8 August 2017

Respectfully to: Ministry of Public Security
Hanoi, Vietnam

Attention: Senior Lieutenant General To Lam
The Minister

Joint Industry Comments on Draft Law on Cybersecurity

The American Chamber of Commerce Hanoi, BSA | The Software Alliance, The Computing Technology Industry Association (CompTIA), DIGITALEUROPE, The Information Technology Industry Council, The Japan Electronics and Information Technology Industries Association (JEITA), The Semiconductor Industry Association, The US-ASEAN Business Council, and The U.S. Chamber of Commerce write to express our sincere gratitude to the Ministry of Public Security ("MoPS") for the opportunity to submit comments on the Draft Law on Cybersecurity ("Draft Law").

We strongly support Vietnam's efforts to establish a legal framework on cybersecurity. Network systems today underpin many critical systems, and as such, need to be adequately protected against cyber threats. Similarly, the increasing dependence on information and communication systems raises the importance of ensuring public confidence and trust in the security of the underlying infrastructure. Users must know that their data will be properly managed and secured by the best available technologies. It is also important to acknowledge that the benefits of the digital economy can be offset by the cost of cyber-attacks and cybercrime, unless the online environment is adequately protected. A clear need exists for a national cybersecurity strategy that encourages defenses that are proactive, intelligence driven, and capable of protecting against a broad threat spectrum.

Our members are global and, as such, have experience with dozens of national approaches aimed at addressing cyber risk. This background has afforded our members a sophisticated understanding of what makes for an effective national cybersecurity approach, and in this submission, we seek to offer constructive feedback on what we believe are unclear, or even potentially harmful, provisions in the Draft Law.

Our comments, laid out in detail below, can be summarized by the following points:

1. **The scope of the Draft Law is too broad.** We recommend that the Draft Law should be generally limited to maintaining the security of network and information systems.
2. **The Draft Law would potentially impede the digital economy in Vietnam**. The uncertainty and the potential liabilities imposed on companies may dampen innovation in the provision of internet services and, on a wider scale, the growth of the digital economy in Vietnam.

3. **The Draft Law will increase the difficulty and cost of doing business in Vietnam**. The requirements set out in the Draft Law, particularly those related to data storage, threaten to increase the costs of doing business in Vietnam, for both foreign and local enterprises. Small and medium enterprises (SMEs) in particular will be more negatively impacted as they have lesser resources to comply with data storage requirements and the potentially rigorous licensing, audit, and compliance requirements.
4. **The Draft Law may be inconsistent with WTO commitments**. The application of vague appraisal procedures may constitute unnecessary technical barriers to trade or domestic regulations which are inconsistent with Vietnam's WTO commitments. We urge the Government to revisit the provisions highlighted below and align them more closely with international practices.
5. **Criminal liability should be reserved for actors with malicious intent**. The breadth of the Draft Law, the vagueness of certain of its provisions and the absence of guidance as to which provisions attract criminal liability add to the uncertainty of the law's implementation and fears that it could be arbitrarily applied. Securing the online environment today is a complex process that does not come with 100% guarantees. Criminal prosecution should therefore be reserved for those seeking to destabilize the environment and not those who are the victims of such malicious activity. We urge the government to omit the provisions related to criminal prosecution or to limit their application to actors with clearly malicious intent.
6. **Effective cybersecurity practices are iterative in nature and focused on risk**. The Draft Law places a large emphasis on ex-ante measures to ensure that systems are secure. This requires industry to divert a large proportion of their resources towards averting a single, static vulnerability, and away from myriad evolving threats which are the source of most cyber-attacks. Instead, cybersecurity efforts should be premised on a risk-management based approach. This includes an outcome-focused methodology and the assessment of risk by identifying threats, vulnerabilities, and consequences, then managing these risks through mitigation measures, controls, costs, and similar measures.
7. **Cybersecurity is best when embedded in global and industry-driven standards.** Standards and best practices are optimally led by the private sector and adopted on a voluntary basis, and most effective when developed and recognized globally. Rather than building out a set of risk management practices from scratch, utilizing tried and tested methods developed by industry and adopted internationally provides governments with a valuable starting point, helping to quickly raise the level of ecosystem cybersecurity, gaining compliance efficiencies, and creating opportunities for shared learning and exchange. International policymakers should align ex-ante measures with industry-backed approaches to risk management, such as the ISO/IEC 27000 family of information security management systems standards or the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*.
8. **Data Localization requirements will only hurt Vietnam and Vietnamese consumers**. The Draft Law requires personal information and critical data to be stored within Vietnam. Data localization will limit Vietnamese consumers', enterprises', and government agencies' access to services and technology rely on international transfers of data (e.g. cloud based services, fraud tools).
9. **The private sector should not be required to proactively monitor or manage internet activity.** While industry is willing to work with the government to respond to clear attempts to use the

Internet to facilitate or conduct malicious activity, it is neither feasible nor desirable for industry to monitor and manage all internet activity.

