



13 December 2018

General To Lam  
Ministry of Public Security  
44 Yet Kieu Str., Hoan Kiem Distr., Hanoi City

**Subject: Comments on the Draft Decree Guiding the Implementation of Law on Cybersecurity**

Dear Minister To Lam:

The Asia Internet Coalition (AIC) and its members express our sincere gratitude to the Ministry of Public Security (“MOPS”) and the Government of Vietnam for the opportunity to submit comments on the latest version of the Draft Decree Guiding the Implementation of Law on Cybersecurity (“LOCS”) or the "Draft Decree".

The AIC is an industry association comprised of leading Internet and technology companies. AIC seeks to promote the understanding and resolution of Internet and ICT policy issues in the Asia Pacific region. Our member companies would like to assure MOPS that they will continue to actively contribute to the security of digital platforms, products and services in support of the digital economy goals of Vietnam.

We commend MOPS and the Government of Vietnam for their efforts on cybersecurity measures. While we support these efforts to develop a legal framework for cyber and information security, we express our concerns on the requirements imposed under the Draft Decree. **The data localization requirements will stifle investment in Vietnam’s digital economy and prove harmful to Vietnam’s long-term economic growth. This will not only hurt international players but will also impact Vietnamese small businesses if they are faced with similar data localization measures as in other countries as they seek to expand. The requirement on the establishment of branches or representative offices in Vietnam ignores the benefits of global business models as legitimate cyber security concerns can be addressed without the imposition of this localization requirement. This requirement will also create undue burden for foreign businesses which are located in Vietnam.**

We urge MOPS and the Government of Vietnam to consider the potential consequences of the Draft Decree in order to prevent unexpected negative impact on the Vietnamese economy. As such, please find appended to this letter detailed comments and recommendations, which we would like MOPS and other relevant agencies to consider when reviewing the draft implementing decree for LOCS. We are grateful to MOPS and the Government of Vietnam for upholding a transparent, multi-stakeholder approach in developing this implementation decree.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact me directly at [Secretariat@aicasia.org](mailto:Secretariat@aicasia.org) or +65 8739 1490 or +84 165 839 0988. Thank you for your time and consideration.

Sincerely,

A handwritten signature in blue ink that reads "Jeff Paine".

**Jeff Paine**  
Managing Director

Cc:

Ms. Nguyen Thi Kim Ngan, National Assembly Chairwoman  
Mr. Nguyen Xuan Phuc, Prime Minister  
Mr. Mai Tien Dzung, Office of the Government, Chairman  
Lt. Gen. Nguyen Manh Hung, Minister of Information and Communications  
Mr. Tran Tuan Anh, Minister of Ministry of Industry and Trade  
Mr. Nguyen Chi Dzung, Minister of Ministry of Planning and Investment

## Detailed Comments and Recommendations on the Draft Implementation Decree

### 1. Scope of Application (Articles 2 and 24)

According to Articles 2 and 24, we understand that the Draft Decree will govern the majority of the online services provided by either domestic or foreign entities, regardless of whether they are operating under Vietnamese law or foreign laws. We are concerned that this scope of application is extremely broad and lacks enforceability, especially with regard to the foreign entities operating under foreign laws.

### 2. Cyber Security Audit (Article 19)

Article 19.1 of the Draft Decree provides that the competent management authority will conduct the cyber security audit of an information system under their authority except for critical information systems. Article 19.1.a which stipulates the cases and subjects of the audit, refers to Article 13 and Article 24 of the LOCS. While Article 13 of the LOCS stipulates the audit of critical information systems, Article 24.1 broadly refers to any cases, where (i) there is an act that prejudices national security or causes serious harm to social order and safety; or (ii) there is a request from the competent management authority. *This provision is misleading and creates a significant confusion because:*

- It stipulates the cyber security audit of non-critical information systems but refers to the cases of auditing critical information systems under Article 13 of the Draft Decree;
- The cases which are subject to the audit are broad and need to be clarified;
- It creates a situation where the audit is decided at the sole discretion of a competent management authority upon their own requests.

