This material from BRIEFING PAPERS has been reproduced with the permission of the publisher, Thomson Reuters. Further use without the permission of the publisher is prohibited. For additional information or to subscribe, call 1-800-344-5009 or visit west.thomson.com/fedpub. BRIEFING PAPERS is now available on Westlaw. Visit westlaw.com

BRIEFING PAPERS® SECOND SERIES

WEST®

PRACTICAL TIGHT-KNIT BRIEFINGS INCLUDING ACTION GUIDELINES ON GOVERNMENT CONTRACT TOPICS

CLOUD COMPUTING ACQUISITIONS & CYBERSECURITY

By David Z. Bodenheimer

Cloud computing has been described by some as evolutionary. Others have called it revolutionary. Either way, the accelerating federal "Cloud First" initiatives, the tightening squeeze for greater governmental efficiencies, and the spiraling advances in cloud technology have converged, unleashing extraordinary incentives for—and pressures upon—federal agencies and Government contractors to find cloud solutions to federal information technology needs. As a result, both agencies and contractors will face the challenges of traversing this seismic shift from traditional IT buys to cloud acquisitions—while at the same time, the acquisition practices, cybersecurity rules, and cloud technology all continue to evolve in parallel.

Cloud computing brings a host of complexities to the federal acquisition process and information security. First, the cloud takes many forms, thus requiring acquisition methods and security safeguards to be tailored to the particular type of cloud chosen by the parties. Second, a variety of economic factors drive the rapid spread of the cloud, sometimes outpacing the evolution of standardized acquisition and security programs in the public sector. Third, security continues to be a major concern in the movement to the cloud, thus magnifying the challenges of adapting evolving security programs to moving targets in cloud technology. Fourth, acquisition of cloud computing in the public sector remains as relatively new territory for both agencies and contractors—and its newness presents its own set of challenges.

This BRIEFING PAPER addresses these four core challenges of adapting existing acquisition rules and practices to procurements for cloud services

IN BRIEF

David Z. Bodenheimer is a partner in the Washington, D.C. office of Crowell & Moring LLP, where he heads the Homeland Security Practice and specializes in Government contracts, False Claims Act, privacy, and cybersecurity litigation, investigations, and counseling.

 THOMSON REUTERS © COPYRIGHT 2012 ALL RIGHTS RESERVED

and technology, while maintaining cybersecurity and privacy and meeting other federal mandates for federal IT systems and information. The PAPER considers the following questions:

(1) *Defining the Cloud*. What forms does the cloud take—and how do acquisition practices and information security need to be tailored for these differences?

(2) *Driving the Cloud*. What are the drivers speeding the cloud into the public sector—and what does this mean for cloud acquisitions and cybersecurity?

(3) *Securing the Cloud*. What are the key concerns about cloud security—and what are the security regimes applicable to the public sector?

(4) *Acquiring the Cloud*. What is the public sector guidance on cloud acquisitions—and what are the challenges ahead?

For these questions, some of the answers exist in freshly minted guidance that has not been fully implemented, much less tested in the heat of major litigation, congressional scrutiny, or serious security breaches. Until agencies and contractors in the public sector gain greater experience and more detailed guidance on cloud acquisitions and security, the current standards and directives from the federal sector identify some of the key risks, issues, and business decisions that public and private professionals face in working on the cloud frontier.

Defining The Cloud & Its Variations

Like its namesake, cloud computing takes many forms. Indeed, its wide-ranging variability is one of the cloud's great advantages—it can be flexibly adapted to a multitude of customer needs. However, these many variations in clouds may present differences in acquisition and security risks, needs, and allocation of the parties' responsibilities.

Defining the cloud has important practical consequences for agencies and contractors. For example, different cloud service models and deployment methods may require different allocations of risks and responsibilities between the agency and the cloud service provider. In addition, poorly defined cloud requirements may invite protests and claims from contractors due to misunderstandings about the agency's actual needs and requirements. Finally, whether an IT acquisition qualifies as a cloud procurement is important for such purposes as the Office of Management and Budget's oversight and metrics, choice of the information security regime, and methods for acquisition. As a result, defining the cloud and its different guises is an important first step to picking the right contract and security arrangements between the parties.

■ Definition Of Cloud Computing

The National Institute of Standards and Technology has been active in providing guidance and definitions to establish a common language for discussing, acquiring, and securing the cloud in the public sector.[1] NIST defines "cloud computing" as follows:[2]

> Cloud computing is a model of 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.

WEST®

BRIEFING PAPERS

This publication was created to provide you with accurate and authoritative information concerning the subject matter covered; however, this publication was not necessarily prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice, and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional.

BRIEFING PAPERS® (ISSN 0007-0025) is published monthly except January (two issues) and copyrighted © 2012 ■ Valerie L. Gross, Editor ■ Periodicals postage paid at St. Paul, MN ■ Published by Thomson Reuters / 610 Opperman Drive, P.O. Box 64526 / St. Paul, MN 55164-0526 ■ http://www.west.thomson.com ■ Customer Service: (800) 328-4880 ■ Postmaster: Send address changes to Briefing Papers / PO Box 64526 / St. Paul, MN 55164-0526

BRIEFING PAPERS® is a registered trademark used herein under license. All rights reserved. Reproduction, storage in a retrieval system, or transmission of this publication or any portion of it in any form or by any means, electronic, mechanical, photocopy, xerography, facsimile, recording or otherwise, without the written permission of Thomson Reuters is prohibited. For authorization to photocopy, please contact the Copyright Clearance Center at 222 Rosewood Drive, Danvers, MA 01923, (978)750-8400; fax (978)646-8600 or West's Copyright Services at 610 Opperman Drive, Eagan, MN 55123, fax (651)687-7551.

Some may find this definition to be too abstract for such a multi-faceted and fluid concept. To provide more concrete descriptions of cloud computing, NIST has also identified five essential characteristics, three service models, and several deployment models that may foster a sharper understanding for agencies and contractors to identify what falls within the broad ambit of the many forms of the cloud.[3]

These NIST definitions and taxonomy of cloud computing have gained wide currency in the federal sector, as the Federal Chief Information Officer, the Government Accountability Office, trade organizations, and industry members have adopted NIST definitions and terminology for the cloud.[4]

■ Essential Characteristics Of The Cloud

Some have compared the cloud to a utility like electric service.[5] Rather than each consumer having his or her own candle (or power generator), the consumer instead uses power from the electric power company when needed (by flipping on the light switch) and as much as needed (by turning off the light when done). In turn, the power company measures the amount of electric service and sends a bill each month based upon the consumer's usage.

Given that the cloud takes many forms, NIST has captured this basic consumer/utility relationship and summarized it into five essential characteristics defining the cloud:[6]

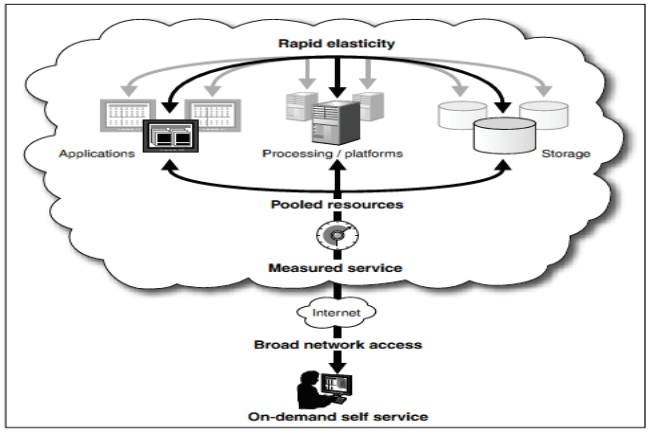
> *On-demand self-service.* A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
>
> *Broad network access.* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
>
> *Resource pooling.* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, and network bandwidth.
>
> *Rapid elasticity.* Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
>
> *Measured service.* Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

These characteristics reflect the utility model in which a provider gains economies of scale by investing in bulk capacity, aggregating consumers, and furnishing on-demand services that—from the consumer's vantage point—may appear virtually unlimited and infinitely elastic. The consumer receives services when, where, and how much needed, paying only for what is actually used.

To provide a visual example of these five fundamental characteristics of cloud computing, the GAO developed Illustration I, below, showing both the interface and allocation of functions between the consumer and the cloud provider:[7]

Illustration I

Figure 3: NIST Essential Characteristics



This model works well when service is flowing without interruption—like an electric utility before

the storm-driven power outage. However, when the utility becomes a target for foreign adversaries or terrorists,[8] then risk allocation and security issues become paramount. In short, the cloud's utility model alters the nature and allocation of the risk of security breaches, denial-of-service attacks, and network penetrations as hackers have fewer—but richer—targets for attacks.

