicals. Joe is regularly quoted in widely respected publications such as the *National Law Journal*, Advertising Age, the American Banker, Euromoney and has been interviewed and appeared as a commentator on CNBC's *Squawkbox* and CNN Financial's *Business Unusual*. Joe is General Counsel & Secretary to the Interactive Advertising Bureau and a member of the Advisory Board of the Center for Law, Science and Technology at the Sandra Day O'Connor College of Law at ASU.

Adam W. Snukal
Senior Associate, Advertising Technology & Media Law Group
Business & Finance - Corporate & Securities
asnukal@reedsmith.com
+1 212 549 0333

Adam is a senior associate, based in New York, within the global Advertising Technology & Media Group at Reed Smith. Adam's legal background includes diverse, complex and extensive experience both in business law counseling and in advising on advertising, technology and media-related matters. Adam's experience in the area of information technology spans both strategic and commercial software licensing, large-scale procurement, e-commerce-related matters, financial services, health care and medical devices, wireless technology, outsourcing and gaming. In the area of advertising, Adam regularly counsels clients on traditional, online and mobile marketing/advertising related matters, advertising and marketing agreements, media buying, trademark/brand licensing, user generated content, privacy, sweepstakes, contests, gaming and advergaming, website and WAP site development, digital content development/distribution/aggregation, celebrity endorsements and more.

— Endnotes —

1 EXECUTIVE OFFICE OF THE PRESIDENT, BUDGET OF THE U.S. GOVERNMENT, FISCAL YEAR 2011 (Feb. 1, 2010), *available at* http://www.whitehouse.gov/omb/budget/Overview.

2 *See id.* at 42, *available at* http://www.whitehouse.gov/omb/budget/fy2011/assets/budget.pdf ("the Administration will continue to roll out less intensive and less expensive cloud-computing technologies; reduce the number and cost of Federal data centers; and work with agencies to reduce the time and effort required to acquire IT, improve the alignment of technology acquisitions with agency needs, and hold providers of IT goods and services accountable for their performance"); *see also* EXECUTIVE OFFICE OF THE PRESIDENT, ANALYTICAL PERSPECTIVES, BUDGET OF THE U.S. GOVERNMENT, FISCAL YEAR 2011 at 321 (Feb. 1, 2010), *available at* http://www.whitehouse.gov/omb/budget/fy2011/assets/spec.pdf ("Adoption of a cloud computing model is a major part of the strategy to achieve efficient and effective IT").

3 *See, e.g.*, EXECUTIVE OFFICE OF THE PRESIDENT, ANALYTICAL PERSPECTIVES, BUDGET OF THE U.S. GOVERNMENT, FISCAL YEAR 2010 at 158 (Feb. 26, 2009), *available at* http://www.gpoaccess.gov/usbudget/fy10/pdf/spec.pdf ("Initial [cloud computing] pilots conducted in collaboration with Federal agencies will serve as test beds to demonstrate capabilities, including appropriate security and privacy protection at or exceeding current best practices, developing standards, gathering data, and benchmarking costs and performance. The pilots will evolve into migrations of major agency capabilities from agency computing platforms to base agency IT processes and data in the cloud.").

4 Peter Mell and Tim Grance, Nat'l Inst. of Standards and Tech., The NIST Definition of Cloud Computing (2009), *available at* http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc.

5 Vivek Kundra, U.S. Chief Info. Officer, Exec. Office of the President, Press Conference: In the Cloud (Sept. 15, 2009), *available at* http://www.whitehouse.gov/blog/streaming-at-100-in-the-cloud/.

6 *See* U.S. Gen. Servs. Admin., Apps.gov, https://www.apps.gov/cloud/advantage/main/start_page.do (last visited Apr. 14, 2010).

7 *See* Mell and Grance, *supra* note 4.

8 This is also why Apps.gov represents a hybrid cloud. While the website itself technically is not a cloud, the capabilities that are and will be offered through it span the complete range of cloud models.

9 All vendors seeking to offer their commercial products and services through Apps.gov must be part of GSA's Schedule 70 (Information Technology). The process for soliciting a Schedule 70 contract is detailed on the GSA's website (see, for example, http://www.gsa.gov/gettingonschedule) and will not be reviewed here, nor will the unique procedures applicable to Schedule-based procurements. Reed Smith's Government Contracts & Grants attorneys are available to assist with any aspect of GSA's Scheduling process and procurement.