**Recommendation:** We recommend that the drafting authority should review and revise the provision to make it consistent, rational and clear. In addition, we suggest that minimum measurable thresholds should be added to trigger the audit. Further the Draft Decree should also bring transparency on due processes and criminal and administrative procedures.

### 3. Requirements on Data Localization (Articles 24 & 25)

The Draft Decree provisions on data localization are a signal towards a hostile policy environment for the digital economy and for businesses in general. These provisions would be technically infeasible, could create harmful impact for Vietnam's digital economy goals, impose cyber security risks and raise costs that would likely be passed along to the consumer. Importantly, data localization will create additional entry points into Vietnam's IT systems for cyber criminals and reduce the choice of digital products and services for Vietnamese users.

As Vietnam seeks to expand its trading relationships, any mandate on data localization will also signal inconsistencies with the Vietnam's international commitments, such as EU-Vietnam Free Trade Agreement (EVFTA) and Comprehensive and Progressive Agreement for Trans Pacific Partnership

(CPTPP). With respect to foreign direct investment and domestic growth, localization requirements will trigger an arrest to cross-border data flow, thereby discouraging investment in many of the business sectors that are driving the highest economic growth opportunities, including ICT, payments and financial services, health care and life sciences, and the sharing economy. Forcing companies to onshore data in Vietnam runs the risk of duplication by other countries and could negatively impact Vietnamese companies seeking to leverage their innovations in international markets.

We view that data localization requirements do not adequately serve the objectives of greater privacy protection, and therefore any such protectionist measures should be removed to serve the interests of Vietnam's digital economy. ***Below are the detailed concerns on data localization requirements in Articles 24 and 25:***

**A. Data localization would be technically infeasible and could create harmful impact on cyber security**

Businesses and consumers across the world are under frequent attack from increasingly sophisticated cyber criminals and state-sponsored cyber warfare. This is true of the world's largest technology companies, small and medium-sized businesses and individuals alike. Theft of consumer data, hacking of accounts and e-commerce scams are among the many cybercrimes that authorities and companies are fighting off every day.

In order to effectively defend against these threats, companies protect user data and other critical information via a very small network of highly secure regional and global data centers staffed with uniquely skilled experts who are in scarce supply globally. These centers are equipped with advanced IT infrastructure that provides reliable and secure round-the-clock service. The clustering of highly-qualified staff and advanced equipment is a critical factor in the ability of institutions to safeguard data from increasingly sophisticated cyberattacks.

Mandating data localization can reduce opportunities for Vietnam, lower service levels, create cyber security risks and raise costs. If data is restricted to remain in one country, multiple data centers would be required in the same country and increased costs would likely be passed along to the consumer.

Mandating the building of additional data centers will harm cyber security in Vietnam by:

- Creating additional entry points into IT systems for cyber criminals;
- Reducing the quality of cyber security in all facilities around the world by spreading cyber security resources (both people and systems) too thin;
- Forcing companies to disconnect systems and/or reduce services; and
- Balkanizing the Internet and impeding global coordination of cyber defense activities, which can only be achieved efficiently and at scale when and where the free flow of data is guaranteed.

Article 24 requires that certain data related to the “users in Vietnam” be stored in country. For at least some international cross-border service providers, which have billions of users all over the world, it is not currently possible to separate the data of the “users in Vietnam” from their users’ data. Given the Internet and cyberspace have no boundaries, it will also be challenging to determine who are the “users in Vietnam” among the significant number of users all over the world. Even if it could be technically possible to store locally all the data related to “users in Vietnam”, such a requirement would potentially create a focal target for cyber-attacks and consequently make Vietnam more vulnerable in terms of cyber security. At the same time, it would reduce the choice of digital products and services for Vietnamese users and companies and therefore increase the cost of access to such services.