■ Service Models For The Cloud

The level of service by a cloud provider exists upon a sliding scale ranging from providing some basic hardware to furnishing a full turnkey operation. As part of its definitions of cloud computing, NIST has described three service models that vary based upon how much responsibility the customer retains—and how much the customer turns over to the cloud service provider. NIST has defined the following three models of service:[9]

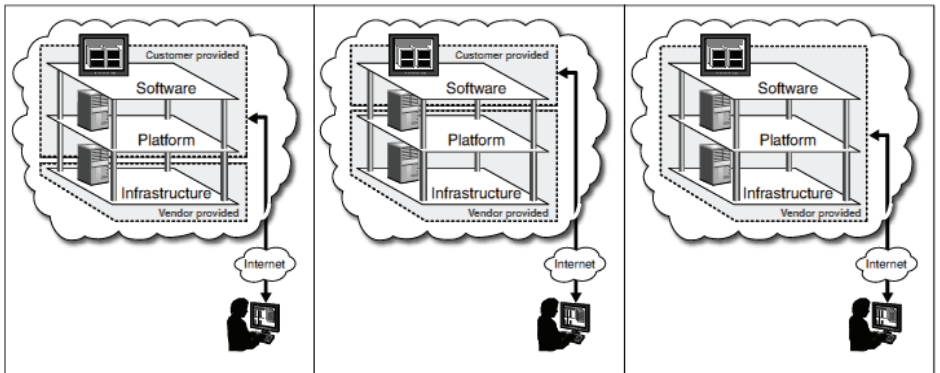
> *Cloud Software as a Service (SaaS).* The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual applications capabilities, with the possible exception of limited specific application configuration settings.
>
> *Platform as a Service (Paas).* The capability provided to the consumer is 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 configuration settings for the application-hosting environment.
>
> *Infrastructure as a Service (Iaas).* The capability provided to the consumer is 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, and deployed applications; and possible limited control of select networking components (e.g., firewalls).

To move from the abstract to the concrete, some have used pictures to illustrate these varying service models. For example, the GAO has presented Illustration II, below. As this illustration reflects, the cloud provider (vendor) furnishes relatively discrete services for "Infrastructure as a service," while "Software as a service" means that the cloud provider essentially provides everything.[10]

In another example, the Corporate Vice President for Trustworthy Computing for Microsoft has demonstrated how the different models shift responsibility

Illustration II

Figure 1: Cloud Computing Service Models



Infrastructure as a service
The consumer has the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run his or her own software, which can include operating systems and applications. The consumer does not manage or control the underlying infrastructure but controls and configures operating systems, storage, deployed applications, and possibly, selected networking components (e.g., host firewalls).

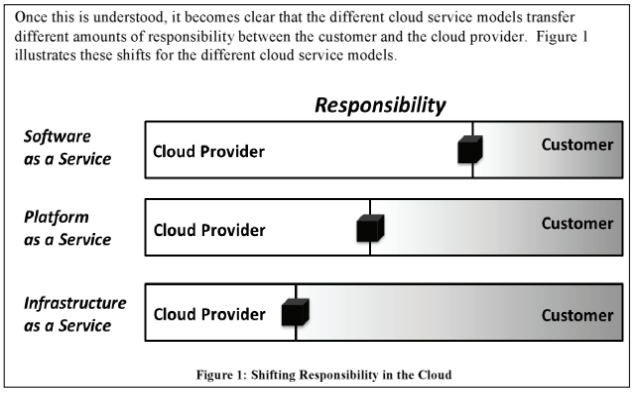
Platform as a service
Consumers deploy consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying infrastructure, but controls and configures the deployed applications and platform.

Software as a service
Consumer uses the provider's applications that are accessible from various client devices through an interface such as a Web browser (e.g., Web-based e-mail). The consumer does not manage or control the underlying infrastructure or the individual application capabilities.

Briefing Papers © 2012 by Thomson Reuters

between the customer and the cloud service provider. This shown in Illustration III, below:

Illustration III



This shift in responsibility also means that the cloud provider undertakes greater responsibility, ranging from "physical and personnel security to the secure development and maintenance of applications and the management of identities for access control."[11]

In summary, the choice of service model for cloud computing not only affects who bears what responsibility for each level of service (infrastructure, platform, and service), but also the security relating to such services. If the security responsibilities are not aligned with the service model, a gap or ambiguity may arise regarding who bore the obligation to secure a particular part of the service and the related interfaces. In other words, the customer and provider need to match the information security responsibility with the service responsibility to avoid contractual disputes between the parties—and potential tort liability in the event of a major security breach.

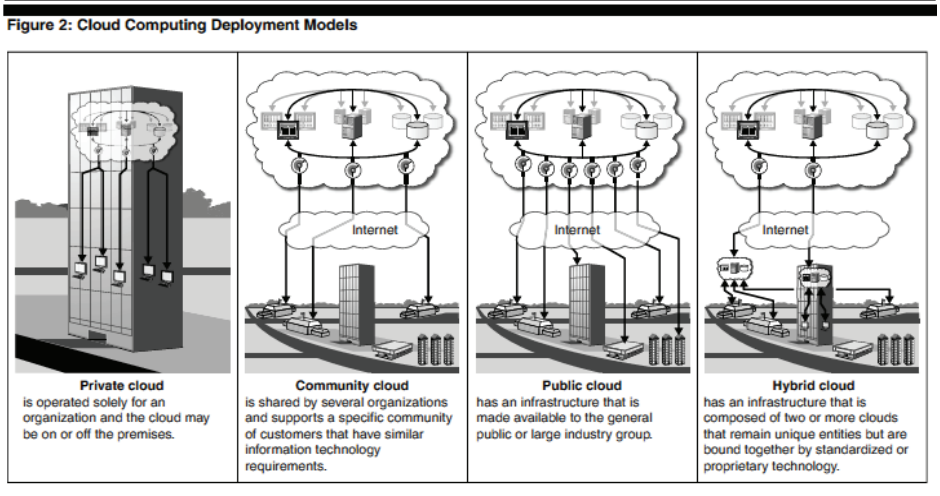
■ Deployment Models For The Cloud

The cloud may vary in yet another way—how widely or narrowly the provider deploys a particular cloud among the customers. NIST has broken these options into four deployment models:[12]

> *Private cloud.* The cloud infrastructure is provisioned for exclusive use by a single organization comprising 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.
>
> *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 premises.
>
> *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.
>
> *Hybrid cloud.* The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and applications portability (e.g., cloud bursting for load balancing between clouds).

Once again, the GAO has provided illustrations showing the similarities and differences of these deployment methods for cloud computing, as shown in Illustration IV, below:

Illustration IV



As these illustrations show, these deployment models affect what customers share a particular cloud and—for a hybrid cloud—under what circumstances.[13]

The deployment method affects the level of security risk to information. In testimony before Congress, the Federal Chief Information Officer (CIO) stated:[14]

> In the case of cloud computing, we expect these risk models to vary based on the specific cloud deployment model used (e.g., private cloud versus public cloud). Agencies will incorporate these risk models into their business decision-making processes and use them to inform the development of comprehensive agency risk management plans that address issues such as continuity of service, quality control, and long-term preservation of data to support Federal records requirements.

Similarly, the GAO has reported that security "risks may vary based on the cloud deployment model."[15] As a result, both the public and private sector need to weigh the particular deployment method against the security threats and controls available to mitigate the risk to information security and privacy.

Driving The Cloud Into The Public Sector Marketplace

The movement of the public sector to the cloud is a virtual certainty. The only real questions are how, when, and at what risk. Three key factors will press the accelerator for the federal transition to cloud computing—budget and cost-cutting pressures, the federal policy favoring cloud implementation, and trends in the commercial marketplace. And, in turn, the federal shift to the cloud will likely expand the cloud market in other public sectors, such as state and local governments.

■ Budget & Cost-Cutting Pressures

The Federal Government represents the largest buyer of IT technology and services anywhere. During a congressional hearing, the Federal CIO underscored this point:[16]

> The U.S. Government is the largest buyer of IT on the planet. We spend approximately $80 billion annually on information technology systems.

Furthermore, such IT expenditures have been steadily rising over the years, "from just over $46 billion in 2001 to nearly $80 billion in fiscal year 2012."[17] The OMB confirmed this sharp rise in IT spending over the past decade, noting that these figures exclude certain expenditures, such as national security systems.[18] Some have questioned whether federal agencies have achieved the expected efficiencies and productivity gains "despite spending more than $600 million on IT over the past decade."[19]

The cloud concept offers potential opportunities to go gain efficiencies and save money on such federal IT expenditures:[20]

> A major benefit of cloud computing is the potential for significant cost savings. It makes sense: cloud computing allows agencies to pool resources and pay only for the computing power that they actually use.

Like the utility model, federal agencies would reduce upfront IT investment costs and gain the cost benefits of economies of scale offered by cloud service providers.