We thank the Government of Vietnam and the Ministry of Public Security for addressing cybersecurity issues, and for undertaking a transparent and inclusive consultation process. We hope to continue to engage with the Ministry as the Draft Law and its implementing regulations are finalized.

We respectfully submit the attached paper which explains our concerns in greater detail, seeks clarification on several provisions, and offers recommendations on policy approaches that will help advance the underlying objectives of this bill.

Our organizations stand ready to work with your government in pursuit of this goal and would welcome a meeting with your Ministry to further discuss our concerns and to propose alternative approaches that would better ensure the security of Vietnam's critical systems.

We thank you for considering our views.

Detailed Comments on Specific Articles on the Draft Law on Cybersecurity

Article	Summary of Content	Comment
Article 1	Scope of the Draft Law.	As written, the Draft Law is incredibly broad, and captures almost every activity and business using information and communications technology. Unfortunately, the highly prescriptive approach outlined in the Draft Law will ultimately make it more difficult for the Government to secure its most important assets. As outlined below, we recommend a number of specific revisions aimed at narrowing the focus of the Draft Law. As a general matter, we also urge the Government of Vietnam to keep the Draft Law narrowly focused on cybersecurity (i.e., maintaining the security of networks and information systems), and to avoid delving into data protection, privacy, cybercrime, and content regulation issues. Indeed, the inclusion of such issues (which as discussed below, are largely covered by existing regulations) threatens to divert much needed attention from the need to address cybersecurity in its traditional formulation. Finally, when considering comparable laws of other countries[1], we are concerned that the Draft Law may ultimately undermine the Government of Vietnam's goal of aligning domestic cybersecurity tasks with international practices and assuring the conditions for international integration in cybersecurity. As detailed below, aspects of the Draft Law deviate from

[1] Japan's Basic Act on Cybersecurity defines cybersecurity as necessary measures that are needed to be taken to safely manage information ... and to guarantee the safety and reliability of information systems and information and telecommunications networks;
Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive") "lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market."
Korea's National Anti-Cyberterrorism Act defines Cyber Security as measures and responses through administrative, physical, technological means in order to protect information telecommunication infrastructure and information from cyber terrorism, and includes cyber crisis management.
The Cybersecurity Act of 2015 of the United States defines "cybersecurity purpose" as the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

		international norms and best practices in ways that could limit the availability of cutting edge cybersecurity services in the Vietnamese market.
Article 3	Definition of terms.	In general, the definitions in the Draft Law lack clarity. Moreover, we would strongly recommend aligning the definition with those used in tried and tested national frameworks around the world. Such an approach would allow the Government to more easily exchange information with its international partners. With that in mind, we recommend that the following definitions be rephrased as: • *Cyber space* is defined as a digital environment, enabling the creation, processing, and exchange of information, created by information systems and services and electronic communication networks. • *Cybersecurity (and cybersecurity protection)* is defined as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: o integrity, which means guarding against improper information modification or destruction, and includes ensuring nonrepudiation and authenticity; o confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and o availability, which means ensuring timely and reliable access to and use of information. • *National information infrastructure* is defined as information and information systems that are owned, operated, controlled, or licensed for use by, or on behalf of, any government department, including information systems used or operated by another entity on behalf of a government department. • *Information systems critical to the national security* is defined as systems and assets, whether physical or virtual, so vital to the country that the

		incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. • *Cyber-attack* is defined as action that may result in unauthorized access to, exfiltration of, manipulation of, harm of, or impairment to the integrity, confidentiality, or availability of an information system or information that is stored on, processed by, or transiting an information system. • *Cyber products and services* are limited to those products, goods, or services intended to detect, mitigate, or prevent cybersecurity threats. • *Cybersecurity threats* are defined as any actions that may result in unauthorized access to, exfiltration of, manipulation of, harm of, or impairment to the integrity, confidentiality, or availability of an information system or information that is stored on, processed by, or transiting an information system. • *Cybersecurity threat indicator* is defined as: o malicious reconnaissance, including anomalous patterns of communications that reasonably appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat; o a method of defeating a technical control; o a technical vulnerability; o a method of defeating an operational control; o a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a technical control or an operational control; o malicious cyber command and control;

		○ the actual or potential harm caused by an incident, including information exfiltrated as a result of defeating a technical control or an operational control when it is necessary in order to identify or describe a cybersecurity threat; ○ any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or ○ any combination thereof; and ○ from which reasonable efforts have been made to remove information that can be used to identify specific persons unrelated to the cybersecurity threat. • *Cybersecurity incident* is defined as an occurrence that actually, or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. • Delete *information on cyberspace and cyber information safety* as they are duplicative terms. • Delete *digital accounts* section, as it extends the scope of the draft Law too broadly, making it impossible for the Government to focus on protecting its most critical assets.
Article 5	Cybersecurity protection principles	In addition to the principles currently identified in Article 5, we recommend that the Government of Vietnam clarify that cybersecurity efforts should be premised on a risk-management based approach. Consistent with such an approach, the Government of Vietnam should also recognize the following principles: • Risk-based approach: Assess risk by identifying threats, vulnerabilities, and consequences, then manage risk through mitigation measures, controls, costs, and similar measures;

