U.S. CHAMBER OF COMMERCE

Brazil-U.S. Business Council

November 18, 2017

Via: denor@bcb.gov.br

Otavio Ribeiro Damaso
Financial System Regulation Department (Denor), SBS,
Quadra 3, Bloco "B", 9° andar, Edifício-Sede,
Brasília (DF)
70074- 900

Subject: Banco Central do Brasil Public Consultation Notice 57/2017

Dear Mr. Damaso:

The U.S. Chamber of Commerce is the world's largest business federation, representing the interests of more than 3 million businesses of all sizes, sectors, and regions, many of whom are major employers and provide significant investment in the Brazilian economy. We welcome the opportunity to provide the following comments as part of the public consultation on the cybersecurity policy and requirements for institutions authorized by the Banco Central do Brasil ["Central Bank"].

The Chamber congratulates the Central Bank for its leadership and private-sector engagement in the development of this regulation. While there are aspects of the public consultation that are positive, we believe that certain changes are needed if the regulation is to be effective in ensuring that the cybersecurity systems of regulated entities are sufficient. We offer the following comments and recommendations:

- **Remove all provisions that require data to be stored within Brazil.** Transferring, processing, or storing data across borders does not expose data to greater security threats. In fact, storing data in Brazil may *increase* the risk of a breach, as companies are forced to choose between a smaller number of contractors, rather than hiring the best available international partners. Further, these regulations will have a chilling effect on innovation, reduce opportunity in the local economy, limit choice to both businesses and consumers, lower service levels, and raise costs for all stakeholders.

  Data localization disrupts centralized data storage and processing so companies are unable to take advantage of economies of scale and a seamless, global internet. A report from the Leviathan Security Group also shows that data localization measures raise the cost of hosting data by 30-60% for companies. This adversely impacts small businesses in particular, by increasing their costs, creating barriers to market entry and stifling innovation. It also risks harming the Brazilian economy by raising domestic prices and non-tariff barriers on imports, and reducing its competitiveness in the long term.[1]

[1] http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf

In particular, the proposed data localization requirements restricting the transfer of data beyond national borders will make it more difficult for affected entities to combat fraud by preventing the identification of patterns of fraud across regions. Effective fraud prevention and mitigation are dependent on cross-border data flows, as they demand sophisticated monitoring of transactions and rapid detection at the point of interaction to interpret and weigh the risk of fraud of each payment transaction. To build effective fraud models and to gain the necessary insights into fraudulent patterns in order to help prevent them, these models must be built from global or multi-country data sets and analyzed in a central location in order to identify and block potentially fraudulent activity in real time.

Finally, these measures unfairly discriminate against companies that do not have a local presence in Brazil. Given that this will likely not lead to an increase in levels of cybersecurity, this could represent a violation of Brazil's international obligations to take the least trade restrictive approach to regulation. As such, we strongly recommend that the Central Bank remove all data localization requirements from the proposed regulation.

- **Remove onerous company reporting requirements.** The proposed regulation requires companies to undertake overly onerous reporting requirements, which will drain cybersecurity resources away from implementing best in class systems in favor of 'check the box compliance'. Requirements to trace the movement of all data, register the location of all data storage facilities, log all "material incidents", provide all contracts and agreements with third party storage providers, and develop an annual report, in particular, will significantly raise the costs of compliance for companies, while providing no increase in the levels of cybersecurity.

- **Enable companies to assess and manage cybersecurity risks to their business, rather than prescribing specific solutions.** A risk management approach to cybersecurity has proven to be more effective than prescribing specific solutions, as it enables companies to assess the needs relevant to their situation and choose from among the range of tools at their disposal. **T**he use of cloud computing, for instance, has the potential to reduce a company's vulnerability to cyber incidents and should not be subject to additional regulatory measures which disincentivize its use.

  Prescriptive requirements such as those in *Article 3.VII.Paragraph 2* force companies to implement systems which may not increase levels of cybersecurity, draining resources away from systems that will. Moreover, such detailed resolutions risk becoming quickly obsolete in the face of rapid technological change, thereby losing efficiency in relation to the larger goal of ensuring the security of Financial Institutions data and information.

- **Facilitate voluntary information sharing, rather than mandating broad reporting requirements.** Frameworks that force companies to report a broad range of cybersecurity incidents can unintentionally inhibit cybersecurity by causing companies to notify regulators of any incident on their systems. This can lead to notification fatigue, increased costs, and operational distractions, which makes it difficult to identify and

address the most important incidents. Accordingly, we recommend that you remove any mandatory information sharing or reporting requirements.

- **Remove requirements that companies share sensitive commercial information without a clear regulatory or investigatory purpose.** While companies may have access to instruments used by contractors, given the sensitivity of this information it should not be *required* of contractors without a specific need. This includes provisions that require an entity to grant regulators access to encryption keys, rather than simply turning over relevant information. Accordingly, we recommend that you remove any such provisions.