Greater efficiencies and cost savings have often been identified as key factors in making the transition to the cloud.[21] The estimates for such anticipated savings vary widely:[22]

> *Cost Saving.* Cloud computing allows customers to pay for just the computer resources that they use. They can avoid both a large initial upfront expenditure in hardware and software, and ongoing operating and maintenance expenses for their own IT. Resource usage can be monitored, controlled, and reported in a transparent way for both the provider and consumer of the cloud service. Indeed a Brookings Institution study found that "…agencies generally saw between 25 and 50 percent savings in moving to the cloud"; this same report refers to other studies which claim savings from 39% to 99%.

For federal agencies, the prospect for significant savings will make the switch to the cloud virtually irresistible, particularly with looming austerity measures and budget cuts around the corner.

Everybody knows about the federal budget crunch. And federal IT spending has landed in the middle as a potential target for the budget chopping block:[23]

> Congress has curtailed IT funding along with other investments, with little or no new money

Briefing Papers © 2012 by Thomson Reuters

> for realizing IT's potential. Financial relief is not likely for several years to come, yet during that time citizen demand for digital public service will continue to swell.

The OMB articulated its "do-more-with-less" view for federal IT efforts: "Agencies today face unprecedented pressures—a rapidly evolving technology landscape, rising public expectations, and the need to operate securely in an increasingly interconnected world—all while we are driving toward flat or declining budgets."[24]

Both Congress and the OMB view cloud implementation as a key to expanding IT services while cutting IT expenditures.[25] Such budget pressures increase the leverage of both Congress and the OMB to drive agencies towards more rapid transition to the cloud. And the prospect of cost savings multiply the likelihood that such agencies will move faster to embrace the cloud.

■ Federal Policy Of "Cloud First"

The OMB has made the transition to the cloud an Executive Branch priority. In February 2011, the OMB issued its cloud strategy establishing a "Cloud First" policy:[26]

> The *Federal Cloud Computing Strategy* states that "When evaluating options for new IT deployments, OMB will require that agencies default to cloud-based solutions whenever a secure, reliable, and cost-effective cloud options exists."

More recently, the OMB reaffirmed its "Cloud First" strategy to accelerate implementation of cloud services:[27]

> Federal Agencies are to implement this strategy and make Shared-First the default approach to IT service planning and delivery. By August 31, 2012, Federal Agencies must submit to OMB an Enterprise Roadmap for the FY 2012–2015 timeframe that includes a business and technology architecture, IT asset inventory, Portfolio Stat results, and IT Shared Services Plan. A [Line-of-Business] Plan will also be included in the Enterprise Roadmap of the hosting Federal Agency.

This "Cloud First" policy has "led to the successful migration of 40 services to cloud with an additional 39 migrations to come by June 2012."[28]

As these federal policies underscore, the OMB holds both the carrot (money for cloud IT) and the stick (not approving non-cloud IT initiatives) for agency IT budgets. As a result, the OMB has considerable leverage to make cloud technology and services a priority, thus pressuring federal agencies to steer their IT requirements towards cloud solutions.

Federal acquisitions of cloud technology and services will also spur more sellers to enter the federal marketplace:[29]

> Further, the [OMB] strategy notes that an estimated $20 billion of the federal government's $80 billion in annual IT spending is a potential target for migration to cloud computing solutions.

The infusion of approximately $20 billion into the federal market will attract more competitors, better technology, and greater savings, thus potentially accelerating the pace of implementing the cloud among federal agencies.

■ Cloud Trends In The Commercial Marketplace

In the private sector, the surge to the cloud continues to accelerate, as businesses seek to cut IT investments and reap substantial cost savings and efficiencies:[30]

> [A] McKinsey survey of 250 chief information officers (CIOs) of large companies across different industries found that they expect over two-thirds of corporate applications to be virtualized by 2014. Virtualization cuts the cost of computing by up to 50 percent with savings gains from lower infrastructure operational costs. Not only are legacy applications being virtualized, new IT investments are predominantly in cloud computing. [International Data Corporation] estimates that 80 percent of new commercial applications deployed this year will be on cloud computing platforms.

Similarly, global markets will drive the transition to cloud computing, as cloud sales generate multi-billion-dollar marketplaces:[31]

> Worldwide adoption of cloud computing is growing rapidly. On the low end, the International Data Corporation (IDC) estimates that the global market for cloud computing will grow to $56 billion by 2014. American Megatrends, Inc. (AMI) research predicts that the market for cloud computing will reach $100 billion by 2014 for small and medium businesses alone. Forrester Research predicts the market for cloud computing will grow from approximately $41 billion in 2011 to $241 billion by 2020. Software as a service is expected to make up the bulk of this market at approximately $133 billion in 2020 worldwide.

Escalating commercial sales have significant implications for federal cloud acquisitions. Global

competition will expand cloud options, propel innovation, and further reduce costs, thus making it more difficult for federal agencies to justify non-cloud solutions for future IT acquisitions.

In addition, the Federal Acquisition Streamlining Act of 1994 directs federal agencies to acquire commercial items "to the maximum extent practicable."[32] By law, this statutory preference for commercial items applies to both military and civilian agencies.[33] As the cloud displaces other IT options, this statutory preference ("Commercial First") will reinforce federal policy ("Cloud First"), thus applying additional pressure upon federal agencies to switch to the cloud.

Finally, contractors should benefit from the commercial nature of cloud services, as the streamlined procedures for the acquisition of commercial items in Federal Acquisition Regulation Part 12 should relieve contractors of many of the regulatory burdens that have discouraged commercial contractors from selling to the Government in the past. In recent years, both Congress and agencies have throttled back on what acquisitions qualify for commercial item status. In this environment, cloud providers must be alert to preserving FAR Part 12 commercial status for cloud acquisitions to assure that agencies reap the full benefits of acquiring cloud services available in the commercial marketplace—including commercial technology innovation, economies-of-scale efficiencies, and expanded fields of competitors.

Securing The Cloud In The Security-Breach Era

Effective information security is paramount to successful cloud computing. As stated by the General Services Administration Associate Administrator responsible for cloud implementation, "[o]ne of the most significant obstacles to the adoption of cloud computing is security."[34] As a result, both federal agencies and Congress have underscored the importance of sound information security as an essential element of federal cloud initiatives. Both NIST and the GSA have been active in developing cybersecurity standards for cloud acquisitions. At the same time, some of these security measures raise significant acquisition issues.

■ Security Concerns Relating To Cloud Computing

Congress, the GAO, and federal agencies have all expressed concerns about cloud initiatives compromising information security. During hearings, members of Congress have identified "security and privacy [as] real concerns."[35] Similarly, the GAO has issued a host of reports addressing the information security risks of cloud computing. For example, the GAO recently summarized its findings, placing federal security requirements at the top of the list of challenges to cloud computing:[36]

> Common Challenges to Cloud Computing
>
> 1. Meeting Federal Security Requirements
>
> 2. Obtaining guidance
>
> 3. Acquiring knowledge and expertise
>
> 4. Certifying and accrediting vendors
>
> 5. Ensuring data portability and interoperability
>
> 6. Overcoming cultural barriers
>
> 7. Procuring services on a consumption (on-demand) basis

The Associate Administrator heading the GSA's cloud implementation has acknowledged that "the number one issue for years in cloud has been security."[37] A GAO survey of major federal agencies confirmed security as a major concern for cloud computing:[38]

> The use of cloud computing can also create numerous information security risks for federal agencies. Specifically, 22 of 24 major federal agencies reported that they were either concerned or very concerned about the potential information security risks associated with cloud computing. Risks include dependence on the security practices and assurances of vendors and the sharing of computing resources.

History bears out these concerns. In the private sector, one of the largest security breaches involved a provider of cloud services:[39]

> Epsilon, an email service provider for companies, reported a breach that affected approximately 75 client companies. Email addresses and customer names were affected. Epsilon has not disclosed the names of the companies affected or the total number of names stolen. However, millions of customers received notices from a *growing list* of companies, *making this the largest security breach ever*. Conservative estimates place the number of

Briefing Papers © 2012 by Thomson Reuters

> customer email addresses breached at 50 to 60 million. The number of customer emails exposed may have reached 250 million.
>
> * * *
>
> The Epsilon breach is also significant because it highlights the risk of cloud-based computing systems and the need for greater cloud security measures.

Similarly, "Google reported that in December 2009, an attack was made on e-mail accounts that it provided, which resulted in the inadvertent release of sensitive information."[40]

In summary, the federal "Cloud First" policy necessarily hinges upon effective information security as a prerequisite. Without such security, cloud computing will not be viable. Nor have Congress, the GAO, or federal agencies shown enthusiasm for accepting serious risks to national security information, trade secrets, or sensitive personal data now housed in federal networks and databanks without adequate security precautions being implemented as part of cloud computing initiatives.