		• Outcome-focused methodology: Focus on the desired end state, rather than prescribing the means to achieve it, and measure progress towards that end state; • Prioritized scope: Adopt a graduated approach to criticality, recognizing that disruption or failure are not equal among critical assets or across critical sectors; • Practicable policies: Optimize for adoption by the largest possible group of critical assets and implementation across the broadest range of critical sectors; and • Globally relevant results: Integrate international standards to the maximum extent possible, keeping the goal of harmonization in mind wherever possible.
Article 10.1-2	Prohibited acts include: (1) *'The use of cyberspace to prejudice the national sovereignty, interests and security, or the social order and safety.* (2) *Posts, preparation and dissemination of information on cyberspace prejudicial to the legitimate rights and interests of organisations or individuals, or contrary to the morality or the fine customs and practices or against the State of the Socialist Republic of Vietnam.'*	In an effort to narrow the scope of the law, we strongly recommend that cybercrime and content regulation related issues be addressed through a separate legislative instrument. The language below contains a wide definition of what would prejudice the national sovereignty and/or morality. Should the Government retain this provision, we would suggest a more limited definition that is focused on cybersecurity-related harms, as opposed to content regulations.
Article 12.1-2	The handling of violations *(1) 'An individual violating legislation on cybersecurity shall, subject to the nature and severity of such violation, be*	This article provides that violations of the law may be subject to criminal prosecution, but does not specify which breaches would be deemed criminal. As noted above, the Draft Law deals with an overly broad subject matter well beyond what is traditionally in the sphere of cybersecurity. The broadness of the Draft Law, the vagueness of certain of its provisions and the absence of

	disciplined, administratively sanctioned, or subjected to a criminal prosecution; where any damage is caused therefrom, shall compensate therefore in accordance with legislation. (2) Organizations violating legislation on cybersecurity shall, subject to the nature and severity of such violation, be administratively sanctioned, or subjected to suspension of operation; where any damage is caused therefrom, shall compensate therefore in accordance with legislation.'	guidance as to which provisions attract criminal liability add to the uncertainty of the law's implementation and fears that it would be arbitrarily applied. In any case, we recommended that criminal liability should be imposed only on parties that intentionally and maliciously bring about a violation of law. There are, for example, administrative requirements for which the imposition of criminal penalties to address breach would be too harsh. Likewise, there are strong concerns about the use of administrative sanctions or suspension of operations. Greater clarification as to what criteria will be assessed when deciding whether to take such measures would be welcome.
Article 13.1	Criteria for classification of an information system as critical to national security. *'Information systems critical to national security shall be identified based on how critical they are to national security and the social order and safety, and the extent of possible consequences or damages when they are encroached upon:* *a) Affecting national sovereignty, interests and security.* *b) Seriously affecting social order and safety.* *2. Information systems critical to national security shall include* *a) Information systems serving the protection of national security;* *b) Information systems processing State secret information;* *c) National information systems serving the development of e-government;* *d) Information systems of finance, transportation and chemical sectors;*	Industries deemed "critical to national security" are subject to a range of highly prescriptive and resource intensive requirements. Unfortunately, the criteria for determining which systems will be subject to these heightened cybersecurity standards and audits (Articles 14-18) are both broad and vague, potentially giving the MoPS unrestricted access to and control of large segments of the economy. Rather than designate entire sectors of the economy as "critical," it is important to delineate those services which are vital to the functioning of Vietnamese society and those that are not. We highly recommend that the government revisit this section and narrow the focus of the legislation to "systems and assets, whether physical or virtual, so vital to the country that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The requirement for whole industries to adhere to the heightened cybersecurity standards and audits (Articles 14-18) will find the resources required to be significant, particularly for small and medium enterprises (SMEs).

