November 21, 2017

Mr. Otávio Ribeiro Damaso
Director
Financial Systems Regulation Department
*Via e-mail: denor@bcb.gov.br*

Re.: Comments on the Brazilian Central Bank´s Proposed Regulation on Cybersecurity Policies and the Procurement of Data Processing, Data Storage, and Other Cloud Computing Services – Public Consultation 57/2017

Dear Director Otávio Ribeiro Damaso,

**I – Introduction:**

BSA | The Software Alliance[1] is thankful for the opportunity to offer comments on the Brazilian Central Bank´s Proposed Regulation on Cybersecurity Policy and on the Procurement of Data Processing, Data Storage, and Other Cloud Computing Services – Public Consultation 57/2017 (hereinafter "Proposed Regulation"). As the leading advocate for the global software industry, BSA is greatly interested in contributing to initiatives that seek to advance cloud computing adoption around the globe.

In our view, a regulatory environment that enables businesses, consumers and governments to leverage the full benefits of cloud computing is the key to driving the digital

[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, DocuSign, IBM, Microsoft, Oracle, Salesforce, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro and Workday.

economy. Reaping those benefits requires policies and regulations for cloud computing that permit free movement of data across borders, avoid data localization requirements, rely on international technical standards, protect privacy and intellectual property, and include robust enforcement and deterrence of cybercrime.

BSA and its members have extensive experience working with regulators and other stakeholders around the world on policies related to cloud computing. We share the views below to assist your efforts to implement a regulation that will meet the underlying regulatory objectives in a manner that also improves the ability of financial and other institutions regulated by the Brazilian Central Bank to use cloud technologies to their benefit and, ultimately, to the benefit of Brazilian citizens.

We commend the Brazilian Central Bank for including references in the Proposed Regulation that would promote a risk based approach to cybersecurity. We are concerned, however, about the rule that would prohibit financial institutions and other institutions regulated by the Brazilian Central Bank from using cloud computing services from providers that store or process information outside Brazil. For the reasons explained below, this mandate would not improve the Brazilian Central Bank's access to information, it would not enhance its performance of its regulatory duties nor would it increase cybersecurity.

We also suggest improvements on a few other Proposed Regulation sections.

**II - The Brazilian Central Bank's Ability to Perform its Regulatory Duties Does Not Require Data and Infrastructure Localization**

We understand that one of the goals of the Proposed Regulation is to ensure that the Brazilian Central Bank has access to information it needs to perform its regulatory duties. We agree that this is an important objective. The proposed prohibition on using services that store or otherwise process information abroad would not, however, advance this goal.

The data and infrastructure localization rules set forth in Article 11, as well some of the contractual requirements for the provision of cloud services set forth in Article 12 are unnecessary, overly restrictive and will make it difficult for Brazilian financial institutions to use the most current and advanced technology. Specifically, Article 11 requires that financial institutions may only use Cloud Service providers if the financial institution's data is hosted in Brazil. Article 12 prescribes, in part, that the Brazilian Central Bank will have direct audit rights and direct access to the financial institution's data. Neither Article 11 nor the sections of Article 12 giving the Brazilian Central Bank rights to direct physical access to cloud provider facilities are necessary to ensure its regulatory authority or to promote security.

Article 9 of the Proposed Regulation already requires that (i) that the Brazilian Central Bank's regulated entities "adopt practices of corporate governance and management in proportion to the relevance of the service to be hired and the risks to which they are exposed"; and (ii) that the regulated entities ensure their contracts with cloud computing and data storage vendors provide that the regulated entities have access to and the ability to retrieve their data and that the confidentiality and integrity of such data is maintained, regardless of where the information is stored or otherwise processed. Moreover, Article 9 also provides that financial institutions should ensure they have the ability to audit the cloud service or data storage provider.

If the guidelines set forth in Article 9 are followed, then the Brazilian Central Bank will have the same degree of control as if the financial institutions were hosting the data themselves. The Brazilian Central Bank has jurisdiction over the regulated entity and can, with these contractual obligations in place, require the regulated entity to provide the data (regardless of where it is stored). It is irrelevant whether the data is stored in Brazil, outside Brazil, with the regulated entity or with a third party. Therefore, the data and infrastructure location will not prevent the Brazilian Central Bank from legally obtaining the data of a regulated institution.

