October 2, 2019

Colonel Arthur Pereira Sabbat
Director of the Department of Information and Communication Security (DSIC)
Institutional Security Secretariat, Office of the Presidency

Re: Comments on the Proposed National Cybersecurity Strategy

Dear Colonel Arthur Pereira Sabbat

BSA | The Software Alliance (BSA)[1] welcomes the opportunity to offer comments on the Proposed National Cybersecurity Strategy (Proposed Strategy). 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 strengthen cybersecurity in Brazil.

The Proposed Strategy contains many positive elements. We particularly commend GSI for its focus on strengthening collaboration between stakeholders across society in a manner that promotes innovation, flexibility, and international engagement. In addition, we offer some general recommendations applicable throughout the strategy, as well as some recommendations specific to individual strategic actions, which we believe are important to ensuring robust, effective 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

[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, Akamai, Apple, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens PLM Software, Sitecore, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

cybersecurity policies and we share the views below to assist GSI in its efforts to achieve this goal.

General Recommendations:

BSA recommends that the Proposed Strategy make it clear that future cybersecurity policies be based on all the following six overarching principles:

1 - Policies Should Be Aligned with Internationally Recognized Technical Standards. Internationally recognized technical standards provide widely vetted, consensus-based frameworks for defining and implementing effective approaches to cybersecurity, and facilitate common approaches to common challenges, thus enabling collaboration and interoperability. This alignment is particularly important with regard to the strategy's prioritization of protecting National Critical Infrastructures; internationally recognized technical standards and guidance, as outlined in the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Technical Report 27103, can ensure both that Brazil's National Critical Infrastructures adopt proven approaches to cyber defense and that Brazil is postured to cooperate interoperably with the international community in confronting transnational threats. Likewise, any cybersecurity certifications contemplated under Strategic Action 1 should be aligned with internationally recognized technical standards for similar reasons.

2 - Policies Should Be Risk-Based, Outcome-Focused, and Technology-Neutral. Malicious cybersecurity activity carries different risks for different systems. There are generally multiple approaches to defending against the same type of cyber attack, and multiple approaches to improving system security and resiliency in general. Policies should reflect these variables, prioritizing approaches that address different levels of risk and enable owners and operators of networks and systems to defend their infrastructure with the technologies and approaches they deem best to meet the level of security desired. BSA recommends that the Proposed Strategy endorse a risk-based, outcome-focused, and technology-neutral approach throughout the strategy.

3 - Policies Should Rely on Market-Driven Mechanisms Where Possible. Information technology is constantly evolving, and cybersecurity threats evolve with it. Neither technologies nor threats are bound by national borders, meaning that overreliance on government structures or regulatory enforcement is unlikely to achieve desired results. Policies that leverage market forces to drive cybersecurity are likely to be most successful in keeping pace with the changing security environment and in achieving the broadest effect.

4 - Policies Should Be Oriented to Protect Privacy. No approach to cybersecurity should compromise the integrity of the data it seeks to defend against malicious cyber activity; cybersecurity policies should be carefully attuned to privacy considerations. Key considerations include ensuring civilian leadership, encouraging strong data protections, protecting personal information in information-sharing mechanisms, and avoiding policies that undermine the use of privacy-enhancing technologies.

Specific Recommendations on Strategic Actions Set Forth in the Proposed Strategy:

In addition to reliance on the principles described above, we offer the following recommendations with regard to specific entries within the Strategic Actions Section of the Proposed Strategy.

Strategic Action 1 – Strengthen Cybersecurity Governance

- BSA agrees that establishing minimum cybersecurity requirements in public procurements can serve as a powerful tool in enhancing public sector cybersecurity and incentivizing stronger security throughout the marketplace. When establishing such requirements, it is important ensure that acquisitions remain technology neutral, avoid domestic preference requirements, ensure any required certification schemes are voluntary, market-driven, broad-based, and internationally aligned, and are consistent with internationally recognized standards.

Likewise, cybersecurity certifications can incentivize cybersecurity awareness and enable consumers to prioritize security when comparing competing products or services. As with procurement standards, certifications should be technology neutral, voluntary, market-driven, and aligned with internationally recognized standards. In addition, as countries throughout the world consider cybersecurity certification schemes, the Government should take measures to ensure any certification schemes established in Brazil are interoperable and reciprocal with similar certifications in foreign markets. Doing so will enable Brazilian businesses to compete more effectively in foreign markets, while contributing to a common baseline of security.

