28 May 2018

Respectfully to: **The National Assembly of Vietnam**
22 Hung Vuong, Ba Dinh, Hanoi

Attention: **Madame Nguyen Thi Kim Ngan**
The Chairwoman

Joint Industry Comments on May 24 Revised Draft Law on Cybersecurity

On behalf of the US-ASEAN Business Council (**"the Council"**), Asia Internet Coalition, BSA | The Software Alliance (**"BSA"**), JEITA, ITI, and our members, we write to express our sincere gratitude to the National Assembly for the opportunity to submit comments on Draft 18 of the Law on Cybersecurity ("**Draft Law**").

We remain strong supporters of Vietnam's continued efforts to establish a legal framework on Cyber Security, which strengthens information security, and enhances the preparedness for the prevention, and response to cybercrime. We appreciate the National Assembly ("**NA**") and the Ministry of Public ("**MPS**") for developing this Draft Law. As evidenced in our previous submissions,[1] we continue to share the common goal of establishing a trusted cybersecurity culture for users that supports the growth of Vietnam's digital economy and of reducing cyber incidents, such as ransom-ware, cyber theft, banking fraud and disruptions to Internet services, in ways that are mutually beneficial to Vietnam and industry stakeholders.

We commend the government of Vietnam for the added provision of including the Ministry of Foreign Affairs in international cooperation efforts against cybercrime. Such inter-agency cooperation is globally recognized as a best practice for cybersecurity legislation development and implementation, and can lead to stronger and more efficient cybersecurity protection and enforcement. Increasingly, the balance between cyber trust and crime prevention is a key determinant. Technologies can clearly bring tremendous benefits to citizens and customers and guarding against criminal exploitation is only one aspect of trust in cyberspace. Much of cyber trust goes to how systems are built and used in relation to their purposes. Vietnam is cognizant of how these functions are regulated separately to achieve a harmonious balance.

However, the Council, Asia Internet Coalition, BSA, JEITA, ITI, and our members remained concerned about certain provisions in the Draft Law that remain unclear and pose challenges to our member companies – specifically regarding ambiguous language surrounding content restrictions and data localization requirements that unintentionally end up weakening rather than strengthening the existing cybersecurity infrastructure. Data localization will restrict business opportunities not only for multinational companies, but also severely limits the capabilities of many small and medium-sized enterprises (**"SMEs"**) both foreign and domestic. We also remain concerned about the proposed audit and certification systems, the operation of which remains unclearly defined and presents a potentially onerous cost to businesses, a cost which will disproportionately affect SMEs.

[1] The US-ASEAN Business Council submitted comments on the previous versions of the Draft Law on Cybersecurity on August 25, 2017; October 31, 2017; February 26, 2018; and May 17, 2018.

Therefore, we would like to respectfully request the NA, MPS, and other relevant agencies to consider the following comments and suggestions when reviewing the Draft Law and make the necessary changes before enactment:

1. National security is not clearly defined and limited under the Draft Law

Issue:

National security is the main concern and the driving force behind the Draft Law. However, national security and its related terms (e.g., *information that is important to national security* under **Article 26**) are not clearly defined under this Draft Law.

Many prohibited acts under this Law are not national security issues but rather general threats to law and order; however, all such acts are all treated as national security concerns and are managed and handled with the same level of severity.

Analysis:

1.1. International practices require national security to be clearly and narrowly defined

We understand that the State has legitimate concerns regarding national security and there are certain national security exceptions under international treaties such as the GATT, the GATS, the TRIPS Agreement and the CPTPP. However, the national security exceptions in these international agreements are not meant to be all encompassing. As such, the Draft Law may not be fully consistent with the obligations Vietnam has under these agreements.

National security should be defined clearly and narrowly to justify a compromise with civil rights and business interests of the people. The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights provide that national security may be invoked to justify measures limiting certain rights only when they are taken to protect the existence of the nation, its territorial integrity or political independence against force or threat of force.

National security cannot be invoked as a reason for imposing limitations to prevent merely local or relatively isolated threats to law and order. National security cannot be used as a pretext for imposing vague or arbitrary limitations and may only be invoked when there exist adequate safeguards and effective remedies against abuse.[2]

1.2. The scope of national security under the Draft Law is overly vague and broad, which gives great discretion to the MPS:

The Draft Law does not include any definition of "national security" under **Article 2**, and the Law on National Security defines "national security" in a very general way, stating that *national security means the stability and sustainable development of the socialist regime and the State of the Socialist Republic of Vietnam, the inalienability of the independence, sovereignty, unity and territorial integrity of the Fatherland*.

