Cloud Computing Contracting Concerns

The following is the product of the cloud computing working group operating under the auspices of the IT Investigations Subcommittee of the CIGIE IT Committee. Charles Coe, Chair of the IT Investigations sub-committee initiated a cloud computing work group with volunteer membership from several federal agencies. The member of this group were Craig Goscha, USDA OIG, craig.goscha@oig.usda.gov; Earl Baker, NASA OIG, Earl.E.Baker@jpl.nasa.gov; Sabrina Segal, USITC OIG, Sabrina.Segal@usitc.gov; and Lisa Bergman, ED OIG, Lisa.Bergman@ed.gov.

Cloud Computing Contracting: Important questions to ask and concerns to address

Cloud computing is a completely different animal when applied to the Federal government as opposed to its existence in the private sector. The private sector does not have the wide variety of regulations, restrictions, and concerns that face the Federal government daily. As such, this section of the memorandum will address important questions to ask and concerns that agencies will need to address prior to jumping head first into cloud computing. Addressing all of these areas will help ensure that an agency is entering into this new area of technology with its "eyes wide open" and that decision makers are not only aware of the benefits of cloud computing, including cost savings and portability, but also the risks, including greater liability for leakage of data and loss of public trust.

Overarching Questions:

The following are a sampling of essential questions that must be asked and satisfactorily answered prior to entering into a cloud computing contract. There are many wrong answers to these questions and very few right ones. For example, agencies must ask:

- Who has access to the data, both in its live state and when backups are made?
- How is the data handled?
- What is the computing environment?
- What are the geographic boundaries? Where are the servers located and how will this impact the access and security of the data?
- What are the security guidelines?
- How are upgrades and maintenance handled?
- Can the vendor access or use the information in aggregate?
- How do we cancel the contract and migrate the information?
- How are data and media destroyed?

Because the government standards for most, if not all, of these questions are higher than the private sector, cloud computing vendor answers may not always be sufficient. The whole concept of economies of scale that underpin the value in a cloud environment may be unraveled at the first question because the vendor may not be able to provide the

agency with an "out of the box" solution and must, instead, customize a cloud environment which almost always results in price increases.

Government in the Cloud Concerns:
There are seven areas which raise major concerns that a government agency must be actively aware of before entering into a cloud computing contract. Agencies should insist on clear and satisfactory answers to all of these areas before moving their data into the cloud in order to prevent incurable actions such as breaches of systems or leaks of information. This is one area where, as they say, the toothpaste cannot be put back into the tube.

1. **Data Security**
   Agencies must be vigilant about data security and this area must be their number one concern. Agencies must insist on satisfactory incident response. Incident response is the vendor's reaction to breaches of systems, leaks of data, and access to data. The remedies presented by vendors must be adequate and vendors should not be able to contract away their liability for data security. Applying FISMA, TIC, ISSO 27001 standards, and running EINSTEIN is practically and realistically impossible and is essentially a non-starter for most vendors.

   Presently, cloud vendors take ownership of their "containers" but not the data that is placed into those containers. If their containers spring a leak because they have been negligent in applying patches, monitoring their systems, or even by brute force then the owners of the data in those containers are responsible for cleaning up the mess. The cloud providers have clean hands and agencies can be left with the responsibility and the potentially astronomical real and perceived cost of providing credit monitoring, contacting the subjects of the data, and answering to the public regarding the poor security posture. This outcome puts the agency in a no-win-situation, leaving it to explain why the breach occurred even though there was no first-hand way to prevent it or for that matter to even know that the breach occurred. Vendors must be required to indemnify the government should a breach occur.

   Cloud providers must be held accountable for ensuring service availability and held accountable for incident responsiveness in cases of data security. Among other things, agencies should know how long a vendor will wait to let them know their data has been compromised, how the vendor plans on re-securing the system, and how long the system will remain off-line.

   Cloud providers must also be able to provide agencies with a list of the locations of all of their servers where government information could potentially be housed and, depending on the sensitivity of the information, ensure that only properly cleared or approved individuals will have access to those servers.

Finally, a less urgent but equally as important aspect of data security is the disposal of government data. The agency must confirm that the data will not remain the property of the vendor and that the vendor will properly destroy the data and dispose of any hardware that contained government data.

2. Access to Information

Agencies must also take into consideration the amount of access they wish to retain to the network over which their information and data is traveling. For example, in a normal network configuration, the CIO can conduct active network monitoring simply by placing a network monitoring tool on the system and reviewing the results. Since the agency controls the network, no additional permissions or approvals are necessary other than those required by policy. This is an advantage to agency components such as the Inspector General or Office of Security and the access often permits these entities to build a case and take administrative or other action when necessary.

In a cloud environment, the agency no longer owns the network and access to real time monitoring may be difficult, or even impossible, depending on the level of access the vendor will agree to and whether additional approvals such as warrants for wiretapping are deemed necessary. This could present an insurmountable challenge for agencies trying to investigate or discipline employees who are misusing or committing crimes using government resources. However, real time monitoring is not the only access challenge agencies could face. They may also have restricted access to network logs, archived data, or other information that is not readily available as part of the cloud service.