## **B. Data localization requirements are inconsistent with Vietnam’s international commitments**

In addition to the negative signaling to business, data localization and local presence requirements run counter to a number of international trade agreements to which Vietnam is a party or hopes to be a party. Thus, MOPS is sending a mixed signal to its trading partners and friendly governments in the region and the world. The data localization requirements in the law and Draft Decree, for example, are concerning enough to the European Union (EU) to potentially disturb the passage of the EVFTA through Parliament.

As Vietnam seeks to expand its trading relationships with the world's leading markets and economic blocs, moving in such a counter-trend direction on one of the most important topics in international trade will cause friction and impede progress on future trade agreements. It may also subject Vietnam to suits being filed against it in international trading fora to which it is a party or hopes to become a party.

Under the WTO, Vietnam committed to allow various services to be provided cross-border and to provide full “national treatment” for service providers not located in Vietnam. The data localization (and local representative office) requirement makes it much more difficult or impossible to provide a service on a cross-border basis and discriminates against that cross-border service provider compared to a provider locally established in Vietnam.

In addition, next-generation trade agreements have specific provisions on data flow to ensure no such restrictions in any sector. Rather than restricting data flow and inserting provisions that create artificial borders within the Internet, next generation trade agreements have disciplines to support ever-more efficient and open data flow. For example, the recently negotiated US-Mexico-Canada Agreement (USMCA, also referred to as “NAFTA 2.0”) prohibits data localization requirements. The USMCA sets a new standard for multilateral trade agreements that takes into account the digital environment and reflects the trend of trade agreements to include provisions that support global e-commerce and digital trade. The CPTPP, to which Vietnam is a party, also includes provisions prohibiting data on-shoring.

We highly recommend that the drafting authority considers the consistency of data localization requirement with the Vietnam’s commitments under the WTO and the CPTPP. For instance, under Article 14.11 and 14.13 of the CPTPP, a Party shall allow cross-border data transfers and shall not require businesses to locate computing facilities in that Party’s territory as a condition for doing business. (While in CPTPP Vietnam negotiated a short-term standstill on dispute settlement, we recommend that the MOPS consider a long-term implementation which does not need to change in the next five years to avoid a legal challenge under CPTPP.)

### **Articles 14.11 and 14.13 of the CPTPP states:**

#### *Article 14.11 Cross-Border Transfer of Information by Electronic Means*

*.. 2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.*

#### *Article 14.13 Location of Computing Facilities*

*.. 2. No Party shall require a covered person to use or locate computing facilities in that Party’s territory as a condition for conducting business in that territory.*

Article 24’s requirement to store certain data in the country amounts, indeed, to a forced requirement to “use or locate computing facilities in the country,” and thus represents a direct violation of Article 14.13 of CPTPP.

In addition to international trade requirements, there is a general recognition by global trade and industry bodies that data localization regulations are likely to hinder innovation and economic development. In June 2017, the Asian Development Bank Institute (ADBI) published a Working Paper Series on the Trans-Pacific Partnership Rules for Digital Trade in Asia (the “ADBI Working Paper”). In that paper, the ADBI states that data localization regulations “often come at a cost for businesses because they are forced to locate their data storage centers onshore or use computing facilities onshore – which prevents businesses from making the most cost-effective decision”.

Forced data localization directly undermines the free and open structure of the Internet. Instead of traveling by the most technically viable routes, data flow would be constrained by geopolitical considerations and regulations. Such requirements would fragment the Internet, reduce consumers’ access to valuable information and communication tools, and discourage innovation. Data localization requirements could have a severe impact on companies — especially Vietnamese start-ups and small businesses — and Internet users alike due to the technical difficulty and cost of compliance. That’s why a growing body of trade agreements and principles explicitly guarantee free cross-border data flow.

### **C. Data localization requirements will stifle investment and growth in Vietnam**

We reiterate that data localization provisions prevent the free flow of data between borders. We submit that there are both economic and technical reasons why this provision should be removed, and data should be allowed to flow freely. Data localization inhibits the functionality and smooth running of global technology platforms. In practice, international technology platforms rely on global cloud infrastructure to deliver consistent services. It is generally not possible or practicable to neatly segregate cloud-based data by jurisdiction. We stress that data localization requirements do not adequately serve the objectives of greater privacy protection and regulatory oversight. Rather, they are harmful in that they inhibit deployment of cloud services in Vietnam and constrain Vietnamese enterprises seeking the benefits of cloud computing, as cross-border data flow enable market access through greater trade and can provide enhanced data security.