■ Security Standards For The Cloud

In outlining its cloud strategy in 2011, the OMB stated its objective to achieve higher security with cloud computing than security existing in the current IT environment:[41]

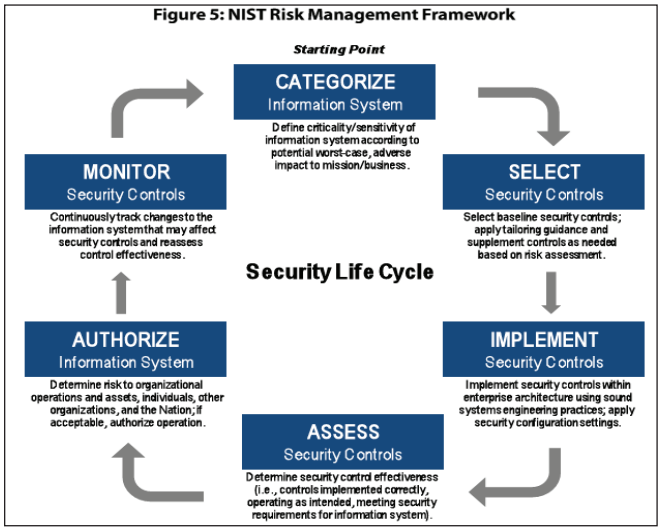
> The Federal Government will create a transparent security environment between cloud providers and cloud consumers. The environment will move us to a level where the Federal Government's understanding and ability to assess its *security posture will be superior to what is provided within agencies today.*

In addition, the OMB outlined key security considerations that must be considered as part of the cloud transition:[42]

- *carefully define security and privacy requirements* during the initial planning stage at the start of the systems development life cycle
- *determine the extent to which negotiated service agreements are required* to satisfy security requirements; and the alternatives of using negotiated service agreements or cloud computing deployment models which offer greater oversight and control over security and privacy
- *assess the extent to which the server and client-side computing environment* meets organizational security and privacy requirements
- *continue to maintain security management* practices, controls, and accountability over the privacy and security of data and applications

(a) *Risk Management.* The OMB tasked NIST with developing security guidance for cloud computing based upon NIST's six-step risk management framework, shown in Illustration V, below:[43]

Illustration V



(b) *Key Security and Privacy Issues.* Since the OMB's direction in February 2011, NIST has issued a series of special publications addressing cloud security. In December 2011, NIST published its "Guidelines on Security and Privacy in Public Cloud Computing."[44] In these guidelines, NIST identified a host of "key security and privacy issues" that the customers and cloud service providers need to address for cloud security. Issues include:[45]

(1) *Governance.* Cloud computing amplifies the need to address governance issues and security—in short, who is responsible for what in assuring adequate information security and privacy.

(2) *Compliance.* Parties must comply with laws, regulations, and policies (e.g., Federal Information Security Management Act of 2002, Privacy Act of 1974, Health Insurance Portability and Accountability Act, Federal Records Act, etc.) applicable to the data being moved to the cloud.

(3) *Data Location.* If the cloud moves data across national borders, the parties need to

address potential risks, such as e-discovery and international privacy requirements.

(4) *Trust.* The customer must gain a high level of trust in the cloud provider, given issues such as insider threats, data ownership rights, visibility into security practices, and risk management.

(5) *Architecture.* Cloud providers deploy a wide array of architecture (hypervisors, virtualization platforms, virtual machine images, etc.), each with different strengths and weaknesses in security that the customer should weigh in the security risk assessment.

(6) *Identity and Access Management.* Customers need to confirm what methods of identity and access management will be employed, given that certain technologies that work in a noncloud environment are not suitable for the cloud.

(7) *Data Protection.* Cloud security needs to recognize unique risks associated with data aggregation ("value concentration"), multi-user tenancy ("data isolation"), and duplicate imaging ("data sanitization").

(8) *Availability.* Given that data availability represents a core objective of security, the cloud parties must address risks of both temporary and prolonged outages.

(9) *Incident Response.* When a breach occurs, the customer and provider need a well-defined plan for who is responsible for what, when, and how.

(c) *Practical Security Recommendations.* In a more recent synopsis of its guidance on cloud security, NIST provided a list of practical recommendations for better protection in the cloud:[46]

(1) *Risk of Unintended Data Disclosure.* Encrypt sensitive data if the customer has both cloud services (with nonsensitive data) and noncloud services (sensitive data).

(2) *Data Privacy.* Address heightened privacy risks, given the legal and ethical risks in the event of a cloud breach.

(3) *System Integrity.* Consider any lack of visibility into the cloud provider's security mechanisms as part of the overall risk assessment and mitigation measures.

(4) *Multi-Tenancy.* Identify specific security safeguards (e.g., encryption and private clouds) to lessen risks associated with multi-tenancy.

(5) *Browsers.* Reduce risks of browsers being compromised by assessing available security controls (e.g., accessing clouds behind application gateway, restricting browser types, or limiting browser plug-ins).

(6) *Hardware Support for Trust.* Recognize that a virtualized Trust Platform Module (TPM) remains a technical challenge with no proven solution.

(7) *Key Management.* Work with the cloud provider to assure proper protection of consumer cryptographic keys.

Even in a shortened list format, this NIST synopsis reflects the level of complexity, the multitude of technical and management challenges, and the evolving technology confronting federal agencies and private sector entities that are embarking on the transition from traditional agency-specific IT systems managed by a single agency to multi-tenant cloud services outsourced to a cloud provider.

(d) *Continuous Monitoring.* As a key element of cloud security, the OMB and the GSA have underscored the need for continuous monitoring. The Federal Risk and Authorization Management Program (FedRAMP) highlighted continuous monitoring as a key part of the ongoing authorization process for cloud service providers (CSPs):[47]

> Ongoing assessment and authorization, often referred to as continuous monitoring, is the third and final process for cloud services in FedRAMP. Ongoing assessment and authorization is part of the overall risk management framework for information security and is a requirement for CSPs to maintain their Provisional Authorization. This process determines whether the set of deployed security controls in an information system remain effective in light of planned and unplanned changes that occur in the system and its environment over time.

Briefing Papers © 2012 by Thomson Reuters

Such monitoring requires the provider to identify threats and update security continuously, rather than on an annual basis. In its Concept of Operations, the GSA has broken the continuous monitoring process down into three steps—operational visibility, change control, and incident response—and provided diagrams for each function in the process.[48]

(e) *Security Implementation Challenges.* In reviewing the status of cloud implementation, the GAO identified a number of challenges. One area related to difficulties in finding cloud providers that could perform unique federal security requirements like continuous monitoring and system inventories:[49]

> *Meeting federal security requirements*: Cloud vendors may not be familiar with security requirements that are unique to government agencies, such as continuous monitoring and maintaining an inventory of systems. For example, [Department of] State officials described their ability to monitor their systems in real time, which they said cloud service providers were unable to match. Treasury officials also explained that the Federal Information Security Management Act's requirement of maintaining a physical inventory is challenging in a cloud environment because the agency does not have insight into the provider's infrastructure and assets.

In summary, no ready-made solutions exist for cloud security in the federal sector. Even the most recent NIST recommendations identify certain areas as uncharted territory. The OMB policies, NIST standards, and FedRAMP guidance offer valuable starting points for initiating the security process, but both federal customers and contractors face many decisions of first impression in pioneering the cloud in the public sector.

■ FedRAMP Security Authorization Process

The economies of scale represent one of the great potential advantages of the cloud. However, redoing the security accreditation and certification process for multiple agencies is not. To achieve the benefits of cloud computing in which a provider serves multiple agencies, the approval process needs greater consistency between agencies:[50]

> While the decisions to use cloud computing are made at the agency level by agency Chief Information Officers and Chief Information Security Officers, the potential benefits of cloud computing won't be fully realized if every agency independently reviews and certifies solutions. The current fragmented process—where agencies independently conduct certifications and accreditations on the same products—is redundant, and adds both time and cost to an already complex procurement process.

(a) *Approve Once and Use Often.* To relieve cloud providers of undergoing multiple security reviews by individual agencies, the OMB directed that a streamlined security process be developed:[51]

> To improve readiness for cloud computing, the Federal Government will facilitate an "approve once and use often" approach to streamline the approval process for cloud service providers. For instance, a government-wide risk and authorization program for IaaS solutions will allow agencies to rely on existing authorizations so only additional, agency-specific requirements will need to be authorized separately.

(b) *FedRAMP Overview.* In a December 2011 memo, the OMB formalized this "approve once and use often" approach by establishing the FedRAMP program.[52] FedRAMP has been summarized as follows:[53]

> FedRAMP will assist agencies to acquire, authorize and consume cloud services by adequately addressing security from a baseline perspective. FedRAMP will allow Federal agencies to coordinate assessment and authorization activities from the first step in authorizing cloud services to the ongoing assessment of the risk posture of a cloud service provider's environment. However, FISMA requires that Federal agencies authorize and accept the risk for placing Federal data in an IT system. Consistent with existing law, agencies will maintain this responsibility within FedRAMP. However, FedRAMP will standardize and streamline the processes agencies use to accomplish assessment and authorization activities, saving time and money.