	đ) Automatic control and supervision systems in key national works, and targets critical to national security; *e) Information systems serving radio, television, newspapers and publishing;* *g) Information systems serving concentrated data storage in respect of any type of national critical information and data;* *h) National information infrastructure systems for the purpose of interconnecting Vietnamese and international operations.'*	It is suggested that the law imposes obligations that are commensurate to the nature of the industry, lest these requirements have an inadvertent effect of creating disincentives to digitizing certain businesses. The classification of "finance" is too broad, as financial services such as insurance should not be considered "critical to the national security". The reference to finance should be modified by adding 'exclusive of insurance, re-insurance and social insurance'. We also seek greater clarity on whether freight forwarding, express delivery services, and postal services are considered to be "national key industries and sectors," as well as whether "transportation" also encompasses goods transportation services.
Article 13.2 h):	*'Information systems critical to national security shall include h) national information infrastructure systems for the purpose of interconnecting Vietnamese and international operations.*	The provision on information systems critical to national security that includes "national information infrastructure systems for the purpose of interconnecting Vietnamese and international operations" is too broad. This covers all international interconnection – commercial and/or non-commercial, public and/or private – and creates unnecessary business burden. The provision should be narrowly defined such that commercial non-critical interconnection is excluded.
Article 17	Cybersecurity audit and assessment requirements	The Government of Vietnam should include the choice of third-party audits in the Draft Law to ensure that the quality of audits is based on international auditing standards and practices.
Article 17.2 a) and b)	*'Cybersecurity audits and assessments in respect of the information systems critical to national security shall be based on:*	Clarification as to what requirements must be met during an audit is absent from the Bill, making it hard for companies to comply with the new regulation. We recommend that such requirements be focused on ensuring that products and services are designed with security in mind, rather than on measuring their security at any static moment in time. The government should be wary of reliance on mandatory ex-ante audits of software or hardware as a means of increasing cybersecurity. Because modern technologies are often updated on a weekly (and occasionally daily) basis to ensure they are protected against the latest threats, an ex-ante audit

		provides very little insight into the security posture of a product or service. At the same time, such audits add to the cost of cutting edge security technologies and can delay their market availability.
Article 17.4-5	(4) '*The owners of the information systems critical to national security shall carry out cybersecurity audits and assessments at least once a year and frequently audit when the cybersecurity condition may affect the information systems administrated by them.* *(5) The Ministry of Public Security shall take the main responsibility for, and coordinate with the Government of Cipher Commission in audit and assessment of cybersecurity of the cipher communication networks.'*	Whereas Article 17.4 permits the owners of information systems critical to national security to perform audits on their own systems, Article 17.5 requires that audits involving "cipher communication networks" be performed by the the MoPS. However, the Draft Law does not define the term "cipher communication networks" nor establish the objective criteria by which such audits will be performed. Vague review / appraisal procedures may result in non-transparent procurement procedures and discrimination between offshore suppliers and domestic suppliers. Additionally, the application of vague appraisal procedures may constitute unnecessary technical barriers to trade or domestic regulations which are inconsistent with Vietnam's WTO commitments. We recommend adding text that would state the review will not discriminate against products and services outside of Vietnam, either intentionally or by adopting requirements that have a disproportionate impact on non-Vietnamese companies, except insofar as such requirements have a demonstrable effect on increasing security.
Article 18.3	*'When any incident occurs, the owners of information systems critical to the national security shall in a timely fashion give notices to, and coordinate with, the Ministry of Public Security…'*	Seek clarification on the threshold for "*any incident*". We recommend that the Government of Vietnam limit the obligation under Article 18.3 to "significant cyber incidents" resulting in: a) the exfiltration of data that is essential to the operation of critical cyber infrastructure; or b) the defeat of an operational control or technical control, essential to the security or operation of critical cyber infrastructure. We likewise recommend that the obligation to report significant cyber incidents to the MoPS be limited to critical infrastructure operators alone, and

		that IT providers report any cyber incidents directly to their clients, in line with their contractual obligations.
Article 18.4	*'The Minister of Public Security shall give status notices in respect of cybersecurity incidents, and temporarily limit the operation of the information systems at certain areas when necessary.'*	The resolution of cybersecurity incidents should be led by organizations themselves, which have the necessary expertise, without forced intervention by the government.
Article 19.6	*'Telecommunication, internet information technology, and cybersecurity services providers shall be responsible to coordinate with the cybersecurity specialized agencies in cybersecurity monitoring in order to protect national security and social order and safety.'*	We recommend that the obligation requiring companies to monitor systems be limited only to extreme circumstances. We also recommend that the parameters of such engagement should be more clearly defined and done in a targeted manner that limits the impact on privacy interests. Additionally, to the extent companies are required to monitor in those limited circumstances, they should also be provided adequate liability protections.
Article 23	*'Where necessary, the Ministry of Public Security shall make a proposal to the Government on the suspension of the provision of cyber information at certain areas for the purposes of responding to and remedying any cybersecurity incidents to protect national sovereignty, interest, and security and to secure social order and safety.'*	As with Article 18.4, the resolution of cybersecurity incidents should be led by organizations themselves, which have the necessary expertise, without forced intervention by the government.
Articles 24-27	The development of standards and technical regulations on cybersecurity	Given the inherently global nature of the ICT industry, the development of country-specific standards creates a risk of limiting the availability of best in class security offerings. Articles 24-27 should be clarified to encourage reliance on global information security standards that are based on consensus industry processes. We would also caution against overreliance on certification and product testing. The rapid pace of technological and online threat innovation means