Data localization requirements will stifle investment in Vietnam's digital economy and prove harmful to Vietnam's long-term economic growth. Requiring companies to localize data will discourage investment in many of the business sectors that are driving the highest economic growth opportunities, including ICT, payments and financial services, health care and life sciences, and the sharing economy. These are the same digital economy sectors where continued growth and investments are necessary in order for Vietnam to be competitive and for it to continue its rapid upward economic trajectory.

There are three central mechanisms by which data localization discourages digital economic investment and growth:

- By lowering — not raising — cyber security protections and standards for businesses and consumers;
- By impeding the free flow of data across borders, which is one of the fundamental foundations upon which the global digital economy is built and is a basic requirement for businesses to digitalize and stay competitive; and
- By running counter to international trade trends, therefore sowing uncertainty and doubt within the business community about whether Vietnam's regulatory ecosystem is a safe environment in which to invest.

The net negative impact on Vietnam's economy stands to be very substantial, with 61% of companies, including non-US companies, stating in a recent survey that they will be less likely to invest in Vietnam if data localization is mandated and 89% said the law would make Vietnam’s digital

economy less competitive.<sup>1</sup> Another study by the Brookings Institution highlights the potential significant economic impact of data localization in Vietnam:<sup>2</sup>

- Jobs: Reduce 146,000 jobs in Vietnam
- Sales: Wipe out USD 10 billion of business-to-customer (B2C) sales by 2020
- Growth: Missed USD 5.1 billion opportunity of increase in GDP from mobile Internet by 2020

Governments in the region, including Malaysia, Singapore, and Thailand, are supporting cross-border data flow and the use of cloud technology. Indonesia is likely to amend its regulations to allow for cross-border data flow. Australia and Japan are strong supporters of cross-border data flow at the regional and global level and in bilateral discussions. Given Vietnam's policies toward international economic integration and digital economy, as well as the Fourth Industrial Revolution, it is important that Vietnam follows international best practices to enhance its national competitiveness in comparison to other countries in the region.

#### **D. Data localization requirements impedes economically essential cross-border data flow**

While constructing data centers represents a one-time, large capital investment, forced localization of data may cause severe economic harm to Vietnam's economy by impeding the free flow of data upon which the global digital economy is built. In the digital economy, global services are underpinned by the free-flow of data. Everything from payments to email to shipping relies on data being allowed to flow freely across borders. As cited in a recent [CSIS report](#)<sup>3</sup> on data localization — “In an ever more connected world, we cannot expect data flows to remain confined within national borders. Moves towards data localization, or the Balkanization of the Internet, risk stifling the competition, innovation and trade which produce better services for consumers, and can weaken data security.” (according to “The Exchange and Protection of Personal Data: A Future Partnership Paper”. Her Majesty's Government, August 2017.)

Cross-border data access, usage, and exchange are essential to economic growth in the digital age. Every sector—including manufacturing, services, agriculture, and retail—relies on data and on the global flow of that data. Whether directly, or by indirectly taking advantage of global-scale data infrastructure such as cloud computing, global connectivity has enabled cross-border economic activity, allowing individuals, startups, and small businesses to participate in global markets.

