July 14, 2017

Major José Garcia da Luz
General Coordinator, Information Security and Communications Management
Institutional Security Secretariat, Office of the President

Re: Comments on the National Information Security Policy Draft Bill

Major José Garcia da Luz,

BSA | The Software Alliance (BSA)[1] welcomes the opportunity to offer comments on the National Information Security Policy Draft Bill (Draft Bill). BSA members have a deep and long-standing commitment to protecting their customers' data across technologies and business models. We, therefore, commend the Office of the President Institutional Security Secretariat's (GSI) for its efforts to promote information security in Brazil.

BSA supports cybersecurity strategies that are risk-based, technology neutral, and flexible. We also support policies that foster education and awareness about cybersecurity risks. In addition, given that cyber threats are global, effective cybersecurity policies and strategies need to maintain an international outlook as no country or

[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.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro and Workday.

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

government can address cybersecurity risk in isolation. Collaboration with non-governmental entities, including private sector, as well as with international partners and allies is a crucial component of an effective approach to cybersecurity. We are encouraged to see that many of these elements reflected in the Draft Bill.

Although the Draft Bill contains many positive elements, we strongly suggest additional factors be considered to ensure robust cybersecurity policies are in place in Brazil. BSA and its members have extensive experience working with governments and other stakeholders around the world on policies that promote strong cybersecurity policies and we share the views below to assist GSI in its efforts to achieve this goal.

Personal Data Protection

The Personal Data Protection Bill discussion, which is currently being held in the Brazilian Congress, is an opportunity to approach data protection in a holistic and effective way. Data privacy policy, including the definition of personal data, will be better addressed through the Personal Data Protection Bill governed by civilian institutions, consistent with international best practice.

We are concerned that, by defining personal data, the Draft Bill may create contradictory obligations and/or legal uncertainty. We urge the Draft Bill refer to the Personal Data Protection Bill for the definition of personal data.

Recommendation:

- We urge Article 3, IV be modified to say that personal data will be addressed in specific legislation (Personal Data Protection Bill).

Standards

Technology standards play a vital role in enabling and enhancing cybersecurity. The Draft Law should promote the use of global, voluntary standards developed through a multi-stakeholder processes. Local, Government-mandated standards rather than improving security tend to freeze innovation and force consumers to use products that might not suit their needs. In addition, requiring companies use national and unique standards prevents countries from leveraging the benefits provided by the use the best available technologies designed to respond to the latest threats, thus increasing exposure to cyber-attacks.

In addition, it would be important to establish a common set of minimum security baselines across government and critical infrastructures to prevent duplication and drive harmonization and consistency in requirements.

Recommendation:

- The Draft Law should be amended to include the use of global, voluntary standards developed through a multi-stakeholder processes as one of the principles that apply to the law itself, as well as future implementing regulation with the goal of increasing cybersecurity.
- The Draft Law should also determine that in the future a common set of minimum security baselines across government and critical infrastructures be estalished. We strongly recommend that Brazil follow the United States National Institute of Standards and Technology (NIST) Cybersecurity Framework for that purpose[2].

Use of Licensed Software and Software Asset Management Practices

The use of unlicensed software exposes enterprises and government agencies to heightened risks of malware infections and other security vulnerabilities. Indeed, a study by IDC identified a strong correlation (0.79)[3] 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, including by government agencies, is still a significant problem. According to the most recent data, the rate of unlicensed software use in Brazil is 47 percent.[4]

In many cases, the use of unlicensed software is simply a function of government agencies lacking awareness of the software assets resident on their systems. Most agencies do not have adequate policies for managing software licenses.

---

[2] The NIST Cybersecurity Framework has been developed through a genuine multi-stakeholder process and it references globally recognized standards for cybersecurity. The NIST framework has earned tremendous legitimacy among policymakers and throughout industry globally. Canada, Japan, and Australia are among others the countries that have used the NIST Cybersecurity Framework to help develop their own cybersecurity policies. The NIST Cybersecurity Framework is available in English at https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

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

[4] 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.

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. Federal Agencies should lead by example and adopt SAM practices based on international standards for their own procurement and software asset management, which can send a powerful example to private enterprises in Brazil while increasing efficiencies.

GSI can play a leading role in addressing this issue by requiring Federal agencies ensure that they only use properly licensed software and that they maintain appropriate SAM practices based on international best practices. This will help improve cybersecurity.

Recommendations:

- GSI should promote efforts to ensure the use of properly licensed software by Federal Agencies.
- GSI should require the use of robust SAM practices based on international best practices to ensure software license compliance, to reduce costs, and increase security.

Additional Recommendations:

BSA also strongly recommends that GSI or another Agency designated by GSI:

- coordinate the identification of private-sector recommended voluntary outcome-based cybersecurity practices with critical infrastructure operators, private sector entities, relevant government departments, institutions of higher education, and appropriate non-governmental cybersecurity experts;
- establish an incentives-based cybersecurity program for critical infrastructure to encourage adoption of voluntary outcome-based cybersecurity practices;
- develop procedures to inform critical infrastructure owners and operators of cyber threats, vulnerabilities, and consequences.

We would like to once again thank you for the opportunity to offer this initial set of comments. that we hope will contribute to creating a robust cybersecurity framework in Brazil. 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
Brazil Country Manager

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

P 202-872-5500
W bsa.org