The Software Alliance

BSA

March 24, 2017

Marcelo Daniel Pagotti
Information Technology Secretary
Ministry of Planning, Development, and Management
Setor de Edifícios Públicos Norte, Bloco D - 1º andar
Quadra 516 - Asa Norte
Brasília - DF - CEP: 70770-524

Re: Public Consultation – Public Procurement of Cloud Computing Services Draft Guidelines

Dear Mr. Secretary,

BSA | The Software Alliance ("BSA")[1] is thankful for the opportunity to offer comments on the Public Procurement of Cloud Computing Services Draft Guidelines ("Draft Guidelines") consultation. As the leading advocate for the global software industry, BSA is greatly interested in contributing to

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, IBM, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro and Workday.

initiatives that seek to advance cloud computing adoption by governments around the globe.

We believe that a policy environment that enables businesses, consumers and governments to leverage the full benefits of cloud computing is the key to driving the digital economy. We observe that the countries with the most favorable policies for cloud computing are those which prioritize free movement of data across borders, respect for international standards, protection of privacy and intellectual property, and robust enforcement and deterrence of cybercrime. We also find that many countries recognize that coordination of national cloud computing policies, both internally and with those of other nations, will facilitate benefits for all countries participating in the global economy.

Government procurement is a related and extremely relevant aspect for the development of cloud computing. Traditional purchasing practices and contract terms may hinder the scalable, cost-effective, and innovative nature of cloud computing. Quick and flexible procurement processes that are not hampered by burdensome terms and conditions will allow users to fully leverage the vast array of benefits offered by cloud computing technologies.

BSA and its members have extensive experience working with governments and other stakeholders around the world on policies that promote cloud computing adoption. We share these views hoping to assist your efforts to implement a set of cloud computing procurement guidelines that will further advance the adoption of cloud computing by the Government of Brazil greatly benefiting the country.

Data and Infrastructure Location:

The Draft Guidelines[2] do not allow data to be stored or mirrored/copied outside of Brazil. In addition, the Draft Guidelines require[3] cloud service providers to use infrastructure located in Brazil. These requirements would defeat two goals the Draft Guidelines seeks to achieve: improving security and increasing cost-effectiveness in cloud public procurement.

Requiring cloud service providers to confine data and data centers in Brazil could prevent them from enhancing security by backing up data in multiple locations, thus decreasing security. Data security is ultimately not dependent on the physical location of the data or the location of the infrastructure supporting it. Security is instead a function of the quality and effectiveness of the mechanisms and controls maintained to protect the data in question. Companies consider many factors when deciding where to locate digital infrastructure such as servers and gateways, including maximizing Internet speed and access, implementing redundancy and backup capabilities, and ensuring the deployment state of the art security for user data. Requiring localization of servers in Brazil will undercut such decisions and would jeopardize security instead of increasing it.

In addition, requiring data centers to be located in Brazil would increase the costs of services as global supply chain operations could not be leveraged.

Furthermore, applying a “one size fits all” approach to all government cloud purchases covered by the Draft Guidelines and prohibiting data from being stored or even replicated outside Brazil is not the best strategy. Instead, a risk-level approach that focus on the intended use of the service being procured should be taken into consideration for the purposes of this regulation.

For example, national security-related data and information on bird migration patterns linked to research efforts undertaken by universities are very

[2] See Article 18.2.3, Reference Terms

[3] See Article 1.1.2.1, Annex II

different in terms of their sensitivity levels and, thus, should not be subject to the same stringent data localization requirements.   In very narrow instances – for example, in the case of national security data that requires being separated from the global network with separate security protocols – it may make sense to require that certain types of data remain in Brazil. However, this requirement should not be the default but rather a very narrowly crafted exception. A broad requirement to keep all data from all entities that will need to comply with the Guidelines (including but not limited to the universities per the example above) would not generate any benefits.

Therefore, BSA recommends that the server and data localization requirements set forth by Articles 18.2.3 of the Reference Terms and Article 1.1.2.1 of the Annex II be remove and issues pertaining to highly sensitive data be addressed on a case by case basis through contract.

Encryption

Section 1.1.3 of Annex II of the Draft Guidelines requires that, in all instances, data be encrypted in transit and in rest.

While BSA strongly agrees that encryption is a powerful tool to protect information in transit and at rest and its use should be encouraged, it should not be mandated in all instances. Security protections should be tailored to the sensitivity of the data being collected and its potential risk profile. Encryption should not be the only method considered as far as information security is considered either. Companies that provide cloud services must also ensure they are securing data and operation of their infrastructure using the best available technologies.

Furthermore, the Draft Guidelines should not prohibit or require the acquisition or deployment of specific products or technologies, including specific encryption methods.

Cloud service providers seek to protect a wide spectrum of targets against a wide variety of potential threats. Policies targeted at increasing information security should enable the implementation of security measures that are most appropriate to mitigating the specific risks each company faces to increase effectiveness. Technology neutrality is important to ensure this objective is achieved.

BSA recommends Section 1.1.3 be modified to strongly encourage the use of encryption when appropriate rather than mandating it.

Procurement Preferences

Promoting the procurement of the best available products or services regardless of the nationality of the provider or of where the technology is developed ensure cost savings and increases cybersecurity. Procurement decisions should be made based on whether a product or service best meets the needs of the contracting agency and provides good value for money. The larger the number of vendors participating in government bids on equal footing, the better the chances that prices will be lower and products more secure.

Although the Draft Guidelines do not prohibit the participation of foreign providers in public procurement of the covered cloud offerings, references to preferences for local products and services, as well as to technology developed in Brazil, may limit government access to state-of-the art products, increase costs, and compromise cybersecurity.

We strongly urge the government of Brazil to re-consider its procurement preference policies and that Article 12.4.8 be removed from the draft.

Customer Services Call Center Location

Section 17.1 of the Draft Guidelines require cloud service providers to offer customer services thought the telephone, in Portuguese, from a call center located in Brazil.

The physical location of the call center will not impact the quality of the services rendered. Allowing the cloud service provider to offer these services from the location that best fits its business model will prevent unnecessary costs increases that compliance with this requirement could create.

We recommend this provision be modified to allow these services to be provide in Portuguese from any location.

We hope you find the information provided above useful to your efforts. We look forward to continue participating in this important discussion and stand ready to answer any questions you may have.

Sincerely,

Antonio Eduardo Mendes da Silva
Country Manager - Brasil