		that some of the inherent challenges posed by static certification frameworks have become more acute: ▪ **Cybersecurity is not static**: By its definition, certification implies a rigid system that works well for products that do not change once installed. With new technologies, such as cloud computing, that is no longer possible. New features get added continuously, oftentimes improving the security of a particular product or service. Moreover, because certification frameworks can take years to develop, they frequently entrench older technologies rather than encourage adoption of the latest and most secure products and services. ▪ **A one-size-fits-all approach cannot work for a diverse ICT ecosystem:** Not all technologies are the same, nor are all technologies created equal. Certification frameworks therefore need to distinguish between the different products and services, from Internet of Things to cloud computing, as well as to acknowledge that each technology has its own set of risks, security and network challenges. Security requirements and risk management approaches therefore also need to differ. ▪ **Certifications can create a false sense of security:** Although well intentioned, certification risks creating a false sense of security for consumers and enterprises, since they rarely provide meaningful information about security. It can also encourage a compliance focused approach to security rather than encouraging wholistic cross-organizational risk management approaches. ▪ **Certification can involve considerable costs**: Creating certification frameworks imposes a high costs and time commitment on both the government, who must maintain the certifications, and the private sector, where small and medium sized businesses in particular can struggle to navigate the often complicated compliance processes. ▪ **Cybersecurity is a global issue**: Cybersecurity challenges cut across national jurisdictions and a global approach is required to solving them. When countries take different regulatory approaches, gaps can be

		created that may lead to further vulnerabilities in the system, or overlaps that can misrepresent security. Leveraging existing certification systems that have proven to work will help increase market efficiency, boost innovation, and help smaller companies compete on the market.
Article 24	'*1. The State encourages agencies, organizations and individuals to develop standards and technical regulations on cybersecurity, and participate in protection of cybersecurity in accordance with legislation.* *2. The Ministry of Public Security shall take the main responsibility for and coordinate with the relevant agencies in the development of draft national standards on cybersecurity, and propose the appraisal of, and announce national standards on cybersecurity; take the main responsibility for the development of, and promulgate national technical regulations on cybersecurity in accordance with legislation.* *3. The Ministry of Science and Technology shall take the main responsibility for and coordinate with the relevant agencies in organizing the appraisal and announcement of national standards on cybersecurity; and appraise draft national technical regulations on cybersecurity in accordance with legislation.'*	We strongly recommend that the Government of Vietnam rely on cybersecurity standards that are consistent with global cybersecurity standards. Global companies should be encouraged to implement 'best in class' cyber security standards across jurisdictions, such as the ISO/IEC 27000 family of information security management systems standards or the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity,* rather than diverting resources towards compliance with fragmented regulatory regimes.
Article 26	The assessment of compliance with standards and technical regulations on cybersecurity	This article mentions the recognition of third party standards/certifications. An explicit reference to using international standards would be helpful here.
Article 27.1.d	Cybersecurity assurance requirements for cyber products and services	It should be made clear that the exact nature of the flaw does not need to be made public – as this may tip off criminals to new attack vectors.

	'When any cyber product or service is found to have any security error or flaw, actions shall be taken to remedy consequences, a timely notice shall be given to its users, together with a report being submitted to the relevant State authorities.'	Vulnerabilities ("security errors or flaws") in cyber products/ services are to be reported to users and authorities (31.1d). However, there are already mature industry-wide approaches at the global level for vulnerability disclosure. This requirement should be removed or framed along the lines of a requirement on vendors to have a security vulnerability policy and publish advisories.
Article 27.1.dd	Cybersecurity assurance requirements for cyber products and services *'Cyber products and services having the function of collecting user information shall be indicated, the users shall be informed of such function and the consents of the users shall be required.'*	Clarification is needed to better define the instances where consent is required, how consent can be obtained, and whether responsibility for obtaining consent falls on the deployer/customer of the cyber product/services and not the vendor.
Articles 28-33	Business licenses for cybersecurity assurance services	Articles 28-33 create stringent business license requirements for a broad range of cybersecurity service providers. By limiting the availability of such licenses to companies that are "duly incorporated and operating in Vietnam" (Art. 30.1(a)) these provisions will limit access to the Vietnamese market for many international companies that offer cutting edge cybersecurity services. These provisions also limit local organizations and businesses from engaging international professional service providers to secure their systems, leaving information systems in Vietnam unnecessarily exposed and vulnerable to cybersecurity incidents. The draft bill does not indicate whether cybersecurity services can be provided on a cross-border basis. Unless international organizations are able to compete in the Vietnamese market, a number of credible entities will be prevented from providing services within Vietnam. These provisions may also create overlaps with the Law on Information Network Security (LOINS), which has been enacted since 2016 and includes licensing requirements for information security services as well. It is unclear