- **Avoid Creating Overlapping Cybersecurity Regulatory Requirements.** The Institutional Security Office of the Presidency of the Republic (GSI) is in the final phase of preparing a draft Public Consultation on the topic of National Information Security Policy. Considering the transversality of their work, covering critical infrastructure sectors such as finance, there is significant potential for this proposal to require measures that contravene, or overlap with, those of the GSI. Accordingly, we recommend that you delay the further development of this proposal until such a time as the GSI requirements are finalized.

The attached table explains our concerns in greater detail, seeks clarification on several provisions, and offers our recommendations. If you have any questions or need further information, please contact me (ccarvalho@uschamber.com) or my colleagues Sean Heather (sheather@uschamber.com) and Ann Beauchesne (abeauchesne@uschamber.com).

Sincerely,

Cassia Carvalho
Executive Director
Brazil-U.S. Business Council
U.S. Chamber of Commerce

Sean Heather
Vice President
Center for Global Regulatory Cooperation
U.S. Chamber of Commerce

Ann M. Beauchesne
Senior Vice President
National Security and Emergency Preparedness
U.S. Chamber of Commerce

Article	Summary of Content	Comment
Article 3.II-IV	*"stipulate the controls and technologies adopted by the institution to reduce its vulnerability to incidents and address other stipulated cybersecurity objectives; define specific controls, including those used to ensure data traceability in order to secure sensitive information; stipulate logging or recording, analysis of cause and impact, and control of the effects of incidents that are material for the institution's activities;"*	Without clear examples of how this would be implemented, we would suggest rewording this provision to be less restrictive, while maintaining the underlying regulatory intent. In this regard, we would suggest merging provisions II-IV, such that they read "Identify controls and technologies used by the institution, including those used to document access, data management, data control, and incident management as stipulated under the institution's cybersecurity objectives."
Article 3.III	*"define specific controls, including those used to ensure data traceability in order to secure sensitive information."*	Given that companies may hire contractors that manage data servers around the world, requirements to ensure the traceability of all consumer data would pose a large and unnecessary burden on consumers. As such, we recommend that you remove this requirement.
Article 3.IV	*"stipulate logging or recording, analysis of cause and impact, and control of the effects of incidents that are material for the institution's activities."*	While many of these activities will be undertaken by companies as part of their cybersecurity processes, mandating these processes is unnecessarily prescriptive and risks placing an unnecessary administrative burden on companies. As such, we recommend that your remove this requirement.
Article 3.VII	*"stipulate initiatives to share information with other institutions involving material incidents."*	While information sharing can be an effective tool in increasing cyber resilience, *mandatory* requirements to report cybersecurity incidents can unintentionally inhibit cybersecurity by causing companies to notify regulators of any incident on their systems. This can lead to notification fatigue, increased costs, and operational distractions, which makes it difficult to identify and address the most important incidents. Moreover, cyber threat information sharing is most effective when it involves the proactive sharing of indicators and contextual information, rather than reactive attempts to disseminate information. As such, we recommend that you remove mandatory

		requirements to share incident information and encourage regulated entities to leverage established information sharing entities such as the Financial Services ISAC.
Article 3.VII.P1	*"ability to prevent and detect cyber related incidents while reducing vulnerability in this respect"*	Requirements that data be localized in Brazil expressly limit the ability for companies to monitor and proactively identify vulnerabilities worldwide. As such, we strongly recommend that you remove the data localization requirements outlined in Articles 11, 12.VIII, and 19 & Sole Paragraph.
Article 3.VII.P2	*"controls and technologies … should at the least cover authentication, encryption, preventing and detecting intrusion, preventing data leakage, controlling of hardware and software updates, periodic testing and scanning to detect vulnerabilities, protection against malicious software, controls of access and segmented computer networks."*	A risk management approach to cybersecurity has proven to be more effective than prescribing specific solutions, as it enables companies to assess the needs relevant to their situation and choose from among the range of tools at their disposal. Prescriptive requirements such as this force companies to implement systems which may not increase levels of cybersecurity, draining resources away from systems that will. As such, we recommend that you remove this requirement.
Article 3.VII.P4	*"The registration, analysis of cause and impact, and control of effects of incidents mentioned in subparagraph IV must also include information received from Third Party Service Providers."*	While many of these activities will be undertaken by companies as part of their cybersecurity processes, mandating these processes is unnecessarily prescriptive and risks placing an unnecessary administrative burden on companies. Moreover, if the regulatory reporting requirement is not well defined, proprietary information and client data would be subject to exposure would be placed at greater risk of exposure to a cyber incident. As such, we recommend that you remove this requirement.
Article 3.VII.P6	*"Cybersecurity policy should be spread using language compatible with the complexity of the functions involved to reach."*	Greater clarity is requested regarding what is required of companies in this regard.
Article 5	*"The institutions referred to in article 1 shall designate a director or officer in charge of cybersecurity policy and*	While establishing a point of contact may be an effective means of communication, we request greater clarification as to what, if any, legal liabilities this person would be subject to. We would strongly