(c) *FedRAMP Implementation Issues.* In its Concept of Operations, the GSA targeted June 2012 for initial operating capability of the FedRAMP program.[54] In the meantime, the GAO found that cloud certification and accreditation efforts have been a challenging process for agencies and contractors alike:[55]

> *Certifying and accrediting vendors:* Agencies may not have a mechanism for certifying that vendors meet standards for security, in part because

> the Federal Risk and Authorization Management Program (FedRAMP) had not yet reached initial operational capabilities [prior to June 2012]. For example, GSA officials stated that the process to certify Google to meet government standards for their migration to cloud-based e-mail was a challenge. They explained that, contrary to traditional computing solutions, agencies must certify an entire cloud vendor's infrastructure. In Google's case, it took GSA more than a year to certify more than 200 Google employees and the entire organization's infrastructure (including hundreds of thousands of servers) before GSA could use Google's service.

Future FedRAMP approvals for cloud providers will apparently continue to be arduous and time-consuming. According to the GSA's Federal Cloud Computing Initiative Program Management Office, "the goal is for two or three companies to undergo the FedRAMP process and receive approval from the board by year's end."[56]

Acquiring The Cloud In The Public Sector

The unique aspects of cloud services generally require federal agencies to consider very different approaches to IT acquisitions. Instead of buying IT products and services over which the agency has substantial control, cloud services change the business relationship in fundamental ways. In its policy statement in February 2011, the OMB recognized a need to streamline the acquisition process for acquiring cloud services.[57]

■ Overview Of Key Acquisition Issues

In February 2012, the CIO Council and Chief Acquisition Officers Council identified in a "Best Practices for Acquiring IT as a Service" guide the top 10 areas that procuring agencies need to address in the unique process of buying cloud services.[58] In its July 2012 report to Congress, the GAO summarized these areas as follows:[59]

- Selecting a cloud service—choosing the appropriate cloud service and deployment model.
- Cloud service provider and end-user agreements—terms of service, and service provider and end-user agreements need to be fully integrated into cloud contracts.
- Service-level agreements—agreements need to define performance with clear terms and definitions, demonstrate how performance is being measured, and identify why enforcement mechanisms are in place to ensure the conditions are met.
- Roles and responsibilities—cloud service provider, agency, and integrator roles and responsibilities should be clearly defined.
- Standards—NIST's cloud reference architecture should be used for cloud procurements.
- Security—requirements for the service provider to maintain the security and integrity of the agency data must be clearly defined.
- Privacy—privacy risks and responsibilities need to be addressed in the contract between federal agencies and service providers.
- E-discovery—service providers need to be aware of the need to locate, preserve, collect, process, review, and produce electronically stored information in the event of civil litigation or investigation.
- Freedom of Information Act (FOIA)—all relevant data must be available for appropriate handling under the act.
- E-records—agencies need to ensure that service providers understand the federal agencies obligations under the Federal Records Act.

For buying cloud services, the "Best Practices for Acquiring IT As a Service" guide provides specific guidance for incorporating essential security requirements into cloud contracts for the federal sector:[60]

> When Federal agencies consider implementing a cloud computing solution, there are seven key security areas they need to address: clear security authorization requirements, continuous monitoring, incident response, key escrow, forensics, two-factor authentication with [Homeland Security Presidential Directive] 12, and auditing.

For each of these seven areas, this "Best Practices" guide details the key security factors that acquisition professionals must weigh in the buying process.[61] To assist procuring agencies in addressing specific acquisition and security issues, this guide also incorporates an appendix with specific questions to be answered in cloud acquisitions. For example, the guide provides a checklist for cybersecurity issues shown in Illustration VI, below:[62]

Briefing Papers © 2012 by Thomson Reuters

Illustration VI

Cybersecurity Questions
1. Does the contract include provisions to meet all FedRAMP requirements?
2. If authentication and digital signature are required, is HSPD-12 required as the standard?
3. Does the contract address how FISMA, TIC, ISO 27001, NIST standards, and EINSTEIN are applied by cloud providers operating in a non-USG (commercial) environment?
4. What is the CSP's key escrow program for USG encrypted data and how are the terms and conditions of escrow applied to accessing encrypted USG data?
5. Is it clear that the agency's owns all network logs, archived data, or other information and access to this must not be restricted? [NOTE: logs are needed by Federal agencies conducting, for example, OIG investigations].
6. What requirements (clearances, etc.) apply to cloud providers' employees accessing USG data in a cloud environment?
7. What happens when material infringing on the intellectual property rights of the USG or others is located in a cloud system deployed by a cloud provider for the benefit of the USG? a. What level of indemnity and supporting insurance and/or capital will be provided by the cloud provider to the USG? b. What access to cloud provider intellectual property rights will the USG need to address various issues, particularly law enforcement investigations and audits?
8. What happens when USG data is stored or transported in non-bannered environments and devices, particularly if those environments also contain data not belonging to the USG?
9. What security guidelines apply to operations of various cloud components and how are they measured for compliance? (SA-1, CA-2, SA-4, SA-13)
10. Was there an assessment by the agency or cloud provider of how server and telephony locations may impact access and security of the data? (AC-1, AC-16, SA-4)

■ Key Acquisition Challenges In Buying Cloud Services

As discussed above, cloud computing brings bright prospects for a multiplicity of benefits to federal IT procurements: broader flexibility, faster technology upgrades, greater cost savings, and more. At the same time, recent GAO findings, agency procurements, and protest litigation predict some stormy weather and heavy fog ahead for cloud competitions and resulting contracts.

(a) *Organizational Conflicts of Interest.* The federal "Cloud First" policy has opened markets not only for cloud service providers, but also for contractors who perform third-party security assessments.[63] As part of the security review and approval process, the FedRAMP program specifically requires cloud service providers to undergo a third-party assessment by an accredited "Third-Party Assessment Organization" (3PAO).[64] In some cases, contractors may seek to be both cloud service providers and third-party assessors: "Under the FedRAMP rules, third-party assessment organizations can sell cloud services if they adequately wall off that portion of their business from the evaluation side."[65] However, such arrangements may pose potential organizational conflicts of interest if not properly mitigated. The FAR states:[66]

> Contracts for the evaluation of offers for products or services shall not be awarded to a contractor that will evaluate its own offers for products or services, or those of a competitor, without proper safeguards to ensure objectivity to protect the Government's interests.

When such OCIs cannot be mitigated, agencies and contractor-awardees alike have ended up on the losing side of protests.[67] Accordingly, agencies and contractors must tread carefully and address OCIs fully whenever a cloud service provider also seeks to provide third-party assessment services.

(b) *Follow-on Competition.* Inevitably, agencies must prepare for follow-on competitions after the award of contracts for cloud services, platforms, or infrastructure. However, in reviewing issues relating to cloud procurements, the GAO identified "data portability" for follow-on contracts as one of the acquisition challenges:[68]

> *Ensuring data portability and interoperability:* To preserve their ability to change vendors in the future, agencies may attempt to avoid platforms or technologies that "lock" customers into a particular product. For example, a Treasury official explained that it is challenging to separate from a vendor, in part due to a lack of visibility into the vendor's infrastructure and data.

In short, will the agency be perpetually stuck with the incumbent? If so, potential cloud competitors may have a viable protest under the Competition in Contracting Act.[69] As the GAO has stated, agencies "cannot take a passive approach and remain in a noncompetitive position where they could reasonably take steps to enhance competition."[70] Accordingly, agencies must be careful to build transition and exit strategies into the solicitation and resulting contract—and contractors must be alert to repetitive sole-source extensions of incumbent contracts.

(c) *Unduly Restrictive Security Provisions.* As discussed above, security remains a paramount concern for federal cloud acquisitions. In turn, this concern drives tougher security measures for cloud solicitations. While agencies have considerable discretion in choosing security requirements, unduly restrictive provisions may fail to pass muster under the Competition in Contracting Act and implementing regulations.[71] For example, the GAO upheld a protest where a solicitation for cloud computing services restricted competition to U.S. sources or Trade Agreements Act "designated countries":[72]

> We do not, however, conclude that GSA's explanations for the non-U.S. data center location requirements are otherwise reasonable, or withstand logical scrutiny. First, with regard to GSA's argument that the government has a need to know where U.S. government data resides and transits, this objective is accomplished by the requirement for vendors to identify the locations of their data centers. Second, while we appreciate the security concerns and legal ambiguities associated with subjecting U.S. government data to the jurisdictions of foreign countries, to the extent the solicitation allows for locating U.S. government data outside the United States, it is apparent that the limits drawn by GSA in this regard have been established in an arbitrary manner.
>
> …GSA has provided no explanation for why its security concerns would be less acute in relation to data stored or processed in designated countries, which include, for example, Yemen, Somalia, and Afghanistan, versus data stored or processed in non-designated countries, such as Brazil, India or South Africa.

In contrast, the GAO upheld the agency's requirement for a "Government Community Cloud" due to "the additional layer of security provided by a cloud limited to U.S. government entities."[73] As this case illustrates, agencies may impose reasonable security requirements, but must be able to explain why such requirements are not unduly restrictive of competition.