Finally, Article 12, VIII requires data backup copies be stored in Brazil. For the reasons above mentioned, the location the information is kept is irrelevant for the purpose of access or security. This provision, therefore, should be modified to allow data backup copies be stored anywhere, subject to the contractual requirements discussed above.

Other central banks and financial regulators who have considered this issue have concluded that data residency requirements are unnecessary--in part because they provide very little in the way of added benefits, but also because they inhibit competition and the choice of technology that may be best suited to the financial institutions' needs. By requiring that data is hosted within Brazil, the Brazilian Central Bank will eliminate many data storage and cloud service providers from those available to its regulated entities. Even where a particular provider may have hosting facilities in Brazil, it is likely that some of the functionality it can provide will require that data is stored outside of Brazil because of how platforms are configured. It is simply not practical for providers to have all of their services and functionality available in every country. Part of the cost savings and efficiencies that cloud service providers are able to offer result from economies of scale which may require data be stored outside Brazil.

**Recommendations**:

- BSA urges the Brazilian Central Bank to reconsider the prohibition to procure services from providers that store or otherwise process information outside Brazil and remove Article 11 from the Proposed Regulation.
- BSA also recommends the removal of the aforementioned sections of Article 12, as unnecessary and harmful to Brazilian interests as explained above.
    - These changes will not affect the Brazilian Central Bank's ability to access data.

**III - Data and Infrastructure Location Restrictions Weaken Cybersecurity**

One of the stated goals of the Proposed Regulation is to improve cybersecurity practices adopted by financial and other institutions regulated by the Brazilian Central Bank.

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. The data localization and contractual requirements of Article 11 and Article 12 would prevent regulated institutions from enhancing security by backing up data in multiple locations that are in different regions. Therefore, requiring localization of servers in puts data at risk.

Moreover, many cloud computing service providers with excellent security do not have data centers in Brazil. Data residency requirements would exclude those providers and prevent Brazilian financial institutions from using solutions that offer strong security.

**Recommendation**:

- BSA urges the data localization requirement set forth by the Proposed Regulation be eliminated. Article 11 and Article 19 should, therefore be removed.

**IV - Use of Licensed Software and Software Asset Management Practices**

One practice the Brazilian Central Bank should consider recommending to the institutions it regulates to increase cybersecurity is the use of licensed software and software asset management practices based on international standards.

The use of unlicensed software exposes enterprises to heightened risks of malware infections and other security vulnerabilities. Indeed, a study by IDC[2] identified a strong correlation (0.79) between the presence of unlicensed software and the incidence of malware encounters. Because unlicensed software is less likely to receive critical security updates that would otherwise mitigate the risks associated with malware exposure, its use heightens the risk of harmful cybersecurity incidents.

Unfortunately, the use of software that is not properly licensed is still a significant problem. According to the most recent data, the rate of unlicensed software use in Brazil is 47 percent[3]. In many cases, the use of unlicensed software is simply a function of organizations lacking awareness of the software assets resident on their systems. Most organizations do not have adequate policies for managing software licenses.

Transparent and verifiable software asset management (SAM) practices identify situations where entities are using unlicensed software, as well as situation where the licenses they have far exceed the number of users. Under-licensing creates legal liability and security risks, while over licensing creates inefficiencies and unnecessary costs.

All institutions regulated by the Brazilian Central Bank should adopt SAM practices based on international standards, which can increase efficiencies while improving cybersecurity.

**Recommendation**:

- The Brazilian Central Bank should consider requiring the use of SAM best practices based on international standards as part of its proposed regulation.

****

BSA appreciates the opportunity to participate in this public consultation process. We look forward to continuing this important dialogue and we stand ready to answer any questions you may have.

---

[2] IDC White Paper, *Unlicensed Software and Cybersecurity Threats (2015)*, available at http://globalstudy.bsa.org/2013/cyberthreat.html

[3] Data on the rates on unlicensed software use and commercial values are taken from the 2016 BSA Global Software Survey at http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf . This study assesses the rates of unlicensed software use and the commercial value of unlicensed software installed on personal computers during 2015 in more than 100 markets. The study includes a detailed discussion of the methodology used.

Sincerely,

Antonio Eduardo Mendes da Silva
Country Manager - Brasil

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org