	the action plan and incident response procedure mentioned in article 4."	recommend that no personal legal liability be attributed to a person in this role if companies are to be able to hire the most talented people for such a role.
Article 6	*"The institutions referred to in article 1 shall prepare an annual report covering their action plans and incident response procedures as mentioned in article 4, by base date December 31."*	This will force companies to undertake overly onerous reporting procedures, which drains cybersecurity resources away from implementing best in class systems in favor of 'check the box compliance'. As such, we recommend that you remove this requirement.
Article 6.P2.I	*"the efficacy of the action plan and incident response."*	Greater clarity is requested regarding what benchmark criteria would be utilized in this assessment.
Article 6.P2.III	*"business continuity test results, including downtime scenarios arising from incidents"*	Greater clarity is requested regarding what benchmark criteria, tests or exercises would be expected of the relevant entities. We recommend further clarifying these as "business continuity for cybersecurity events".
Article 9.II.c)	*"auditing of the services provided and their compliance with rules and regulations."*	Greater clarity is requested regarding whether such an audit would be conducted by the contractor, the contracting party or a government regulator.
Article 9.II.d)	*"financial institution's access to instruments used to monitor and manage the controls provided by the contractor in providing the services."*	While companies may have access to instruments used by contractors, given the sensitivity of this information, it should not be required of all contractors, nor without a specific regulatory need. As such, we recommend that you remove this requirement.
Article 9.III	*"ensure the contractor has the ability to deploy physical or logical controls used to identify and segregate the financial institution's client data."*	Greater clarity is requested regarding what specifically would be required of contractors under this provision.
Article 9.III.P3	*"the institution shall ensure that the contractor adopt controls to mitigate the effects of any vulnerabilities when new versions of the application are rolled out."*	As part of their ongoing cybersecurity procedures, companies assess the vulnerabilities associated with a given product. Moreover, there is little evidence that a newer version of a product is more likely to contain a vulnerability. As such, we recommend that you remove this requirement.

Article 11	*"Material data processing, storage and cloud computing services must not be provided abroad."*	Transferring, processing, or storing data across borders does not expose data to greater security threats. In fact, storing data in Brazil may increase the risk of a breach, as companies are forced to choose between a smaller number of contractors, rather than hiring the best available international partners. Depending on how the Central Bank of Brazil defines "material" data processing, data storage, and cloud computing services, the proposed language could prevent affected entities from using their state-of-the art and globally centralized facilities for the processing of financial information for payment transactions and other information necessary to provide cutting edge value-added services and solutions. In addition, data localization disrupts centralized data storage and processing so companies are unable to take advantage of economies of scale and a seamless, global internet. A report from the Leviathan Security Group also shows that data localization measures raise the cost of hosting data by 30-60% for companies. This greatly impacts small business and start-ups who experience increased costs and barriers to market entry, stifling innovation and reducing an economy's competitiveness in the long term. Finally, these measures unfairly discriminate against companies that do not have a local presence in Brazil. Given that this will likely not lead to an increase in levels of cybersecurity, this could represent a violation of Brazil's international obligations to take the least trade restrictive approach to regulation. As such, we strongly recommend that you remove this requirement.
Article 12.I	*"Data processing, storage and cloud computing service agreements shall stipulate the locations of facilities where services will be provided and data will be stored, processed and managed."*	This provision places a huge burden on regulated entities, in particular those who contract with cloud service providers. One of the benefits of cloud computing services is the ability for information to be moved and stored seamlessly across borders. Among other benefits, this enables regulated entities to store data where it is likely to be most secure.