(d) *Evolving Standards and Needs.* Another acquisition challenge arises from the evolving standards and guidelines for competing, buying, and securing cloud services, infrastructure, and platforms. In its review of cloud acquisitions, the GAO highlighted the difficulties of conducting these procurements while still trying to define requirements:[74]

> *Obtaining guidance:* Existing federal guidance for using cloud services may be insufficient or incomplete. Agencies cited a number of areas where additional guidance is needed such as purchasing commodity IT and assessing Federal Information Security Management Act security levels.

Without a clear baseline for the cloud, bidders may be competing on different bases. To ensure competition on an equal basis, agencies must provide contractors with "a common basis for preparation and submission of proposals" and assure evenhanded evaluation of offers against common requirements and evaluation criteria.[75]

For cloud acquisitions, contractors need to apply particular care in reviewing and understanding the requirements not only because cloud acquisition guidance continues to evolve, but also due to the complexity in the allocation of risks and responsibilities relating to agency needs, security requirements, and other acquisition issues highlighted by the GAO, the OMB, NIST, and the Chief Acquisition Officers Council.

(e) *Undefined and Ambiguous Requirements.* The NIST definitions and GAO reports above illustrate that the cloud takes many forms, each with differing contractual responsibilities, risk profiles, and security issues for the parties. Such variety increases the likelihood of gaps, ambiguities, and conflicts in the solicitation requirements and resulting contract. For example, a recent Request for Proposals sought a wide range of cloud services (including storage, secure file transfer, virtual machine, database hosting, web hosting, and other services). This solicitation included the following statement: "Figure 2 Scope of Requirements and Related Service Delivery Models**,** below illustrates the scope of the [agency] hosting requirements and portfolio of service delivery/fulfillment models anticipated under this solicitation." That "Figure 2" provided:

Cloud Service Model	Cloud Deployment Model			
	Private	*Community*	*Public*	*Hybrid*
IaaS/PaaS				
SaaS				

Figure 2 Scope of Requirements and Related Service Delivery Models

While these blanks in the solicitation may increase flexibility for the offerors, they also magnify the risk that the offerors will propose apples-and-oranges and the agency will not get what it needs. In one cloud acquisition where the agency failed to provide a sufficient definition of "external network connection," the GAO found an ambiguity in the solicitation and sustained the protest.[76] The better the agency can define its cloud requirements fully and clearly, the greater the chance the agency will get what it sought—and the less chance that the GAO will sustain a protest where the offerors had differing interpretations of the RFP requirements.

Briefing Papers © 2012 by Thomson Reuters

★ GUIDELINES ★

These *Guidelines* are intended to assist you in understanding the standards, issues, and risks relating to cloud computing acquisitions and cybersecurity in the federal sector for agencies and contractors. They are not, however, a substitute for professional representation in any specific situation.

1. *Prepare for the cloud.* The cloud is coming and both agencies and contractors need to prepare for the paradigm shift in IT procurements driven by the federal "Cloud First" policy, the economies of scale, and global commercialization, all of which will bring new ways of buying IT and securing federal data and networks.

2. *Think commercial first.* The private sector is moving rapidly to implement the cloud, meaning that agencies need to plan for "Commercial Item First" and contractors should press for commercial terms to the maximum extent practicable to bring the greatest innovation and best value pricing to the federal sector.

3. *Define agency needs.* With so many cloud options, agencies must take extra care in defining contractual responsibilities, allocating risks, and identifying security needs for the selected cloud service and deployment models—and thus avoid offerors' misunderstandings leading to apples-and-oranges proposals and ensuing protests.

4. *Scrub the requirements.* With evolving standards and emerging practices, contractors need to be alert to ambiguities, inconsistencies, and gaps in cloud solicitations and requirements that may lead to competitive losses, protest grounds, or contract disputes due to missing what the agency really wanted.

5. *Build in security.* Given the federal consensus on information security as a paramount consideration in cloud acquisitions, review the security requirements closely, consult the OMB, NIST, and FedRAMP guidance, and assure that the security controls match the risk associated with the selected cloud model.

6. *Use the available guidance.* The available guidance (e.g., OMB, NIST, and FedRAMP) are not meant to be cookbooks telling agencies and contractors exactly how to structure each individual cloud solicitation and proposal, but they do provide valuable summaries of questions, issues, and risks that need to be addressed for such acquisitions.

7. *Anticipate transition/exit strategies.* Recognizing that as new cloud competitions may bring in new cloud service providers, agencies must incorporate robust plans for transition and exit ramps to handle the tasks of moving services and data securely and seamlessly from the incumbent to the follow-on contractor.

8. *Watch out for OCIs.* Contractors seeking to be both cloud service providers and third-party assessment entities should beware of potential OCIs, develop strong mitigation plans, and work closely with agencies to assure that sufficient safeguards are in place to mitigate or avoid OCI risks.

9. *Prepare for lessons learned.* With cloud computing in its early stages of implementation in the federal sector, agencies and contractors can expect both great successes and hard lessons learned—all of which should be captured, analyzed, and understood to make the next cloud acquisition a success.

★ REFERENCES ★

1/ See, e.g., NIST Special Publication 800-145, The NIST Definition of Cloud Computing (Sept. 2011); NIST Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing (Dec. 2011); NIST Special Publication 800-146, Cloud Computing Synopsis and Recommendations (May 2012). NIST Special Publications are available at http://csrc.nist.gov/publications/PubsSPs.html.

2/ NIST Special Publication 800-145, The NIST Definition of Cloud Computing 2 (Sept. 2011).

3/ NIST Special Publication 800-145, The NIST Definition of Cloud Computing 2–3 (Sept. 2011).

4/ Cloud Computing: Benefits and Risks of Moving Federal IT Into the Cloud: Hearings Before the Subcomm. on Government Management, Organization, and Procurement of the H. Comm. on Oversight and Government Reform, 111th Cong. 15 (July 1, 2010) (statement of Vivek Kundra, Federal CIO), http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg58350/pdf/CHRG-111hhrg58350.pdf; GAO, Information

Technology Reform: Progress Made But Future Cloud Computing Efforts Should Be Better Planned 3 (GAO-12-756, July 11, 2012); Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators: Hearings Before Subcomm. on Intellectual Property, Competition, and the Internet of the H. Comm. on the Judiciary, 112th Cong. 10, 36–37 (July 25, 2012) (statements of Robert W. Holleyman, Business Software Alliance, and Daniel Castro, Information Technology and Innovation Foundation), http://judiciary.house.gov/hearings/Hearings%202012/hear_07252012_2.html.

5/ Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators: Hearings Before Subcomm. on Intellectual Property, Competition, and the Internet of the H. Comm. on the Judiciary, 112th Cong. 37 (July 25, 2012) (statement of Daniel Castro, Information Technology and Innovation Foundation), http://judiciary.house.gov/hearings/Hearings%202012/hear_07252012_2.html; Cloud Computing: Benefits and Risks of Moving Federal IT Into the Cloud: Hearings Before the Subcomm. on Government Management, Organization, and Procurement of the H. Comm. on Oversight and Government Reform, 111th Cong. 11 (July 1, 2010) (statement of Vivek Kundra, Federal CIO), http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg58350/pdf/CHRG-111hhrg58350.pdf.

6/ NIST Special Publication 800-145, The NIST Definition of Cloud Computing 2 (Sept. 2011) (footnote omitted); see also Cloud Computing: Benefits and Risks of Moving Federal IT Into the Cloud: Hearings Before the Subcomm. on Government Management, Organization, and Procurement of the H. Comm. on Oversight and Government Reform, 111th Cong. 21 (July 1, 2010) (statement of Vivek Kundra, Federal CIO), http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg58350/pdf/CHRG-111hhrg58350.pdf.

7/ GAO, Information Security: Federal Guidance Needed To Address Control Issues With Implementing Cloud Computing 14 (GAO-10-513, May 27, 2010).

8/ GAO, Cybersecurity: Challenges in Securing the Electricity Grid 1 (GAO-12-926T, July 17, 2012).

9/ NIST Special Publication 800-145, The NIST Definition of Cloud Computing 2–3 (Sept. 2011) (footnotes omitted).

10/ GAO, Information Security: Federal Guidance Needed To Address Control Issues With Implementing Cloud Computing 12 (GAO-10-513, May 27, 2010).

11/ Cloud Computing: Benefits and Risks of Moving Federal IT Into the Cloud: Hearings Before the Subcomm. on Government Management, Organization, and Procurement of the H. Comm. on Oversight and Government Reform, 111th Cong. 87 (July 1, 2010) (statement of Scott Charney, Microsoft VP for Trustworthy Computing), http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg58350/pdf/CHRG-111hhrg58350.pdf.

12/ NIST Special Publication 800-145, The NIST Definition of Cloud Computing 3 (Sept. 2011).

