U.S. CHAMBER OF COMMERCE

1615 H Street, NW
Washington, DC 20062-2000
www.uschamber.com

September 19, 2019

Antônio Carlos Oliveira Freitas
Director
Departamento de Segurança da Informação – DSI
Gabinete de Segurança Institucional – GSI da Presidência da República do BrasilPalácio do Planalto, Anexo II, Ala A, Sala 108CEP 70150-900, Brasília-DF

Director Freitas:

The U.S. Chamber of Commerce ("the Chamber") is the world's largest business federation, representing the interests of more than three million businesses of all sizes and sectors, many of whom are major employers and provide significant investment in the Brazilian economy. The Brazil-U.S. Business Council ("Brazil Council") is the premier business advocacy organization dedicated to strengthening the economic and commercial relationship between the two countries. The Brazil Council represents major U.S. companies invested in Brazil and operates under the administrative aegis of the Chamber in Washington, DC.

Over the past 2 years, the Chamber and the Brazil Council has engaged extensively with the Government of Brazil ("Brazil" or "the Government") as it explored which policy proposals would drive the best cybersecurity outcomes in Brazil. Our engagement during this period includes two delegations to Brazil for meetings with several government agencies, as well as formal public submissions. It is indicative of the importance we attach to Brazil-U.S. economic relations.

We commend the Government for engaging such a broad range of stakeholders during the development of the draft National Cyber Security Strategy ("the Strategy"), including foreign governments, civil society and the private sector. Incorporating a wide range of perspectives serves to enrich the quality of policies and strategies, as is evident in the draft that you have presented.

The Chamber considers cybersecurity to be a top priority. Network systems today underpin many of the most critical systems in our respective economies. These systems must be adequately protected against cyber threats if we are to ensure that the benefits created by the digitization of our economies are not outweighed by the risks.

Accordingly, the Chamber has worked with more than 35 governments to develop and implement cybersecurity solutions that ensure appropriate levels of cybersecurity for businesses of all sizes and in all sectors of the economy. This engagement has afforded us the opportunity to see first-hand what makes for effective cybersecurity policy.

Our comments on the Strategy are divided into those areas where we consider the approach taken to be effect ("Positive Aspects"), those where we would suggest an alternative approach ("Areas of Concern"), and those where we would welcome further guidance or clarification ("Further Clarification Requested"). We offer this analysis as part of our shared desire to drive enhanced cybersecurity outcomes in Brazil and abroad.

Positive Aspects of the Strategy

- The Strategy consistently refers to the need to utilize a risk management based approach to cybersecurity, an approach which is regarded as an international best practice.
- The Strategy references the importance of utilizing international standards, enabling the deployment of best-in-class cybersecurity solutions across borders, and avoiding the establishment of non-tariff barriers to trade.
- The selection of critical infrastructure sectors is appropriately narrow to ensure a focused approach towards reducing cybersecurity risk in Brazil.
- Recommendations regarding security measures and threat information sharing remain voluntary, enabling appropriate flexibility in their implementation.
- Streamlining Brazil's convoluted information sharing ecosystem ensures that information does not become unnecessarily siloed.
- Oversight of critical infrastructure entities will continue to take place on a sectoral level, which has proven to be an effective approach in Brazil.
- The Strategy places appropriate emphasis on the need to cooperate internationally and with a wide variety of stakeholders.

Areas of Concern with the Strategy

- References to "standardize" best practices seems to indicate a move towards a one-size-fits-all approach. This runs counter to risk management based approaches and, where such national approaches diverge from international best practices, could undermine both trade and cybersecurity outcomes.
- The use of audits on an annual basis is too frequent, given the amount of resources required to fulfill such requirements. This will divert resources away from cybersecurity activities towards compliance, which may lower cybersecurity outcomes.
- A focus on the "measurement" of cybersecurity effectiveness must be balanced. Effective defense and deterrence is seldom quantifiable, given that it prevents incidents from taking place. The Government should avoid basing its recommendations solely off of cyber incidents which succeeded as this gives a distorted view of reality.
- While the report references the use of international standards and best practices in general, it does not reference the most widely utilized of these, such as the ISO/IEC 27000 series or the NIST Framework for Improving Critical Infrastructure Cybersecurity.

Further Clarification Requested

- While the selection of critical infrastructure sectors is appropriately narrow, the list of companies *within* those sectors that are defined as critical infrastructure entities should be clarified and be appropriately narrow, in line with international best practices.
- There is no guidance on thresholds for cyber incident reporting. We would welcome such guidance from GSI.
- The Strategy makes reference to a certification being developed by the cybersecurity center, but does not clarify the focus of purpose of such a certification.

We have included detailed recommendations below regarding the areas of concern, including references to the specific language in the Strategy to which they pertain.
We appreciate your consideration of this submission. Should you have any questions or comments regarding its content, please contact either Sean Heather (sheather@uschamber.com) or Cassia Carvalho (ccarvalho@uschamber.com) at your convenience.