		This provision would create a disincentive to leverage such services, potentially leading to extra costs, lowered performance, and lower levels of cybersecurity. As such, we strongly recommend that you remove this requirement.
Article 12.VII	*"the Central Bank of Brazil has access to contracts and agreements signed for the provision of services, documentation and information involving the services provided, data stored and respective information concerning data processing , as well as the facilities mentioned in subparagraph I."*	Greater clarity is requested regarding whether this requires companies to send all service contracts and agreements to the Central Bank, for them to keep on file, or to provide *access* to them in the event that the Central Bank needs to review them. If the former, we recommend that this requirement be removed as it would place a large and unnecessary burden on regulated entities. If the latter, we would encourage the Central Bank to make clear to regulated entities when they will need to make such information available, ensuring that such instances do not place an unnecessary administrative burden on companies.
Article 12.VIII	*"backups of data and information stored by the contractor together with information about its processing must be kept in Brazil."*	See comment regarding Article 11.
Article 12.X	*"the financial institution must be able to take any measures required by the Central Bank of Brazil."*	As written, this provision is too broad. It could create a situation in which companies are required by law to take a measure by the Central Bank which is prohibited under another statute. As such, we request greater clarity as to the intent of the provision and recommend that it be significantly narrowed in scope.
Article 12.X.P2.I	*"obligation of the contractor to allow full and unrestricted access of the person or entity responsible for the liquidation/winding up arrangements to the contracts, agreements, documentation and information mentioned in subparagraph VII, as well as copies of data and information mentioned in subparagraph VIII, including*	Without a clear legal or investigatory purpose, companies should not be required to provide sensitive commercial information, such as encryption keys, to regulators. Where there is a clear legal or investigatory need to obtain encryption keys, rather than simply be granted access to the required information or data, the Central Bank should request authority to obtain these through traditional legal channels.

	encryption keys and systems required for its processing."	As such, we recommend that this requirement be removed.
Article 12.X.P2.II	*"obligation of giving advance notice to the person or entity responsible for the liquidation/winding up arrangements as to the contractor's intention to cease services at least thirty days before the scheduled date…"*	Where there is a clear investigatory or security need to remove a contractor, the institution should not be bound to retain the contractor for thirty days. As such, we recommend that this requirement identify the scheduled date and that the institution may provide the Central Bank notice of cease of contractor service for just cause within an appropriate time period.
Article 14.II	*"estimates of the period required to resume or normalize its disrupted activities or material services as mentioned in subparagraph I."*	Greater clarity is requested regarding the purpose of this provision. Given that the nature or extent of an attack may not be clear in the immediate aftermath, information provided will likely be at best a rough estimate and should therefore not impose any legally binding obligations on companies.
Article 14.III	*"timely communication to the Central Bank of Brazil of any material incidents and disruptions of the material services mentioned in subparagraph I that prompt the financial institution to declare a crisis situation and measures taken to resume its activities."*	Greater clarity is requested regarding the Central Bank's definitions of "timely communication" and "declare a crisis situation".
Article 16.P1&2	*"The sharing mentioned in the heading must include information received from Third Party Service Providers that handle sensitive data or information that is material to the conduct of the institution's activities.* *The Central Bank of Brazil must have access to the shared information."*	Frameworks that force companies to report a broad range of cybersecurity incidents can unintentionally inhibit cybersecurity by causing companies to notify regulators of any incident on their systems. This can lead to notification fatigue, increased costs, and operational distractions, which makes it difficult to identify and address the most important incidents. Accordingly, we recommend that you remove this requirement.
Article 17	*"…retained at the Central Bank of Brazil's disposal for five years"*	The requirement to maintain security logs, access management records, and processing documents would create an immense data storage requirement that would create additional cost, need to maintain additional servers and operating system structures,

		and create operational distraction in order to maintain archives. As such, we recommend a more narrowed retention period.
Article 18.I	*"the form of sharing and the information that must be shared under article 16."*	See comment regarding Article 16.P1&2.
Article 18.II	*"certifications and other technical requirements to be required of contractors engaged by a financial institution in its capacity as principal for the provision of services mentioned in article 9."*	In order to ensure that they have the effect of increasing levels of cybersecurity, any certifications or technical requirements should be based upon best-in-class, international standards. We strong recommend that you consult with the private sector regarding the development of any such measures, in order to leverage their expertise, and ensure that any resulting requirements are crafted so as to avoid creating barriers to entry for international service providers.
Article 18.III	*"the final dates mentioned in article 14, subparagraph II, for resuming or normalizing disrupted material activities or services."*	Creating timelines for the resumption of services will be counter-productive. Pressuring companies to meet an arbitrary deadline, rather than resuming service at a time when they are confident in the integrity and security of their systems, will lower overall levels of cybersecurity. As such, we recommend that you do not take any such measures.
Article 18.IV	*"the technical requirements and operational procedures to be followed by the institutions in order to comply with this Resolution."*	See comment regarding Article 18.II.
Article 19 & Sole Paragraph	*"Institutions that have already engaged material data processing, data storage and cloud computing services from another country must draw up a schedule for these services to be engaged in Brazil and submit it to the Central Bank of Brazil within ninety days of the date on which this Resolution enters into force.*	See comments regarding Articles 11 and 12.VIII.

	The abovementioned services must be fully deployed in Brazil by December 31, 2021."	
Article 21	*"This Resolution shall enter into force one hundred and eighty (180) days as of its publication date."*	While some companies may be compliant within this time period, this is a fairly short timeframe in which to ensure compliance with such broad provisions. As such, we strongly recommend that the time frame for entry into force be extended.