LJN LAW JOURNAL NEWSLETTERS

The Corporate Counselor®

An ALM Publication

Volume 25, Number 6 • October 2010

Government Contracts and the Cloud

The Data Security Challenge

By Michael L. Whitener

The Obama Administration is rapidly fulfilling its pledge to leap into cloud computing with both feet.

First there was the Cloud Computing Initiative, announced last September as a means of slashing the federal government's IT costs as well as reaping the scaleability and flexibility benefits of hosted IT services delivered over the Web. Then there was the mandate contained in the 2011 federal budget that all federal agencies evaluate cloud-computing alternatives in connection with any budget requests for IT investments. Most recently, the U.S. General Services Administration issued a long-anticipated request for quotations from the private sector to provide infrastructure as a service (IaaS) to federal agencies.

Meanwhile Vivek Kundra, the Federal Chief Information Officer appointed by the President last year, has been criss-crossing the country extolling the virtues of cloud computing and the economic gains that it offers to the public sector. Cloud computing, Kundra argues, "offers transformational opportunity to fundamentally reshape how the government operates, engages the public and delivers services." Kundra's report on the "State of Public Sector Cloud Computing," issued earlier this year, describes how agencies across the government have already begun shifting to the cloud.

The task, and promise, of reshaping federal IT services to fit a cloud environment is undoubtedly huge. The U.S. government is the world's largest purchaser of information technology, spending over $76 billion annually on more than 10,000 different IT systems. The result has been, in Kundra's words, a "fragmented and inefficient" infrastructure. Private-sector IT companies are lining up to assist the federal government with evaluating competing cloud technologies as well as positioning themselves to provide cloud infrastructure and services.

Fly in the Ointment

If there's a fly in the ointment of these ambitious plans, however, it's concern about data security.

The primacy of that concern became obvious when the GSA issued its IaaS solicitation, only to yank it a few months later and return to the drawing board. The GSA emerged with a new solicitation requiring much more stringent data security safeguards. Congress is also keeping a watchful eye. The House Committee on Oversight and Government Reform has begun holding hearings on the "potential and unknown security risks associated with cloud computing across the federal agency community."

To mitigate data security worries, there is a major federal push to accelerate the development of cloud-computing standards for the public sector, led by the National Institute of Standards and Technology (NIST). However, given the time-consuming process of consensus-building in Washington, adoption of formal standards is hardly just around the corner. To help fill the gap, a Federal Risk and Authorization Management Program (FedRAMP) has been launched to assess the security worthiness of specific cloud service offerings. Once FedRAMP approves a cloud service for a specific federal agency, it will be made available to all federal agencies, allowing an evolutionary adoption of new cloud technologies.

Reading the Tea Leaves

With the federal government drive into cloud computing clearly underway, legal counsel advising IT companies that are government contractors, or are looking for opportunities to do business with the government, should aim to anticipate the data security measures that the government will insist upon as a condition for implementing new cloud technologies. Winning companies in the public-sector cloud-computing stakes will be those that read the tea leaves early, have a good grasp of the government's data security

Michael Whitener is a principal in the Washington, D.C. office of VistaLaw International LLC (www.vistalaw.com), a global legal services firm. Michael's clients include a number of software companies and cloud computing service providers. He is the author of *Creating Software Alliances* and a contributing editor to *Softletter* newsletter. Michael can be reached at mwhitener@vistalaw.com.

requirements, and have solutions ready to satisfy those requirements.

In the absence of formal standards for public-sector cloud computing, that might appear to be a daunting prospect. Fortunately, the GSA's recent IaaS solicitation provides a very revealing "sneak peak" into the federal government's evolving standards for data security. The aim of that solicitation was to enable available, convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications and services). The GSA's expectation is that these resources can be rapidly provisioned and released with minimal management effort or service provider interaction, thus creating a more agile federal enterprise.

The GSA proposal took a "kitchen-sink" approach to data security, requiring compliance with three federal laws (the Federal Information Security Management Act, the Information Technology Management Reform Act and the Privacy Act) as well as nine different GSA security policies and more than a dozen other federal security directives, memoranda and guides. While the task of satisfying such an array of data security requirements may appear dizzying, by parsing through the requirements and finding common threads, a fairly clear picture of what the government will be demanding in terms of data security in the cloud emerges.

The Four Pillars of Federal Data Security

Each government solicitation for cloud-computing services will be different, depending upon the technology involved and the sensitivity of the data to be protected. Nevertheless, it can be reasonably expected that there will be certain consistent requirements across all such solicitations. Based upon the recent GSA solicitation, there are four areas of focus that vendors proposing cloud computing solutions will be expected to address: 1) assessment and authorization; 2) reporting and monitoring; 3) certification; and 4) audit. Each of these areas is discussed briefly below.

Assessment and Authorization

Every implementation of a new federal government IT system requires a formal approval process known as "Assessment and Authorization," and cloud-computing systems are no exception. Given the fact that government data will be residing outside federal firewalls, it's not surprising that the assessment and authorization process for applications in the cloud will be especially rigorous.

The vendor will be expected to provide documentation regarding its system security plan, contingency plan (including disaster recovery plan) and independent penetration test report, all completed in accordance with relevant NIST and GSA guidelines. The level of security required will vary, depending upon whether the application is deemed low impact, medium impact or high impact. (In the case of the GSA proposal for IaaS services, the determination was medium impact.)