10 Available at http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

11 *See* U.S. Gen. Servs. Admin., Frequently Asked Questions, https://apps.gov/cloud/advantage/main/start_page.do (follow "Cloud FAQs" hyperlink) (last visited Apr. 14, 2010) [hereinafter *GSA FAQs*].

12 *See, e.g.,* J. Nicholas Hoover, "GSA to Update Cloud Computing Web Site," INFORMATIONWEEK, Mar. 24, 2010, *available at* http://www.informationweek.com/news/government/cloud-saas/showArticle.jhtml?articleID=224200193.

13 *See GSA FAQs*, *supra* note 11.

14 *See* Hoover, *supra* note 11.

15 Available at http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf.

16 *See, e.g.,* J. Nicholas Hoover, "GSA Outlines U.S. Government's Cloud Computing Requirements," INFORMATIONWEEK, Aug. 3, 2009, *available at* http://www.informationweek.com/news/government/cloud-saas/showArticle.jhtml?articleID=218900541.

17 Thus a provider of social media applications does not need to obtain a Schedule 70 contract, or any contract, before requesting to offer its products through Apps.gov. *See GSA FAQs*, *supra* note 11.

18 *See* U.S. Gen. Servs. Admin., Vendor Frequently Asked Questions, https://apps.gov/cloud/advantage/main/start_page.do (follow "Vendor FAQs" hyperlink) (last visited Apr. 14, 2010).

19 See https://forum.webcontent.gov/resource/resmgr/model_amendment_to_tos_for_g.pdf.

20 *See, e.g.*, Eric Chabrow, "DISA's Cloud Computing Initiatives," GOVERNMENT INFORMATION SECURITY, May 27, 2009, *available at* http://govinfosecurity.com/articles.php?art_id+1493&rf=03231eg.

21 *See, e.g., id.*

22 *See* Intl. Bus. Mach., Ctr. for the Bus. of Gov't, Cloud Computing in Government 26 (2009), http://www.businessofgovernment.org.

23 *See id.*

24 *See* Warren Suss, "5 Lessons from DoD's Cloud Computing Efforts," GOVERNMENT COMPUTER NEWS, Sept. 23, 2009, *available at* http://gen.com/Articles/2009/09/28/Warren-Suss-5-lessons-of-cloud-computing.asp.

25 *See* Jill R. Aitoro, "DISA to Offer On-Demand Computing in 2009," NEXTGOV, July 11, 2008, *available at* http://www.nextgov.com/nextgov/ng_20080711_1829.php.

26 *See id.*

27 *See id.*

28 *See, e.g.*, Elizabeth Moltabano, "Navy Awards $1.75 Billion IT Contracts," INFORMATIONWEEK, Mar. 8, 2010. *available at* http://www.informationweek.com/news/government/enterprise-architecture/showArticle.jhtml?articleID=223200156.

29 *See id.*

30 *See, e.g.*, Interview by Katie Couric, CBS News, with Robert Gates, U.S. Sec'y of Def. (Apr. 22, 2009), *excerpted in* "DoD Gates: We're Always Under Cyberattack," TECH NEWS, *available at* http://news.zdnet.com/2100-9595_22-290770.html.

31 *See, e.g., id.*

32 *See, e.g.*, Chabrow, *supra* note 20.

33 *See, e.g., id.*

34 *See, e.g.*, Matthew Weigelt, "Contract Rules Need IT Security Standards, Official Says," FEDERAL COMPUTER WEEK, April 13, 2010, *available at* http://fcw.com/articles/2010/04/13/fdcc-contract-language-gao.asp. The FDCC is a White House initiative that gave agencies a minimum set of standards for protecting their desktop and laptop computers from cyber threats.

35 *See, e.g.*, NetSuite Inc. and OpenAir, Inc., Press Release: OpenAir Expands Research into Government Services Market (Feb. 25, 2009), *available at* http://www.openair.com/home/n_r_022509.html.

36 *See, e.g., id.*

37 "VentureCount Launches New Cloud Accounting Solution for Government Contractors," MARKET WIRE, October 2009, *available at* http://findarticles.com/p/articles/mi_pwwi/is_200910/ai_n39260187/.

38 *See id.*

39 *See* the "Privacy and Security Safeguards" clause at 48 C.F.R. § 52.239-1.

40 *See, e.g.*, DCAA Contract Audit Manual § 3-104.11.

41 *See, e.g.*, the Cost Principles at 48 C.F.R. § 31 and the Cost Accounting Standards at 48 C.F.R., Chapter 99, which apply to certain federal government contracts.

42 *See* 48 C.F.R. §§ 4.7 – 4.8.