Strategic Action 5 – Elevate the Level of Protection of National Critical Infrastructure

BSA agrees that critical infrastructure protection is fundamental for a robust cybersecurity strategy. This strategic action could be further improved by providing guidance for the creation and maintenance of an up-to-date National Cybersecurity Incident Response Plan for Critical Infrastructure. In addition, to ensure strong cybersecurity policies to protect critical infrastructure, the Proposed Strategy should:

- Focus on security outcomes;

- Use risk-based, flexible policy framework;
- Avoid overbroad definition of critical infrastructure;
- Align critical infrastructure security with internationally recognized standards, particularly as outlined in ISO/IEC Technical Report 27103;
- Avoid indigenous security standards;
- Ensure any certification regimes are balanced, transparent, and internationally based;
- Reject requirements to disclose source code and other intellectual property.

Strategic Action 6 – Improve Cybersecurity Legal Framework

BSA commends GSI for promoting a stronger cybersecurity legal framework, which is an important foundation for the deterrence, prevention, and prosecution of cybercrime. The Budapest Convention on Cybercrime establishes an international standard for an effective and just national cybersecurity legal framework; BSA urges Brazil to direct its efforts under Strategic Action 6 toward aligning its legal framework with the Budapest Convention. Moreover, this legal framework should:

- Enable cross-border data flows for business purposes;
- Avoid data localization requirements;
- Maintain a policy environment that enables emerging technologies; and
- Ensure adequate technical training and support for law enforcement.

Strategic Action 8 – Increase International Cooperation on Cybersecurity

As the Proposed Strategy rightfully recognizes, international cooperation on cybersecurity is essential. Multilateral efforts underway right now are aiming to create the standards that will guide security across emerging technologies, such as 5G communications networks and the Internet of Things, as well as in emerging areas of concern, such as supply chain security. In pursuing the international engagement outlined in Strategic Action 8, it is essential that Brazil take part in these future-shaping initiatives. Moreover, as these standards take shape, BSA urges Brazil to work to influence and adopt these international standards rather than seek Brazil-specific solutions to what are clearly transnational challenges.

Strategic Action 10 – Elevate the Level of Cybersecurity Maturity

Strategic Action 10 rightfully identifies the need to promote capacity building in the area of cybersecurity; this action should be clarified by establishing the importance of identifying/mapping the necessary skills and the existing gaps as the first step to achieving this goal.

It is also important to include reference to initiatives to promote the development of cybersecurity skills. Addressing the shortage of workers with cybersecurity skills should include actions that target the entire workforce spectrum.

The Proposed Strategy should encourage initiatives to increase interest in and access to computer science education for students in basic education (“alunos no ensino básico), with a focus on expanding public-private partnerships, re-envisioning vocational education, and training more STEM-qualified teachers. It also important to focus on mid-career retraining programs to provide workers with high-demand cybersecurity skills. This should include initiatives to allow Federal agency employees to leverage private sector expertise for training on a variety of cybersecurity skills and best practices.

BSA Framework for Secure Software

Finally, BSA recognizes that software will play a vital role in the success of all of the Strategic Actions identified in the proposed strategy. Modern society is built on software – software powers personal technologies, critical infrastructure, industries across every sector, and emerging technologies such as 5G and Artificial Intelligence. As communities and businesses become ever more dependent on software, the security of that software becomes paramount.

BSA is committed to elevating the level of software security across the digital ecosystem. Earlier this year, BSA released the *BSA Framework for Secure Software*, a first-of-its-kind benchmark for software security that is specific, measurable, and applicable to software of all kinds. It is intended to enable meaningful evaluation of the security of software products and services and to inform discussions between key stakeholders – developers, suppliers, consumers, policymakers, and others – in order to elevate the security of those products and services and enable security-informed decisions in the marketplace.

We offer the *BSA Framework for Secure Software* as a resource to the Brazilian Government as it pursues initiatives to enhance cybersecurity and look forward to opportunities to collaborate with the government to address the security of software. We would welcome the opportunity to provide more information about the Framework as appropriate.

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
Country Manager – Brazil
BSA | The Software Alliance