13/ GAO, Information Security: Federal Guidance Needed To Address Control Issues With Implementing Cloud Computing 13 (GAO-10-513, May 27, 2010).

14/ Cloud Computing: Benefits and Risks of Moving Federal IT Into the Cloud: Hearings Before the Subcomm. on Government Management, Organization, and Procurement of the H. Comm. on Oversight and Government Reform, 111th Cong. 19 (July 1, 2010) (statement of Vivek Kundra, Federal CIO), http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg58350/pdf/CHRG-111hhrg58350.pdf.

15/ GAO, Information Security: Federal Guidance Needed To Address Control Issues With Implementing Cloud Computing 15 (GAO-10-513, May 27, 2010).

16/ Cloud Computing: Benefits and Risks of Moving Federal IT Into the Cloud: Hearings Before the Subcomm. on Government Management, Organization, and Procurement of the H. Comm. on Oversight and Government Reform, 111th Cong. 10 (July 1, 2010) (statement of Vivek Kundra, Federal CIO), http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg58350/pdf/CHRG-111hhrg58350.pdf.

17/ Innovating With Less: Examining Efforts To Reform Information Technology Spending: Hearings Before the Subcomm. on Federal Financial Management, Government Information, Federal Services, and International Security of the S. Comm. on Homeland Security and Governmental Affairs, 112th Cong. (May 24, 2012) (statement of Sen. Brown), http://www.hsgac.senate.gov/subcommittees/federal-financial-management/hearings/innovating-with-less-examining-efforts-to-reform-information-technology-spending-.

Briefing Papers © 2012 by Thomson Reuters

18/ OMB, Federal Information Technology Shared Services Strategy 3 (May 2, 2012), https://cio.gov/wp-content/uploads/downloads/2012/09/Shared_Services_Strategy.pdf.

19/ See, e.g., GAO, Information Technology Reform: Progress Made; More Needs To Be Done To Complete Actions and Measure Results 2 (GAO-12-745T , May 24, 2012).

20/ Cloud Computing: Benefits and Risks of Moving Federal IT Into the Cloud: Hearings Before the Subcomm. on Government Management, Organization, and Procurement of the H. Comm. on Oversight and Government Reform, 111th Cong. 2 (July 1, 2010) (statement of Rep. Towns), http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg58350/pdf/CHRG-111hhrg58350.pdf.

21/ See, e.g., OMB, Federal Information Technology Shared Services Strategy 3 (May 2, 2012), https://cio.gov/wp-content/uploads/downloads/2012/09/Shared_Services_Strategy.pdf; GAO, Information Technology Reform: Progress Made But Future Cloud Computing Efforts Should Be Better Planned 1 (GAO-12-756, July 11, 2012).

22/ Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators: Hearings Before Subcomm. on Intellectual Property, Competition, and the Internet of the H. Comm. on the Judiciary, 112th Cong. (July 25, 2012) (statement of Dan Chenok, IBM) (emphasis in original), http://judiciary.house.gov/hearings/Hearings%202012/hear_07252012_2.html; see also Cloud Computing: Benefits and Risks of Moving Federal IT Into the Cloud: Hearings Before the Subcomm. on Government Management, Organization, and Procurement of the H. Comm. on Oversight and Government Reform, 111th Cong. 76–77 (July 1, 2010) (statement of Rep. Watson), http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg58350/pdf/CHRG-111hhrg58350.pdf; Cloud Computing: Benefits and Risks of Moving Federal IT Into the Cloud: Hearings Before the Subcomm. on Government Management, Organization, and Procurement of the H. Comm. on Oversight and Government Reform, 111th Cong. 113 (July 1, 2010) (statement of Mike Bradshaw, Google) ("Brookings Institution found that government agencies that switched to some form of cloud computing saw up to 50 percent savings."), http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg58350/pdf/CHRG-111hhrg58350.pdf.

23/ Innovating With Less: Examining Efforts To Reform Information Technology Spending: Hearings Before the Subcomm. on Federal Financial Management, Government Information, Federal Services, and International Security of the S. Comm. on Homeland Security and Governmental Affairs, 112th Cong. (May 24, 2012) (statement of George DelPrete, TechAmerica), http://www.hsgac.senate.gov/subcommittees/federal-financial-management/hearings/innovating-with-less-examining-efforts-to-reform-information-technology-spending-.

24/ Innovating With Less: Examining Efforts To Reform Information Technology Spending: Hearings Before the Subcomm. on Federal Financial Management, Government Information, Federal Services, and International Security of the S. Comm. on Homeland Security and Governmental Affairs, 112th Cong. (May 24, 2012) (statement of Steven VanRoekel, Federal CIO), http://www.hsgac.senate.gov/subcommittees/federal-financial-management/hearings/innovating-with-less-examining-efforts-to-reform-information-technology-spending-; see also OMB, Federal Information Technology Shared Services Strategy 3 (May 2, 2012), https://cio.gov/wp-content/uploads/downloads/2012/09/Shared_Services_Strategy.pdf.

25/ Innovating With Less: Examining Efforts To Reform Information Technology Spending: Hearings Before the Subcomm. on Federal Financial Management, Government Information, Federal Services, and International Security of the S. Comm. on Homeland Security and Governmental Affairs, 112th Cong. (May 24, 2012) (statements of Sen. Carper and Steven VanRoekel, Federal CIO), http://www.hsgac.senate.gov/subcommittees/federal-financial-management/hearings/innovating-with-less-examining-efforts-to-reform-information-technology-spending-.

26/ OMB, Federal Information Technology Shared Services Strategy 12 (May 2, 2012), (quoting OMB, Federal Cloud Computing Strategy (Feb. 8, 2011)), https://cio.gov/wp-content/uploads/downloads/2012/09/Shared_Services_Strategy.pdf; see also GAO, Information Technology Reform: Progress Made But Future Cloud Computing Efforts Should Be Better Planned 1 (GAO-12-756, July 11, 2012) (citing OMB cloud strategy).

27/ OMB, Federal Information Technology Shared Services Strategy 16 (May 2, 2012), https://cio.gov/wp-content/uploads/downloads/2012/09/Shared_Services_Strategy.pdf.

28/ Innovating With Less: Examining Efforts To Reform Information Technology Spending: Hearings Before the Subcomm. on Federal Financial Management, Government Information, Federal Services, and International Security of the S. Comm. on Homeland Security and Governmental Affairs, 112th Cong. (May 24, 2012) (statement of Steven VanRoekel, Federal CIO), http://www.hsgac.senate.gov/subcommittees/federal-financial-management/hearings/innovating-with-less-examining-efforts-to-reform-information-technology-spending-; see also GAO, Information Technology Reform: Progress Made; More Needs To Be Done To Complete Actions and Measure Results 11 (GAO-12-745T, May 24, 2012).

29/ GAO, Information Technology Reform: Progress Made But Future Cloud Computing Efforts Should Be Better Planned 7 (GAO-12-756, July 11, 2012).

30/ Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators: Hearings Before Subcomm. on Intellectual Property, Competition, and the Internet of the H. Comm. on the Judiciary, 112th Cong. 38 (July 25, 2012) (statement of Daniel Castro, Information Technology and Innovation Foundation) (footnotes omitted), http://judiciary.house.gov/hearings/Hearings%202012/hear_07252012_2.html.

31/ Cloud Computing: An Overview of the Technology and the Issues Facing American Innovators: Hearings Before Subcomm. on Intellectual Property, Competition, and the Internet of the H. Comm. on the Judiciary, 112th Cong. 42–43 (July 25, 2012) (statement of Daniel Castro, Information Technology and Innovation Foundation), http://judiciary.house.gov/hearings/Hearings%202012/hear_07252012_2.html.

32/ Federal Acquisition Streamlining Act of 1994, Pub. L. No. 103-355, §§ 8104(a), 8203, 108 Stat. 3243 (1994) (codified at 10 U.S.C.A. § 2377(b); 41 U.S.C.A. § 3307(c)).

33/ 10 U.S.C.A. § 2377(b); 41 U.S.C.A. § 3307(c); see also FAR 12.101.

34/ Cloud Computing: Benefits and Risks of Moving Federal IT Into the Cloud: Hearings Before the Subcomm. on Government Management, Organization, and Procurement of the H. Comm. on Oversight and Government Reform, 111th Cong. 32 (July 1, 2010) (statement of David McClure, GSA Associate Administrator, Office of Citizen Services and Innovative Technologies), http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg58350/pdf/CHRG-111hhrg58350.pdf.