		whether those enterprises which have already been licensed under the LOINS will be exempt from this licensing requirement.
Article 34	*2. 'Measures for handling information contents on cyberspace inciting mass gathering that disturbs security and order:* *a. Require the involved organizations and individuals to remove or correct their information;* *b. Prevent and delete the information;* *c. Temporarily suspend, suspend, or revoke the operating license for posting the information.* *d. Investigation and sanctioning under legislation.'* *3. 'Telecommunication and internet service providers and information system owners shall be responsible to closely coordinate with the competent authorities in handling the information contents in cyberspace that incite mass gatherings disturbing the security and order.'*	To clarify the scope of obligations under Article 34, the Government of Vietnam should provide additional detail about the legal process under the Draft Law for addressing law enforcement issues and government requests. Consistent with international practice, Article 34 should provide for judicial oversight of law enforcement requests for the removal of content. With respect to Article 34.2(b), orders requiring online service providers to "prevent or delete" offending content should identify specific content, and not create a generalized obligation to monitor for potentially unlawful content. Service providers should not be required to remove (or otherwise "prevent" the posting of) content in the absence of a specific court order. Current regulations, primarily Decree No. 72/2013/ND-CP, set out what are deemed to be prohibited acts in relation to the provision and use of Internet services. The list of prohibited acts under this decree already suffers from overbreadth and vagueness. The Draft Law does little to address the uncertainties brought about by Decree No. 72, and instead, in Articles 7 and 10(2), contains even broader and vaguer provisions as to what constitutes prohibited content. Likewise, existing regulations (Decree No. 72/2013/ND-CP and the Law on Telecommunication) define the terms "internet services" and "telecommunications service," respectively. We seek confirmation that the terms used in the Draft Law are to be understood in accordance with the existing definitions.
Article 35	Handling of information contents in cyberspace prejudicial to the legitimate rights and interests of organizations and individuals, or contrary to the morality or the fine customs and practices, and against the State of the Socialist Republic of Vietnam	Article 35 requires enterprises to put in place technical measures to *prevent* the display of information that violates a wide-ranging definition. This language places an undue burden on companies to restrict freedoms of speech and expression, as well as holding companies accountable for the actions of individual users.

	Including the requirement that (art. 35.4) *'Information system owners and telecommunication and internet service providers shall be responsible to put in place technical measures to prevent the displaying of, and delete, any information in cyberspace… against the State of the Socialist Republic of Vietnam.'* Including the requirement that (art. 35.5): '*The Ministry of Public Security shall take the main responsibility for, and coordinate with the Ministry of Information and Communications in, taking technical measures and other necessary ones to prevent the spread of any information in cyberspace prejudicial to the legitimate rights and interests of any organizations or individuals, contrary to the morality or the fine customs and practices, or against the State of the Socialist Republic of Vietnam.'*	Current regulations, primarily Decree No. 72/2013/ND-CP, sets out what are deemed to be prohibited acts in relation to the provision and use of internet services. The list of prohibited acts under this decree already suffers from overbreadth and vagueness. The Draft Law does little to address the uncertainties brought about by Decree No. 72, and instead, in Articles 10 and 35(2), contains even broader and vaguer provisions as to what constitutes prohibited content. This uncertainty and the potential liabilities imposed on Internet service providers would tend to dampen innovation in the provision of Internet services and, on a wider scale, the growth of the digital economy in Vietnam. Finally, the definition of '*technical measures and other necessary ones'* is unclear. Clarification that this will not require companies to reveal confidential and proprietary technical information of the hardware and/or software would be welcome.
Article 36.3 a) and b)	*'The Ministry of Public Security shall be responsible to:* *a) audit and assess cybersecurity in respect of communication equipment, products and services, digital and electronic devices before they are put into use in any State agencies;* *b) audit and assess cybersecurity in respect of information systems critical to the national security in order to detect and remove any malicious codes, to repair any security*	Ensuring the security of ICT products used by state agencies is critical. However, efforts to enhance cybersecurity that inadvertently hamper the development, deployment and use of the best available technologies will harm innovation and perpetuate *insecurity*. It is therefore important that the Draft Law clarify that audits performed in connection with Article 36.3 are designed to be minimally invasive, respect personal, sensitive, and/or proprietary information (e.g. trade secrets), and are subject to oversight to minimize abuse. The Draft Law should also clarify that assessments should be based on technology neutral technical specifications and not on the brand,