During the assessment phase, the government will be looking in particular to see what security controls are provided in the following areas:

- Physical security. In what sort of facility does the data center reside? What authentication and access controls are in place? What physical audit trails are maintained? What sort of surveillance technology is provided?
- Operational security. How is administrative access to client systems logged in and reviewed? What are the vendor's patch management and security policy auditing procedures? What compliance reports are available showing each hosted server's security settings?
- Network security. Is client data intermingled or isolated from other client data? What firewall and intrusion prevention systems are in place? What additional intrusion detection services and intrusion prevention services are available? What data encryption options are offered?

During the authorization phase, the government will determine whether it is satisfied that the vendor meets the government's security requirements and will render an authorization decision to: 1) authorize system operation without any restrictions or limitations; 2) authorize system operation with restrictions; or 3) not authorize for operation.

Reporting and Monitoring

Government contractors providing cloud computing services will face a heavy ongoing reporting and monitoring burden, to allow the government to keep tabs on possible security risks and take action to protect government data as warranted.

Vendors will be expected to provide specific data security reports on a quarterly, annual and biannual schedule. For instance, required quarterly deliverables include updates on plans of action and milestones as well as vulnerability scan reports. Annual deliverables number more than a dozen, including updated system security and contingency plans, data security awareness and training records, system configuration settings and incident response test reports. Biannual deliverables include policies and procedures regarding access control, identification and authentication, system maintenance and personnel security.

Certification

Specific data security certifications are not necessarily required for participation in the federal cloud computing arena. However, certification is an explicit evaluation criterion when assessing the skills and knowledge of an organization and its personnel with regard to data security of information systems (*see, e.g.*, NIST Special Publication 800-53, Revision

2, "Recommended Security Controls for Federal Information Systems").

In the data security world, two audit standards or certifications have emerged as the preeminent benchmarks.

First is the Statement on Auditing Standards No. 70 (SAS 70), developed by the American Institute of Certified Public Accountants. Not strictly a "certification," SAS 70 is actually an auditing framework that focuses on the design of a service organization's security controls. The resulting audit report can be provided to the service provider's customers as evidence of the rigor of its data security measures.

There are two types of SAS 70 audits. A Type I audit addresses the design of controls, while the more stringent Type II audit also evaluates the effectiveness of those controls. Note that SAS 70 audits are conducted against a standard set by the company's own control objectives and supporting control activities, as reflected in a SAS 70 report prepared by the company, rather than an externally imposed set of criteria. So an SAS 70 audit is only as impressive as the SAS 70 report on which it is based.

Second is ISO 27001 certification. Compared with the SAS 70 audit, the ISO 27001 certification focuses specifically on an organization's overall security program rather than the existence or effectiveness of specific controls. It requires a specific framework for managing and controlling information security risks, including documentation, completion of a risk assessment and development of a risk treatment plan. The certification is valid for three years following successful completion of the initial audit, with follow-up surveillance visits conducted annually.

Audit

Companies providing cloud services to the federal government must be prepared to allow an extensive, and perhaps uncomfortable, level of government intrusion into the organization's inner workings. Even with the heavy security documentation and reporting obligations described above, the government's approach to data security is, "trust, but verify."

The government's tool for verification is the audit. The government must be granted the right to perform manual or automated audits, scans, reviews and other inspections of the vendor's IT environment being used to provide or facilitate services for the government.

Specifically, the vendor must provide both logical and physical access to the vendor's facilities, installations, operations, documentation, records and databases within 72 hours of the government's request, to allow the government to conduct an inspection for any threats to the security, integrity or confidentiality of government data. Automated audits may include vulnerability scans of the vendor's operating system/network, Web applications and database applications. In some instances the government may be willing to accept the vendor's own automated scans or audits, but only after the scanning tools and their configuration have been approved by the government.

The Mapping Challenge

"Mapping" in the data security context refers to the process of establishing clear links between the multitude of federal regulations, directives, policies and standards that determine data security benchmarks and the vendors own data security documentation, policies, procedures and technology. In evaluating vendor solutions, the government will expect these linkages to be made explicit; the government will not do the heavy lifting of mapping itself.

Legal counsel can play an especially important role in the mapping process if they are able to straddle the divide between federal data security requirements on the one hand and their client's technological and procedural responses on the other. They should naturally be in the best position to understand the legal and regulatory backdrop to data security mandates, but may have to stretch outside their comfort zone in order to obtain sufficient understanding of IT systems to "connect the dots" between government security requirements and what their client can provide.

Conclusion

The migration of federal IT services to the cloud offers a huge and potentially lucrative but still evolving opportunity for nimble technology companies to provide their services to the federal government via cloud solutions. But this opportunity comes with strings attached in the way of tight data integrity and security controls, as well as heavy reporting burdens and the obligation to give the government the right to conduct intrusive audits. Such is the price of admission — not surprisingly, given the potential adverse consequences of a data rupture or leak involving sensitive government information. Companies that, with the assistance of their legal counsel, anticipate and are prepared to offer data security measures that meet the federal government's stringent requirements will be a step ahead of the pack.

—❖—