However, the Draft Law regulates a wide range of subjects and activities as if they are related to "national security" - e.g., the personal data of individuals, content relating to businesses and the private sector such as finance, banking, e-commerce, e-payment, etc. Not all of these issues can reasonably be considered national

[2] Paragraphs 29, 30 and 31, UN Commission on Human Rights, *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, 28 September 1984, E/CN.4/1985/4, available at: http://www.refworld.org/docid/4672bc122.html [accessed 1 June 2018]

security issues. However, under the Draft Law, they are all managed and handled with the same measures and at the same level of severity. The Draft Law also does not provide any appeal and/or review mechanisms on the cases decided by the MPS.

In any case, this suggests – for example – that criticism of the economy may be considered "illegal" (if such criticisms are considered "fabricated or distorted") under these new provisions. Such vague and broad provisions may potentially violate the legitimate political and civil rights of the people, as well as interfere with the normal operation of private businesses.

Position and Recommendations:

The Council, Asia Internet Coalition, BSA, JEITA, and ITI recommend the Draft Law to clearly define "national security" and limit the scope of issues/activities under national security. Prohibited acts and relevant information regarding social orders, and the rights and interests of organizations and individuals should be managed and handled using different measures at a lower level of severity. National security should be distinguished from the compliance of law and social orders, and other rights and interests of organizations and individuals.

2. The Draft Law's updated prohibited acts in relation to illegal content leave room for ambiguity and do not limit their application to actors with malicious intent. The Draft Law should not require corporations to monitor and police these activities.

Issue:

The Draft Law includes new, ambiguous language in **Article 8.1** that places prohibitions on a variety of potentially unintended and non-malicious actions in cyberspace, including:

- Distorting the history or negating a revolution achievement
- Sabotaging great national unity
- Offending any religion
- Giving misleading information causing confusion among the people, damages to socio-economic activities or difficulties for authorities' operations or officers on official duty, or encroaching upon any legitimate rights and interests of any other entities or individuals

The Draft Law also contains a new provision in **Article 26.2(b)** mandating corporations "delete or prevent the sharing of, information containing any content as stated in Sub-Articles 15.1, 15.2, 15.3 and 15.4 hereof on the services or information systems directly managed by them within 24 hours."

Analysis:

The new clauses under Article 8.1 are more prescriptive compared to the scope of "illegal content" under Decree No. 72, yet are not clearly defined. The clauses can be broadly interpreted in ways which can lead to harm for both Vietnamese and international businesses, including individual and commercial harm, and can impede innovation. For example, criticism of the economy could be considered illegal under Article 8.1(d) should the government consider the statement to be "misleading information". The wide scope of these prohibitions does not explicitly require malicious intent for prosecution.

Additionally, the Draft Law transfers the onus of policing content deemed to be illicit to the private sector. It requires that corporations, both foreign and domestic, "delete or prevent the sharing of," content deemed to be illicit. This clause effectively transfers the state's responsibility of policing to private entities with operations in Vietnam.

Position and Recommendations:

The Council, Asia Internet Coalition, BSA, JEITA, and ITI recommend the Draft Law remove the added clauses under Articles 8.1 and 26.2(b), and to address cybercrime and content regulation related issues through a separate legislative instrument. Should the Government retain Article 8.1, we would suggest a more limited definition of prohibited acts that is solely focused on cybersecurity-related harms, as opposed to content regulations. In addition, the Council urges the Draft Law to limit the application of these clauses to actors with malicious intent.

3. The Draft Law's updated definition of illegal content is more prescriptive, yet not always clearly defined, leading to legal uncertainty and unpredictable commercial outcomes.

Issue:

The Draft Law includes new clauses in **Article 15.4** which prohibits "Information in cyberspace containing contents in violation of the economic management order," including "misleading contents," regarding:

- goods, currencies, money orders, government bonds, cheques and other valuable papers
- finance, banking, e-commerce, e-payment, currency trading, capital mobilization, network business and securities

The Draft Law includes similar language to prohibit "cyberespionage, and encroachments on State secrets, work secrets or personal information in cyberspace," in **Article 16.1.**

Analysis:

The prescriptive nature of these clauses paired with the ambiguous language the Draft Act employs leaves the Vietnamese government with broad power to criminally prosecute any business it views as offering "misleading contents" regarding financial instruments. These clauses also noticeably lack a concern with malicious intent. Additionally, the Draft Act's inclusion of the undefined term "work secrets" creates increased uncertainty.