	vulnerabilities, and to prevent and handle any illegal intrusions; *f) inspect and examine the protection of State secrets in cyberspace by the state agencies and the protection of cybersecurity by the owners of information systems critical to the national security;'*	licensing models, business models, or country of origin of the products or services deployed. The vagueness of these provisions – lacking details on "audit and assess," "inspect and examine" equipment, products, devices and systems creates concerns that companies will be forced to reveal proprietary product technical information in the name of cybersecurity audits. It is critical for the Government to clarify what they plan to audit and assess and what standards the industry providers will have to align to. Moreover, it would be important that the Government aligns to international best practices in this space and accepts proof of cybersecurity audits developed by international organizations. Furthermore, for example the Network and Information Security Directive in Europe only requires post-factum audits – after a security breach has already taken place. Given the cost in time and resources to both industry and government, we strongly encourage that approach to be considered. Furthermore, we strongly encourage the Government to revise or omit section b). Although the inspection might indeed result in discovery of a vulnerability, the Government should communicate such information to the vendor in question to ensure they repair it rather than acting on its own. Finally, there is no definition of what categories of information would be classified as "State secrets." We encourage you to provide greater clarification.
Article 37.2 and 37.4	*'Subject to their respective functions, mandates, powers and responsibilities, agencies, organisations and individuals shall apply measures to identify the origin of cyberattacks in accordance with legislation.'* *'Information system owners shall take any actions allowed by legislation to prevent or eliminate cyberattacks on the information*	Given the difficulty associated with accurately identifying the origin of cyberattacks (attribution), greater clarification is needed as to what is required of companies and individuals under this article. Although the industry is broadly supportive of efforts to attribute the source of attacks, it is important to note that only a small subsection of the industry has effective capabilities in this area. To the extent this provision directs companies to focus on attribution, scarce resources may be diverted from the more important tasks of protecting their

	systems administered by them, and be responsible to coordinate with the specialized agencies in charge of cybersecurity protection in identifying the exact origins of such cyberattacks.'	systems against cybersecurity incidents in the first place, and effectively responding to and mitigating such incidents after they occur.
Article 37.5	*'When there appear any cyberattacks prejudicing the national sovereignty, interests and security on cyberspace, the specialized agencies in charge of cybersecurity protection shall require telecommunication and internet service providers to block or filter information in order to prevent and eliminate such cyberattacks and provide in a timely manner adequate related information and documents.'*	Mitigating cyberattacks at the Internet service provider level is a highly complicated, costly, and cumbersome process. In many instances, it may not be possible for organisations to block or filter information. As such, organisations should not be required under law to conduct activities which are beyond their ability to complete. There are a variety of means to respond to cyberattacks, which are constantly evolving, just as are the cyberattacks themselves. Mandating blocking and filtering, which may not be practical or preferred means to address cyberattacks should not be written into the Law.
Article 38.2	*'Any agency, organization or individual shall regularly review, inspect and assess cybersecurity to eliminate threat of cyberterrorism.'*	It is unclear whether Article 38.2 is intended to create audit and assessment criteria beyond those outlined in Article 36.3. If so, further clarification regarding the nature of the assessment and who would be subject to it is needed.
Article 38.3	*'Any agency, organization or individual, when detecting any sign or act of cyberterrorism, shall promptly report it to the nearest public security body.'*	Clarification on the definition of 'nearest' public security body would be welcome.
Article 39.3	*'When a cyberwar is likely to occur or occurs, each of agencies, organisations and individuals shall, subject to its functions, mandates, powers and responsibilities, proactively take cybersecurity protection measures and protect the information systems administered by it.'*	We appreciate that the Government of Vietnam is taking a forward-looking approach to preventing the escalation of conflicts in cyberspace. As part of this effort, we would encourage the Government to engage with its global trading partners in the development of norms to define the boundaries of appropriate nation state behaviour. In our view, the development of such norms is a critical element to avoiding the outbreak of "cyberwar."

		However, given that the concept of "cyberwar" remains uncertain in the international arena, and in the situation of a war (involving Cyberspace), use of conventional cybersecurity approaches may not be adequate or relevant, we suggest this topic to be treated separately under separate legislature if such legislature is required. Cybersecurity is an ongoing, iterative process in which new threats are identified and steps taken to mitigate them. It is therefore unnecessary to introduce additional burdens on organisations which are already taking steps to neutralize the impact of malicious actors.
Article 40.1 (e)	*'When any of the following circumstances occur, the Prime Minister shall consider and decide, or authorize the Minister of Public Security to consider and decide, an urgent circumstance as to cybersecurity nationwide or at each locality or for a specific target:* *(e) An urgent unexpected order for the reason of protecting the national sovereignty, interests and security on cyberspace.'*	The draft legislation does not have any provision determining the number of organizations/individuals being adversely impacted by the cyberattack as mentioned in Article 40.1. As such, it gives the State authorities (i.e., the MoPS) very broad discretion to determine this number in practice. Such broad discretion of the MoPS could create uncertainty and disruptions in the provision of network-related services that could negatively affect Vietnam's economy. We would welcome greater clarification as to what criteria would be assessed and at what threshold a circumstance would be considered 'urgent.'
Article 41.1 a), d) and dd)	*'When the risk that an urgent circumstance as to cybersecurity may occur increases, the Ministry of Public Security shall take the main responsibility for, and coordinate with ministries, agencies and the people's committees of the provinces and central cities in, taking the following actions:* *a) Requiring related agencies, organisations and individuals to collect and report related information in a timely fashion, and to increase their supervision of the cybersecurity incident;*	As mentioned above, cybersecurity is an ongoing, iterative process which does not require special intervention by government in order to be conducted effectively. a) Further clarification is required as to what further responsibilities organisations would have under this circumstance, what information they may be required to collect or report, and what further supervision would be required. d) Further clarification required as to what precautionary options may be taken and what role would organisations have in this process. Moreover, it is critical that companies who are victims of cyberattacks retain control of their systems and data, to avoid the perception that assets are being