Therefore, preventing the free flow of data:

- Creates artificial barriers to information-sharing and hinders global communication;
- Makes connectivity less affordable for people and businesses at a time when reducing connectivity costs is essential to expanding economic opportunity in Vietnam, boosting the digital economy and creating additional wealth;
- Undermines the viability and dependability of cloud-based services in a range of business sectors that are essential for a modern digital economy; and
- Slows GDP growth, stifles innovation, and lowers the quality of services available to domestic consumers and businesses. (A recent [report published by the Albright Stonebridge Group](#) examines these detrimental effects in detail.)<sup>4</sup>

Liberalizing Vietnam's framework on cross-border data flow would have outstanding positive impact on ICT development and economic growth generally. According to McKinsey & Company, global data flows have increased world GDP by approximately 3.5% over what would have occurred without

<sup>1</sup> <https://www.reuters.com/article/us-vietnam-socialmedia/vietnam-releases-cybersecurity-draft-decree-idUSKCN1N71XY>

<sup>2</sup> [https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy\\_meltzer\\_lovelock\\_working-paper.pdf](https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_working-paper.pdf)

<sup>3</sup> <https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/data-localization-free-all>

<sup>4</sup> <https://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf>

such flows, equivalent to USD 2.8 trillion dollars in 2014. Governments across the Asia-Pacific with the most advanced digital economies, as well as those that are prioritizing digital economic growth, are supporting the free flow of data. These governments include Singapore, Malaysia, Thailand, Japan, Australia, and Hong Kong SAR. It is important that Vietnam remain competitive with others in the region and adhere to international best practices.

Another study by the U.S. Chamber of Commerce<sup>5</sup> indicated that cross-border data flow liberalization would:

- Increase Vietnam's GDP by USD 3.46 billion
- Increase investment in Vietnam by USD 920 million
- Add USD 130 million in government revenue
- Create almost 73,000 new jobs in Vietnam

Additionally, the introduction of the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system and the General Data Protection Regulation (GDPR) in Europe suggest a global trend that privacy regulators are instead looking to facilitate the ability for organizations to engage in the free flow of data, subject to the boundaries set by similar cross-border transfer requirements. Also, it is important to note that the EU recently approved new rules on the “free flow of data” forcing EU countries to update national laws that currently prevent companies from moving data across borders in Europe. Global trade and industry bodies have likewise warned of the harmful effects to innovation, trade and economic development that data localization regulations can have on a country. The APEC CBPR system was developed by participating APEC economies after seeking the views of industry and civil society to build consumer, business and regulator trust in cross border flow of personal information. This comes after recognition by APEC that cross border online data flow are an integral part of today's international trade and governments are working on how to regulate this data flow to both promote e-commerce and protect consumers' data privacy.

#### **E. Data localization creates a Hostile Policy Environment for the Digital Economy and for Businesses in general**

While the technical challenges posed by mandatory data localization are significant, perhaps the worst long-term impact on Vietnam's economy will emerge from the signals sent to the business community. While the ICT sector will be the hardest hit and the fastest to decrease or withdraw investment in Vietnam, the impact will likely be broad-based over time.

Businesses looking to invest globally look for policy environments that are open, stable and optimized to enable growth. Much of the investment in Vietnam to-date was made on the assumption that the government would continue to provide a policy landscape that welcomes the vast majority of business activities and enables businesses to thrive; in particular, those activities focused on digital economic development.

In passing the law and publishing the accompanying Draft Decree, MOPS has sent concerning signals throughout the international business community about the ability to do business in Vietnam and many companies are now rethinking planned investments in Vietnam. If the final decree follows through with the data localization requirement, the resulting reputational damage will call into question the government's previously good-standing with businesses as a strong and trusted partner and will have a lasting impact on foreign direct investment.

The Draft Decree creates uncertainty and poses onerous requirements. While businesses may not be required to localize data immediately, they face the risk of being found to be non-compliant with the

---

<sup>5</sup> [https://www.uschamber.com/sites/default/files/022925\\_ict\\_reportflyer\\_vietnam2.pdf](https://www.uschamber.com/sites/default/files/022925_ict_reportflyer_vietnam2.pdf)

law by MOPS, upon which they would be subject to the data localization requirement or potentially need to pull out of Vietnam. The uncertainty caused by the data localization provision will most certainly deter many businesses from investing further in Vietnam. Businesses cannot/will not expand in an environment where they face daily existential risk. Fifth Era's [Report](#)<sup>6</sup> in 2016 bolsters our contention that data localization could undermine foreign investments. That is, 68% of investors surveyed responded they would hesitate to invest Vietnam if there would be data localization requirement and 76% of investors responded they would also be uncomfortable to invest if there would be local office requirement (see page 83, the Vietnam section).