Position and Recommendations:

The Council, Asia Internet Coalition, BSA, JEITA, and ITI recommend the Draft Law to remove content restrictions unrelated to national security and to limit those subject to prosecution to only those demonstrated to be acting with malicious intent. Instead, we strongly recommend that content regulation issues be addressed through a separate legislative instrument. The wide scope of content restrictions within this Draft Law will inhibit business operations and communications for both foreign and domestic firms.

4. The Draft Law's expansion upon data localization and local office requirements will harm enterprises of all sizes in Vietnam, and also undermine the security of Vietnamese consumers.

Issue:

The Draft Law expands data localization provisions to:

- Include "local and foreign agencies and entities, when providing services on cyberspace or owning any information systems in Vietnam," in **Article 26.2.**

- Require corporations to "set up their mechanisms to authenticate information when users register digital accounts… [and] provide the users' information to the specialized force in charge of cybersecurity protection… in writing," in **Article 26.2(a)**
- Grant the Vietnamese government unrestricted power in the future to "detail what types of information shall be stored in Vietnam and which enterprises are required to locate their head offices or representative offices in Vietnam," in **Article 26.3**

Analysis:

The Draft Law's addition of further ambiguous language, costly requirements, and grant of unrestricted power [to the government? MPS?] with regards to data localization will harm both consumers and businesses in Vietnam by:

- **Unnecessary requirements:** Currently, Vietnam has mechanisms to send takedown requests of illegal content to cross-border service providers of public information under Decree No. 72/2013/ND-CP and Circular No. 38/2016/TT-BTTTT. Following this protocol, international Internet service providers have cooperated with the Ministry of Information and Communications (MIC) to take down thousands of links to illegal content and this effort has been recognized by the MIC itself. Therefore, the presence of a local head office/representative office in Vietnam is not necessary for the cooperation between service providers and the local authorities when there already is a mechanism in place for this purpose.

  Also, current tax withholding mechanisms already account fully for cross-border service providers' tax liability on Vietnam sourced income and ensure equity in business activities between offshore and domestic enterprises. Currently, organizations established and/or operating under Vietnamese law that buy services and make payments to a foreign organization on the basis of a contract must withhold and pay VAT and CIT on behalf of that foreign organization. Vietnam's current foreign contractor withholding tax is also in line with tax practices of other countries. Therefore, the requirement for cross-border service providers to set up local head offices/representative offices in Vietnam is unnecessary in terms of tax collection.

- **Hindering fraud prevention efforts.** The Draft Law limits Vietnamese consumers', enterprises', and government agencies' access to services and technology that rely on international transfers of data (e.g. cloud based services, fraud tools). This in turn hinders fraud prevention efforts as effective fraud models and the real-time blocking of fraudulent activity requires analyzing global or multi-country data sets. The imposition of local data storage requirements that prevents or restricts the transfer of data across borders will make it more difficult for organizations to combat fraud by preventing the identification of patterns of fraud across regions, and may have the unintended and undesirable consequence of benefiting perpetuators of fraud.

- **Increasing costs and unfair competition.** Data localization requirements in this form significantly increase product development costs by requiring equipment to be tailor-made for local markets.

- **Increasing security risks:** Network failures are less disruptive under a globally distributed network, as the free flow of data in the cloud ensures that data remains available on servers in other locations. Restricting the storage of user data geographically prevents Vietnam from benefitting from a more resilient, secure, and reliable system. Using local IT solutions that are out of date with global standards would work against the national security goals of this draft law. Data security furthermore depends on

quality controls and management processes rather than a server's physical location. Businesses choose to store data outside the country of operations to ensure data availability and security in the case of natural disasters, power outages, or other emergencies. Geographic neutrality with regard to data storage enables all companies, particularly small ones, to employ cost-effective information security solutions.

- **Decreasing the security of networks and systems**: Additional approvals may slow down response times when every minute counts in containing threats and more local systems create additional entry points for bad actors to infiltrate. Fragmented data negatively impacts timely responses and visibility to threats, which often impact multiple jurisdictions.