3. Regulatory Compliance

As stated above, the Federal government has many additional and different concerns than the private sector and cloud vendors may flat out not agree or charge an additional amount to comply with the regulatory structure surrounding government data. Some of the more clear-cut regulations with which the government must apply are the Privacy Act, FISMA, and the Federal Records Act. The landscape becomes much more complex when we move from those regulations into those governing classified information, law enforcement and intelligence data, and security regulations (as discussed above). But, even if we remain in the land of simple rules and regulations, what happens if there is a classified leak? For example, what is the government's and vendor's response if someone inadvertently attaches a classified document to an unclassified email that is hosted in the cloud? What personnel will have access to "clean up" those machines? What will happen to the physical machines? Will the government have to pay for what is destroyed during the clean up? What will happen to the non-government information that is comingled on those machines? Will there be an additional cost to the government?

A similar question which needs to be addressed and will be answered in more detail in a subsequent section of this memo is how to ensure Inspector General access to the data for investigation and auditing needs without incurring additional cost or delay.

Concerns that must be addressed for all levels of information, though, include the requirement and enforceability of non-disclosure agreements for vendor personnel, the timeliness of the vendor's response when complying with agency or public requests for access, and the treatment of non-public information such as procurement, pre-decisional policy, physical security, etc. The determination of whether the data remains non-public may hinge on the vendor's access, handling, and compliance with data regulations.

4. Termination & Transition

As briefly mentioned in the Data Security section above, agencies must be sensitive to termination and transition language in cloud computing agreements and must ensure that their data is properly protected, conveyed, and destroyed at the end of a cloud contract.

It is extremely important to address termination with a cloud computing vendor since they may not be as sensitized to the data regulations as described above which continue even after the government moves on to another provider. Some vendors will have standard language that states they retain the information for a certain amount of time after the contract ends or that they have no obligation to provide the information in a format that will allow for transition to a new provider.

Transition is equally as important to address since agencies will not want to find themselves essentially default into a sole source contract simply because the vendor will not provide the data in a format for conveyance or will do so but at an astronomical cost. The latter option is highly likely since transition of data is not typically addressed in out-of-the-box cloud solutions.

5. Asset Availability

Availability, compatibility, software updates, and hardware refresh must also be addressed in any government cloud computing contract. The agreement must clearly state the estimated outage time the vendor foresees for standard hardware and software updates and the vendor's estimated response time should an emergency take the system off line. Usually, there is an opportunity here for an agency to negotiate a cost reduction if the system is off line for a particular amount of time or the outage impairs the agency's ability to work.

The agreement must include a discussion of the hardware and software the agency is currently using and the vendor's assurance that their system is compatible. There must also be language describing the process for ensuring compatibility should the vendor migrate to software or hardware that is not compatible with the agency's configuration and address cost impacts this could present.

Additionally, software updates (including security patching) and hardware refresh will need to be addressed and clear responsibilities will need to be outlined. If applicable, FISMA Certification and Accreditation requirements should be addressed here as well since a review is triggered when any significant changes are made to the system. Agencies need to confirm that these areas are addressed to their satisfaction or else they could face liability and exponential cost increases when faced with situations that were not contemplated ahead of time.

6. **Maintenance**

Similar to the availability discussion above, any cloud computing agreement must have a section addressing patching and version control. Typically, the vendor will be responsible for this activity but the agency must ensure that there is language in the agreement specifically requiring the vendor to take on this responsibility. Further, version control is important, not only to ensure proper patching, but for compatibility with agency systems (see the compatibility discussion above).

7. **Pricing and Time**

The purpose of many of these sections is not only to address any and all aspects of an agency's presence in the cloud but to also avoid unexpected cost overruns and additional charges for actions or responses that the agency didn't address ahead of time. There will be standard pricing for out-of-the-box cloud solutions but, when the government requirements are added, the price may not be as competitive as the present in-sourced solution. Agencies need to be aware of any and all additional costs either stated up front or presented as contingencies should other actions be taken by the vendor.

In addition to pricing, the contract should address any time requirements that the vendor will need to meet in order to comply with government rules and regulations. Everything from FISMA to FOIA to IG investigations and audits have time requirements and cloud vendors should be expected to comply with these requirements at no additional cost. If an additional cost is presented then the agency will need to factor that in to the overall price analysis when determining whether to move into the cloud.

8. **IP**

Intellectual Property must also be addressed in the cloud agreement in order to protect the government and set boundaries for the vendor. Language in the agreement should address how infringing material will be handled if located and the level of indemnity that will be provided by the vendor or the government. Further, access to vendor IP will need to be addressed, particularly in the case of IG investigations and audits. If the IG needs access to the system and that access also includes access to proprietary algorithms or business practices, the government must be sure that those limitations will not compromise its ability to conduct a thorough investigation.

All in all there are many areas where an agency needs to be well educated and aware before it jumps into the cloud head first. Often, managers will present the cloud as a fiscal solution for budgets that are often too small to begin with. A CIO may believe that moving to the cloud will reduce the cost of hosting an email system from $300,000 to $30,000 and that will be the only motivation. It's important that decision makers are presented with all the facts – risks and rewards – before a final decision is made. Otherwise, agencies could end up paying much more in the end, in dollars and integrity, than they are saving.