#### **F. Data localization do not adequately serve the objectives of greater privacy protection and hinders technology adoption**

Many policymakers mistakenly believe that data is more private and secure when it is stored within a country's borders. This misunderstanding lies at the core of many data localization policies. However, in most instances, data localization mandates do not increase commercial privacy nor data security. Therefore, it is important to recognize that the confidentiality of data does not generally depend on which country the information is stored in, only on the measures used to store it securely. Data security depends on the technical, physical, and administrative controls implemented, regardless of where the data is stored.

The increased digitalization of organizations, driven by the rapid adoption of cloud computing and data analytics, has increased the importance of data as an input to commerce, impacting not just information industries, but traditional industries as well. Cloud computing uses Internet access and the ability to move data securely across borders to provide cheaper on-demand computing capacity. This includes basic cloud services such as email, software through to giving users direct access to processing, storage, and other computing resources in the cloud. This reduces the need for up-front investment in IT and the associated costs of maintaining often underused computing power. The benefits of cloud are best realized when there are no data localization restrictions placed on data. Such restrictions undermine the economies of scale as well as the security benefits to be gained from shared computing infrastructure.

It is also important to note that in a cloud computing environment, the distinction between data controller and data processor is important in practice. The data controller is responsible for implementing appropriate technical and organizational measures to protect the personal data under its control against accidental or unlawful destruction, accidental loss, alteration, and unauthorized disclosure or access and privacy protection. Where processing is carried out by a data processor on the data controller's behalf, the data controller is also responsible for choosing a processor that provides sufficient technical and organizational measures governing the processing to be carried out. The data processor typically has over-arching responsibilities with regard to protecting data (including protection from breach of their systems), particularly for protecting its network and infrastructure and ensuring the contractually specified reliability of its systems and availability of data it processes.

Data localization requirements do not adequately serve the objectives of greater privacy protection and regulatory oversight. Privacy protection is best addressed by requiring a data controller to locate data only in jurisdictions with similar legal protections. This is the approach taken by most jurisdictions. Learning from such practices, we propose not establish blanket data localization norms — neither for data controllers nor for data processors. Therefore, the Draft Decree should be flexible to enable innovation and the benefits of new technologies for society and business and economic growth.



**Recommendations:**

- We highly recommend that the drafting authority remove any data localization requirement.
- Given that MOPS is looking to enhance cyber security within its own systems, as well as for local businesses and the Vietnamese people broadly, there are measures MOPS should consider which can significantly enhance Vietnam's cyber defense capabilities. For example, working with companies and law enforcement agencies across borders to ensure legal and speedy access to data by relevant authorities.
- Although Vietnam has entered into side agreements with some countries to suspend dispute settlement under CPTPP for five years, a government decree, which is expected to be valid for years, should be consistent with Vietnam's commitments under international agreements. In addition, WTO requirements are currently in effect with no waiver. Therefore, we recommend revising the law on cybersecurity to signal international trade readiness.

#### **4. Requirements on locating data, establishing branches or representative offices in Vietnam (Article 25)**

##### **A. Requirements on data localization**

As mentioned earlier, we recommend that MOPS review the feasibility of this requirement and its consistency with Vietnam's commitments under CPTPP, when it is applicable to foreign cross border service providers.

As for domestic service providers, Article 25.1 should be clearer on whether the subject must meet all of the conditions stipulated under Article 25.1 or only one of them. For instance, it is understood that they must meet all the conditions under sections (a), (b), (c), (d) of Article 25; but there are various items under each section. For instance, Section 1.b stipulates the condition of "*having the activities of collection, exploitation, analysis, processing data ...*". Should it be understood that the subjects to this requirement must have all the activities at the same time? What if they only do one or some of the activities such as collection and/or exploit, but not analysis and processing of the data?