- **Inhibiting the ability to monitor malicious activity and act on trends:** IP address sharing, profiling suspicious activities, isolating cyber-attacks, or preventing lateral movement requires the ability to detect and analyze threat intelligence via data sharing between a firm's legal entities, inter-bank, or with law enforcement. An inability to access and share threat data globally creates "blind spots".

- **Severely limiting any form of effective global or national supervision:** lack of holistic data or restrictions in the collection and sharing of threat data can prevent regulators from doing their job effectively.

- **Increasing business risks:** Forced localization limits business capacity to access infrastructure and tools necessary to support business operations, employees, and networks around the world. Forced localization also inhibits global operations by restricting the mobilization of user data from region to region. Increased costs for companies to comply with requirements to send data to specific locations undermine efficiency and productivity of these businesses and ultimately burden users, making technology more expensive and less secure.

- **Reducing foreign investment:** Imposing these data localization requirements and introducing the uncertainty associated with enhanced authority to create new such rules will negatively impact the Vietnamese economy's appeal as an investment market. The rules are likely to prevent or dissuade Vietnam's start-ups and other companies in the new digital economy from investing in Vietnam, and may hinder Vietnamese firms' ability to become successful businesses. Such requirements may also prevent or dissuade companies to come to or stay in Vietnam to start up global businesses or add Vietnam-based data infrastructure to their existing global networks and operations.

- **Negatively affecting more sectors than in previous drafts, including financial services:** Financial services and infrastructure are particularly vulnerable to cyberattacks due to the high value assets stored in the networks, With the increasing interconnectedness of critical national infrastructure sectors and wider supply chains due to digital technologies, having the private sector work together to share best practices and adopt high standards is vital. Siloed country and sector approaches are ineffective and create additional vulnerabilities. Inconsistent global cyber legislation, regulation and enforcement materially enhance systemic cyber risk. Regulatory fragmentation and inconsistent legislation and law enforcement approaches present serious challenges to the ability of banks to effectively address cyber risk and the coordination of cybersecurity supervisors. Increased coordination by international standard setters to promote common standards and approaches could prevent fragmentation and further support financial stability.

Position and Recommendations:

Vietnam should utilize global cloud infrastructure rather than store cloud-based data by jurisdiction. Thus, we urge the NA to further amend the provisions and align them more closely with international practices. We recommend that all data localization requirements and provisions be removed from the Draft Law.

- -

The Council, Asia Internet Coalition, BSA, JEITA, and ITI have worked closely with governments around the world in relation to the development of national cybersecurity policies and legislation. In doing so, we have witnessed first-hand the potential for such policy and legislation to effectively deter and manage cybersecurity threats.

As a result of these experiences, BSA has developed the International Cybersecurity Policy Framework ("**International Framework**"), which sets out a recommended model for a comprehensive national cybersecurity policy. The Council, JEITA, and ITI strongly support this framework. We have included a copy of the International Framework with this letter in the hope that the NA and MPS may take a fresh look at the proposed Draft Law and work to develop legislation that is fully informed by international best practices, as described in the Framework.

In summary, the Framework recommends six overarching principles that should guide the development of a successful national cybersecurity policy, namely that policies should:

1. be aligned with internationally recognized standards;
2. be risk-based, outcome-focused, and technology neutral;
3. rely on market-driven mechanisms where possible;
4. be flexible and encourage innovation;
5. be rooted in public-private collaboration; and
6. be oriented to protect privacy.

We would like to thank the National Assembly again for the opportunity to comment on the draft Law on Cybersecurity. We greatly appreciate the NA's kind consideration of our above comments, which we have provided with the hopes of sharing expertise and best practices from trusted industry leaders. In the future, we highly recommend that the NA conduct a more transparent and inclusive public consultation process for this legislation, particularly allowing for more sufficient time to provide comment prior to bringing the legislation to a vote. We strongly believe this will allow the NA to draft the most effective and coherent Draft Law possible.

Should you have any questions or need clarification on any of the points addressed above, please do not hesitate to contact us. Thank you for your time and consideration.

--- END ---

cc: Committee on National Defense and Security

Committee on Science, Technology and Environment
Committee on Economic Affairs
Committee on Legal Affairs