UNC SCHOOL OF GOVERNMENT

Cloud Computing: Contracting Considerations for Inclusion

Pricing:

The contract should include specific price caps to eliminate ballooning costs after the initial investment. For example, a fee increase cap of 3% is commonly used in such contracts, along with a provision to ensure that if the service is offered to other customers at a lower cost, the government will receive that lowest cost pricing. Note: Monitoring the pricing will be incumbent on the government and can be facilitated through regular review of government contracts with the cloud provider, as well as communication among peer governments. Review of pricing for non-governmental entities will be difficult.

Data Assurances:

1. Ownership: The contract should clearly state that the government owns all data residing within the cloud environment. Typically, the contract language will include rights to government data ownership related to issues such as intellectual property as well as disallow accessing the data for corporate gain by the cloud provider or organizations other than the government.

2. Access to Data: The contract should mandate that the government be able to access and retrieve its data stored in the cloud at its sole discretion. The government should have the right to access all data, regardless of who created the content and for what purpose, in order to ensure that individual governmental employees cannot prevent access to data that would have traditionally resided on governmental servers, etc. Furthermore, the contract should specify how the data will be retrieved from the cloud in the event of an emergency or time-sensitive situation, with specific procedures and timelines noted. In all cases involving data access and retrieval requests, the contract should specify the process by which the government will validate the request, including positions within the government authorized to make such a request and to whom within the cloud provider.

3. Disposition of Data Upon Request: The contract should provide a mechanism for the government to require the cloud provider to destroy specified records as requested. The purpose of this mechanism is to allow the government to destroy records when allowed by law (i.e. according to the retention schedule) and not have additional copies of the records residing in other locations, such as the cloud, then making the records subject to disclosure upon public records requests or in the event of litigation.

4. Disposition of Data Upon Contract Termination: The contract should provide clear instructions on how government data will be returned or retrieved in the event of contract termination. It is important to include the timeframe for such provision of all data, the process, and the exact format of the data. It is important to note that most cloud services involve proprietary or non-standard formats of data, which upon exporting to the government, would render it useless. Therefore, the contract should specific a common format for data return/retrieval, such as XML. The contract should also include specifications requiring the vendor to destroy all government data after contract termination, along with the government's right to conduct an audit to ensure the data has been destroyed.

Shannon H. Tufts
tufts@sog.unc.edu

5. Data Breaches: The contract should specify the cloud vendor's obligations in the event of data breach or unauthorized access. It is important to include reporting/notification requirements related to the breach within a specified timeline, as well as details about the breach such as its nature, the data compromised, the involved parties, mitigation efforts, and corrective actions to be taken by the vendor. The contract should also specify indemnification in the event of the breach, as the data breach relates to specific legal, regulatory, and operating agreement provisions. In other words, the cloud provider should be responsible for all damages, fines, etc. including litigation costs related to a breach. Many cloud providers avoid putting this type of language in their contracts, which makes the government liable for costs associated with breaches.

6. Data Storage Location: The legal system cannot keep pace with technology and, currently, most courts are holding that the legal jurisdiction over a contract dispute involving data takes place in the state where the data physically resides. North Carolina has a law (G.S. 22B-3) which voids contract provisions that require disputes under the contract to be litigated outside of the state, but it is important to consider the inclusion of statements about the physical storage location of government data (particularly requiring the data to remain within the United States).

7. Legal Data Holds/Public Record Requests: The contract should include provisions related to litigation holds on data (also called litigation cooperation clause). First, the contract should specify the communication process for informing either the cloud provider or the government of any legal requests (including public records requests), as well as mechanisms to ensure that the data is preserved in its entirety during the duration of the litigation. A legal hold also requires maintaining any media that was used for backup of the data which must be available for searching. Furthermore, the contract should specify that the cloud provider will not provide data to individuals, groups, or organizations making records requests unless directed to do so by an authorized government official. The contract should also include a provision indicated the process by which the data requested will be reviewed and potentially redacted or removed from provision by authorized government officials, in order to ensure compliance with NC General Statutes.

Right to Audit and Inspect:

There are multiple audit formats to be specified in the contract.

1. The government has the right to request third-party audits and/or certifications related to infrastructure and security, including penetration testing and vulnerability assessments. In addition, any reports produced from these audits and certifications will be provided to the government for review.
2. The government (or a third-party provider selected by the government) has a right to perform an onsite inspection of the cloud vendor's infrastructure and security practices on a specified basis.
3. The government has the right to review the infrastructure and security specifications in written format if it so chooses.
4. The government should have a right to audit the performance records of the cloud provider, as well as access to daily and weekly service quality statistics.

Shannon H. Tufts
tufts@sog.unc.edu

UNC SCHOOL OF GOVERNMENT

Service Level Agreements:

The contract should specify service level parameters, minimum levels, and specific remedies and penalties for non-compliance with SLAs. Always include 1) Uptime, 2) Performance and response time, 3) Error correction time, and 4) Infrastructure and security. Ensure that the SLA clearly defines the pertinent terms, such as downtime, scheduled downtime, etc. These definitions eliminate ambiguity in contract enforcement, as well as provide specific mechanisms for calculating compliance with the SLA.

Remediation/Penalties:

Remedies for violation of the SLA should include corrections and/or penalties. Both corrections and penalties should be specific (such as "Service credit will be rendered when SLA is not met by XX Vendor. The service credit will be applied as liquidated damages against the following quarter of service costs." It is important to document how the credit will be provided and when it will be provided. Ideally, the financial penalty should be 10-20 percent of the contract, per Gartner, in order to motivate the vendor to avoid violations. These penalties should be related to SLA performance, while fines and costs associated with data breaches should be covered under the Data Assurances section of the contract.

Disaster Recovery/Business Continuity

The contract should specify minimum disaster recovery and business continuity requirements and ensure that the cloud provider meets the minimums through inspection of documentation, etc. Furthermore, the contract should specify penalties for failures in complying with the minimum requirements, as discovered through onsite inspections, audits, or actual disasters.

Outsourced Services

The contract should require the vendor to inform the government of any outsourced functionality and its provider. The contract should also require the cloud vendor with whom with contract is signed to remain directly responsible for all terms of the contract, regardless of outsourced functions. The contract should also specify that no assignment of the contract or components of the contract can occur without explicit, written agreement from the government.

Termination

The contract should state that the government can terminate the contract "at any time without having to show cause and without additional fees or penalties." The contract should require the cloud provider to provide advance notice at a set time, e.g., 60 days before service discontinuation. As previously noted, the contract should specify how data will be retrieved/returned upon termination by either party. Escrow language should also be considered in the event of a cloud vendor going out of business.

Shannon H. Tufts
tufts@sog.unc.edu