Article 25.1.c provides the condition of "allowing the users to undertake the acts stipulated under sections 1, 2 of Article 8 of the Law on Cybersecurity". However, some digital service providers merely provide Internet platforms for the users. They cannot control the actions or compliance of the users with the law. Therefore, these platforms should not be held responsible or punished for their users' violations. For instance, an electronic mail service provider should not be responsible for what their users write in their emails. Furthermore, we are wondering how it would be technically possible to determine whether the service providers "allow" or "do not allow" the users to undertake the acts under the Article 8.1 and 8.2 of the LOCS and whether its users must violate both sections 1 and 2 of the Article or only one of them to satisfy this condition.

**Recommendation:** We recommend that this requirement is removed.

##### **B. The requirement on establishment of branches or representative offices in Vietnam**

The scope of this provision in the Draft Decree ignores the benefits of global business models. The requirements to set up local branch or representative offices in Vietnam will create undue burden for foreign businesses, especially those whose business scale in Vietnam is small, but are looking to expand. The establishment of branches or representative offices of a business entity should be decided by the business themselves based on the business needs rather than as an imposed remedy against a violation. This requirement is against the business nature and create unnecessary cost burdens for businesses.

This requirement will make Vietnam become unique in forcing foreign businesses to establish representative offices or local branches for the purpose of cyber security, as legitimate cyber security concerns can be addressed without the imposition of such a localization.

**Recommendation:** We recommend that this requirement be removed.

## 5. Definition of information systems critical to national security

The criteria that is used to determine whether an information system is a critical system is very general while the obligations and requirements are substantive. In addition, the Draft Decree fails to clearly specify that the draft list only covers information systems of state authorities which was previously confirmed by the drafting authority. In addition, we understand that during the meeting between MOPS and the Vietnam Business Forum on 13 September 2018, representatives of MOPS verbally confirmed that the List of Critical Systems will only include information systems of state authorities. However, the Draft Decree clearly does not reflect such intention.

**Recommendation:** If the List of Critical Systems is indeed meant to only include information systems of State authorities, we would recommend that the Draft Decree include a provision to reflect this intention.

This consultation is of significant importance and highlights that Vietnam is gearing to strengthen its digital economy. However, the provisions in the Draft Decree could be a bottleneck. AIC has identified that data localization laws raise many uncertainties and have affected and continue to affect many multinational businesses, and industry in general.

Taken in its totality, mandatory data localization and requirement on establishment of branches or representative offices in Vietnam will have a **bottom line impact**, that will not only drain Vietnam of significant amounts of investment, negatively impact GDP, but also handicap Vietnam's digital economy and cost Vietnamese people jobs. Maintaining Vietnam's current posture and continuing to support the free flow of data across borders stands to bring with it significant economic gains.

If written without mandatory data localization requirements, Vietnam's LOCS has the potential to promote a strong cyber security ecosystem and encourage trade and foreign direct investment. We strongly suggest MOPS to engage and leverage the expertise of stakeholders across the Vietnamese government and the international community to align with proven cyber security best practices, promote trade and investment, honor Vietnam's trade commitments and ultimately reduce the risk posed by cyber threats.

AIC reiterates its view that the data localization requirement be replaced with a suitable cross-border transfer mechanism. This approach is aligned with the sentiment of global trade and industry bodies, as well as the approaches taken by the majority of privacy regimes globally and this alignment will put the Vietnam regulatory environment in good stead to facilitate innovation, a more cohesive approach to data management and, ultimately, the growth of industry and economy in Vietnam.

We would like to continue to work with MOPS to provide industry-led solutions to shared cyber security concerns. We urge MOPS to ensure that the practical compliance requirements set out in the Draft Decree for businesses (both based in Vietnam and internationally) are clear and not disproportionately burdensome and harmful.

Thank you for providing this opportunity to participate in the consultation and we hope that our recommendations will be considered to support Vietnam's digital economy goals. We look forward to discussing this submission and will respond to any further questions, via email or in person.