Detailed Comments on Brazil's National Cyber Security Strategy

Language	Issue of Concern	Proposed Solution
"On October 13, 2008, GSI / PR published Complementary Standard No. 02 / IN01 / DSIC / GSI / PR, which provides information security management methodology and guidance on risk definition; procedures for identifying risks and their acceptable levels; impact and probability analysis; and risk treatment options."	Developing and utilizing national standards for cybersecurity can have counter-productive impacts where they diverge with international approaches. Firstly, they establish *de facto* barriers to trade, by requiring critical infrastructure providers to comply with technical cyber requirements that are unique to Brazil. Secondly, they undermine cybersecurity by preventing multinational entities from scaling cyber best practices seamlessly across borders. Finally, the process of creating national standard unnecessarily divertes finite Brazilian government resources, given that high quality international standards already exist.	We recommend that GSI leverage existing international standards and best practices for Cyber Threat risk management, which have proven to be effective, rather than developing new standards at a national level. Such risk-based, future-proof international standards and best practices include the ISO/IEC 27000 series standards and the U.S. National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*.
"It is necessary to standardize best practices and allow even small organizations to take effective measures to protect their information."	While GSI may wish to codify a series of recommendations for small businesses that seek guidance on how to improve their cyber posture, the vast majority of critical information infrastructure providers have established systems and best practices, which are unique to their	Rather than seeking to standardize best practices, GSI should encourage companies to leverage the core of the *Framework for Improving Critical Infrastructure Cybersecurity* as a basis for developing a cyber strategy that is unique to their situation. This includes identifying,

	company, their systems architecture and the risks associated with that company. The divergent approaches taken in different sectors and companies is at the core of a risk management based approach and should be encouraged. It is what enables companies to tailor their cybersecurity programs to their situation, rather than implementing an 'off the shelf' solution that is not relevant to them.	protecting against, detecting, responding to, and recovering from cyber incidents.
"Within this perspective, three important aspects stand out: the measurement of the effectiveness and efficiency of the treatment and response centers for computational incidents; the development of indicators to measure the country's cyber security performance; and the routine establishment of scheduled cyber security audits within public agencies and private entities , so that the right relationship can be established between the technical aspects of IT, such as vulnerability analysis, technical threat reporting, and solution solutions in technology, with business aspects such as service continuity, image risks and decision-making processes."	While both measurements of effectiveness/efficiency and cyber security audits can be useful tools, one should recognize their limitations and utilize them accordingly. Relevant and accurate data from which to draw insights is typically hard to collect. Accordingly, much data focuses on known cyber incidents and is both backwards looking and subject to survivorship bias. Audits, meanwhile, can be a tool for regulators to assess compliance with regulations. Yet they force companies to expend time and money on compliance procedures, meaning these resources are not utilized addressing cyber threats.	Where relevant data is easily collectible, GSI should do so, and attempt to develop meaningful insights from it. These insights should be shared with critical infrastructure operators, who may use it to further enhance their cybersecurity practices. Audits should take place every two to three years, with self-certification mechanisms utilized on a more frequent basis. Where audits take place, sensitive information must be kept secret and no steps should be taken which would deliberately or inadvertently cause disruption to systems.

"While some digital security recommendations are tailored to a specific tool, network technology, or communication medium, other recommendations are universal. In this regard, it is recommended to establish protocols and requirements regarding the prevention, monitoring, and treatment and response to computational incidents, focused mainly on specialized teams that deal with cyber threats."	As stated above, effective risk management procedures by design vary according to a company's risk profile, usage of technology, and many other factors.	While there may be an opportunity to codify certain best practices, GSI should be aware of its limitations. Divergent risk management strategies should be encourage among critical infrastructure operators, where they are tailored to address an organizations risk profile.
"The Telecommunications sector, the Transport sector, the Energy sector, the Water sector and the Financial sector."	While the selection of sectors is in line with international best practices, it is not clear how GSI will define which companies within these sectors will be subject to the Strategy's security measures requirements.	Just as GSI has narrowed the list of sectors to ensure that resources are focused on the most critical areas, so too should they ensure that the list of critical infrastructure entities *within* these sectors is sufficiently narrow.
"These organizations therefore need the means to identify, assess and manage the risk of cyber threats, as well as security automation tools that use artificial intelligence, machine learning, penetration testing, and analysis to identify and contain cyber attacks."	While GSI is correct to clarify the need to identify, assess and manage the risk of cyber threats, requirement to utilize specific capabilities such as machine learning, penetration testing and automation tools is overly prescriptive. While these may be useful tools in some cases, in others they may not. Certainly we cannot be sure of their utility in the future.	We recommend that references to specific tools or technologies be removed from this provision.
"There is no comprehensive cybersecurity framework that contributes to strengthening cyber resilience"	The NIST *Framework for Improving Critical Infrastructure Cybersecurity* is widely regarded, by both public and	We recommend removing this sentence from the Strategy.

	private sector entities, to be a comprehensive framework that strengthens cyber resilience.	
"existing codes, standards and guidelines have not evolved with the development of cybersecurity engineering projects, tools and engineering practices"	While malicious cyber attacks continue to innovate in terms of their activities, so too have cyber defenses continued to improve and adapt to new threats.	We recommend removing this sentence from the Strategy.
"insertion of annual cyber security external audit plans"	As stated above, audits drain resources away from cybersecurity activities and should therefore be used sparingly.	Audits should take place every two to three years, with self-certification mechanisms utilized on a more frequent basis. Where audits take place, sensitive information must be kept secret and no steps should be taken which would deliberately or inadvertently cause disruption to systems.
"certification establishment in cyber ministry"	It is unclear how such a certification would be utilized and what it would cover. Before developing a national certification, GSI should seek to leverage existing international certification mechanisms, to avoid creating trade barriers or inhibiting the ability of international experts to operate in Brazil.	We welcome further clarification as to the purpose of the certification. Where possible, we would encourage the government of Brazil to leverage existing certification mechanisms.