35/ Cloud Computing: Benefits and Risks of Moving Federal IT Into the Cloud: Hearings Before the Subcomm. on Government Management, Organization, and Procurement of the H. Comm. on Oversight and Government Reform, 111th Cong. 2 (July 1, 2010) (statement of Rep. Towns), http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg58350/pdf/CHRG-111hhrg58350.pdf; see also Cloud Computing: Benefits and Risks of Moving Federal IT Into the Cloud: Hearings Before the Subcomm. on Government Management, Organization, and Procurement of the H. Comm. on Oversight and Government Reform, 111th Cong. 8 (July 1, 2010) (statement of Rep. Issa), http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg58350/pdf/CHRG-111hhrg58350.pdf; Cloud Computing: What are the Security Implications: Hearings Before the Subcomm. on Cybersecurity, Infrastructure Protection, and Security Technologies of H. Comm. on Homeland Security, 112th Cong. (Oct. 6, 2011) (video statement of Rep. Lungren (Congress cannot ignore potential cybersecurity risks of cloud services), http://homeland.house.gov/hearing/cloud-computing-what-are-security-implications.

36/ GAO, Information Technology Reform: Progress Made But Future Cloud Computing Efforts Should Be Better Planned (GAO-12-756, July 11, 2012).

37/ Censer, "Keeping the Cloud Secure," Wash. Post, May 7, 2012 (quoting Dr. David L. McClure, GSA Associate Administrator, Office of Citizen Services and Innovative Technologies), http://www.washingtonpost.com/business/capitalbusiness/gsa-readies-fedramp-to-improve-cloud-security/2012/05/04/gIQAinEK6T_story.html.

38/ GAO, Information Security: Additional Guidance Needed To Address Cloud Computing Concerns (GAO-12-130T, Oct. 6, 2011).

39/ Privacy Rights Clearinghouse, Data Breaches: A Year in Review: The Top Half Dozen Most Significant Data Breaches in 2011 (Apr. 16, 2012) (emphasis in original), http://www.privacyrights.org/print/top-data-breach-list-2011.

40/ GAO, Information Security: Federal Guidance Needed To Address Control Issues With Implementing Cloud Computing 3 (May 27, 2010, GAO-10-513).

Briefing Papers © 2012 by Thomson Reuters

41/ OMB, Federal Cloud Computing Strategy 26 (Feb. 8, 2011) (emphasis added), https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf.

42/ OMB, Federal Cloud Computing Strategy 28 (Feb. 8, 2011) (emphasis in original) https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf.

43/ See OMB, Federal Cloud Computing Strategy 26–27 (Feb. 8, 2011) (citing NIST Special Publication 800-37, Rev. 1 (Feb. 2010)), https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf.

44/ NIST Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing, (Dec. 2011).

45/ NIST Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing 14–35 (Dec. 2011).

46/ NIST Special Publication 800-146, Cloud Computing Synopsis and Recommendations § 8 (May 2012).

47/ GSA FedRAMP, Concept of Operations (CONOPS), Version 1.0, at 37 (Feb. 7, 2012), http://www.gsa.gov/graphics/staffoffices/FedRAMP_CONOPS.pdf.

48/ GSA FedRAMP, Concept of Operations (CONOPS), Version 1.0, at 37–40 (Feb. 7, 2012), http://www.gsa.gov/graphics/staffoffices/FedRAMP_CONOPS.pdf.

49/ GAO, Information Technology Reform: Progress Made But Future Cloud Computing Efforts Should Be Better Planned 18 (GAO-12-756, July 11, 2012).

50/ Cloud Computing: Benefits and Risks of Moving Federal IT Into the Cloud: Hearings Before the Subcomm. on Government Management, Organization, and Procurement of the H. Comm. on Oversight and Government Reform, 111th Cong. 19 (July 1, 2010) (statement of Vivek Kundra, Federal CIO), http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg58350/pdf/CHRG-111hhrg58350.pdf.

51/ OMB, Federal Cloud Computing Strategy 28 (Feb. 8, 2011), https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf.

52/ OMB, Memorandum for Chief Information Officers, Security Authorization of Information Systems in Cloud Computing Environments (Dec. 8, 2011), https://cio.gov/wp-content/uploads/2012/09/fedrampmemo.pdf; GAO, Information Technology Reform: Progress Made But Future Cloud Computing Efforts Should Be Better Planned 7 (GAO-12-756, July 11, 2012) (describing background of FedRAMP program).

53/ CIO Council and Chief Acquisition Officers Council, Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT As a Service 12 (Feb. 24, 2012), https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf.

54/ GSA FedRAMP, Concept of Operations (CONOPS), Version 1.0, at 3 (Feb. 7, 2012), http://www.gsa.gov/graphics/staffoffices/FedRAMP_CONOPS.pdf.

55/ GAO, Information Technology Reform: Progress Made But Future Cloud Computing Efforts Should Be Better Planned 19 (GAO-12-756, July 11, 2012) (footnote omitted).

56/ Blake Johnson, "Small GSA Office at Forefront of Government's Cloud Adoption," Fed. Times, June 2012, http://www.federaltimes.com/article/20120622/IT03/306220001/Small-GSA-office-forefront-government-8217-s-cloud-adoption.

57/ OMB, Federal Cloud Computing Strategy 28 (Feb. 8, 2011), https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf.

58/ CIO Council and Chief Acquisition Officers Council, Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT As a Service 12 (Feb. 24, 2012), https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf.

59/ GAO, Information Technology Reform: Progress Made But Future Cloud Computing Efforts Should Be Better Planned 9–10

(GAO-12-756, July 11, 2012) (citing CIO Council and Chief Acquisition Officers Council, Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT As a Service (Feb. 24, 2012), https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf)).

60/ CIO Council and Chief Acquisition Officers Council, Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT As a Service 12 (Feb. 24, 2012), https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf.

61/ CIO Council and Chief Acquisition Officers Council, Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT As a Service 12–16 (Feb. 24, 2012), https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf.

62/ CIO Council and Chief Acquisition Officers Council, Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT As a Service 39, app. A (Feb. 24, 2012), https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf.

63/ Censer, "Companies Show Interest in Being Assessors for Federal IT Buying Program," Wash. Post, July 2, 2012, at A10.

64/ GSA FedRAMP, Concept of Operations (CONOPS), Version 1.0, at 19 (Feb. 7, 2012), http://www.gsa.gov/graphics/staffoffices/FedRAMP_CONOPS.pdf; GSA FedRAMP website, Third Party Assessment Organizations (3PAO), http://www.gsa.gov/portal/content/117675.

65/ Censer, "Companies Show Interest in Being Assessors for Federal IT Buying Program," Wash. Post, July 2, 2012, at A10; see also GSA FedRAMP, Concept of Operations (CONOPS), Version 1.0, at 19 (Feb. 7, 2012) (FedRAMP requirements for "independence"), http://www.gsa.gov/graphics/staffoffices/FedRAMP_CONOPS.pdf.

66/ FAR 9.505-3; see Gould, Inc., Comp. Gen. Dec. B-181488, 74-2 CPD ¶ 205 (agency found OCI where contractor manufacturing torpedoes sought to perform test and evaluation on these same torpedoes).

67/ See, e.g., Aetna Gov't Health Plans, Inc., Comp. Gen. Dec. B-254397.15, 95-2 CPD ¶ 129, at 12–13 (sustaining protest where an employee of the awardee's proposed subcontractor also assisted with the agency's price evaluation).

68/ GAO, Information Technology Reform: Progress Made But Future Cloud Computing Efforts Should Be Better Planned 19 (GAO-12-756, July 11, 2012).

69/ 10 U.S.C.A. § 2304(c); 41 U.S.C.A. § 3304; see also FAR 6.301(c).

70/ eFedBudget Corp., Comp. Gen. Dec. B-298627, 2006 CPD ¶ 159, at 7 (sustaining protest where agency had no record of taking affirmative steps to promote competition by resolving issue relating to restricted access to software source code); see also Test Systems Assocs., Inc., Comp. Gen. Dec. B-244007.2, 91-2 CPD ¶ 367, at 7 n.8 (sustaining protest where agency "has had a duty to take practicable steps to avoid a noncompetitive follow-on contract," but failed to do so).

71/ See, e.g., 10 U.S.C.A. § 2305(a)(1)(A); 41 U.S.C.A. § 3306(a)(1)(A) (requiring agencies to specify needs in way "designed to achieve full and open competition"); see FAR 11.002(a).

72/ Technosource Information Sys., LLC, Comp. Gen. Dec. B-405296 et al., 2011 CPD ¶ 220, at 6–7 (footnote omitted).

73/ Technosource Information Sys., LLC, Comp. Gen. Dec. B-405296 et al., 2011 CPD ¶ 220, at 10–11.

74/ GAO, Information Technology Reform: Progress Made But Future Cloud Computing Efforts Should Be Better Planned 18–19 (GAO-12-756, July 11, 2012) (emphasis in original).

75/ Parmatic Filter Corp., Comp. Gen. Dec. B-285288, 2000 CPD ¶ 185, at 5; see also MVM, Inc. v. United States, 46 Fed. Cl. 126, 134 (2000) ("The only way to ensure adequate competition is to have bidders compete on an equal basis.").

76/ Technosource Information Sys., LLC, Comp. Gen. Dec. B-405296 et al., 2011 CPD ¶ 220, at 12–13.

Briefing Papers © 2012 by Thomson Reuters