	d) Taking precautionary options and carrying out emergency responses in respect of cybersecurity, preventing, eliminating or reducing damages resulting from the cybersecurity incident; *dd) Making available forces and facilities to prevent and eliminate the risk of occurring such urgent circumstance as to cybersecurity.'*	expropriated (which may have a dampening effect on investment) and to enable companies to comply with their data protection responsibilities. *dd)* Further clarification is requested as to what forces and facilities would be made available. Clarification that private sector resources will not be subject to government expropriation, even on a short-term basis, would be welcome.
Article 41.3	*'Telecommunication, internet and information technology enterprises, and related organisations and individuals shall be responsible to coordinate with the Ministry of Public Security in preventing and handling any urgent circumstances as to cybersecurity.'*	The phrase "any urgent circumstances" is vague. In order to provide greater clarity, we would suggest that this provision apply only in circumstances in which a cyberattack creates a risk of physical harm to the public.
Article 47.3 (b)	*'The Ministry of Public Security shall take the main responsibility for, and coordinate with related ministries, agencies and organisations in:* *b) coordinating with related organizations and individuals in assuring the cybersecurity of Vietnamese users' data stored in cloud data centers managed by foreign organizations or individuals'.*	Cloud vendors do not have the relationship with MoPS and it would be inappropriate for MoPS to work directly with them on cybersecurity. Instead, MoPS should work with the company subject to the new requirements, and companies in turn will work with outside vendors (so the obligation remains with the company and not the vendor).
Article 51. 3	*3. Websites, web portals or specialized pages on social networks of agencies, organisations and individuals shall post information in accordance with legislation, and shall not provide, post or transmit information with any content inappropriate to the interests of the country."*	We recommend that websites, web portals or social networks host content that are posted by their users, and thus would not be able to control what the users post. Similar to comments in relation to Article 34, there should be a clear legal process for addressing this issue that, consistent with international practices, should include judicial oversight in respect of requests for content removal.

Article 51.4-.5	*4. "Telecommunication and internet service enterprises and enterprises possessing information systems shall set up their mechanisms to authenticate information when users register digital accounts to assure the confidentiality and the honesty of registration information. The registrants of such digital accounts shall be responsible to protect and use the accounts they create in accordance with legislation."* *5. "Foreign enterprises, when providing telecommunication and/or internet services in Vietnam, shall comply with Vietnamese legislation, respect the national sovereignty, interests and security of Vietnam and the interests of users, obtain licences for their operations, locate their representative offices and servers in which Vietnamese users data are administered in the territory of the Socialist Republic of Vietnam, secure user information and users' account information, and sanction violations stringently under legislation."*	This article sets out requirements that are likely to stifle growth and innovation in the digital sector. Internet service providers are being required to authenticate information provided by their users. Foreign enterprises are required to obtain licenses, and locate officers and servers within Vietnam. These requirements may result in the Vietnamese people being deprived of digital services, or having to pay more for these services, as these burdens become too onerous or costly for businesses to comply with. Requiring local servers and restricting international data flows undermines security by making it harder to aggregate information, which is essential for analyzing emerging cyber threats and fraud. This provision means additional developing and operating cost for business. Accordingly, we request that this language be removed from the Draft Law.
Article 65.1 c)	The responsibilities of telecommunication and internet service providers *'In performing cybersecurity protection tasks* *c) To cooperate with, to provide technical measures and support to, the public security bodies during their criminal investigations and protection of national security under legislation.'*	To "cooperate with and to provide technical measures and support" to public security bodies without proper due process would create a potential requirement to reveal proprietary information such as source code or to decrypt data in a way that would violate data privacy agreements between network service providers and data owners.

Article 65.2.b)	Responsibility of telecommunication and internet service providers, in assuring cyber information safety, c) *'Not to disclose, change or provide any information to any third party without the prior consent of the information owner.'*	This article would create an unclear and concerning requirement for data collection and consent, if it requires companies to obtain explicit consent from their customers. Further clarification is requested on this requirement. In addition, since encryption (for the purposes of protecting sensitive consumer information) requires information to be altered, we would welcome clarification that this would be allowed under law.
Article 65.2 e)	*'Not to provide telecommunication, internet, technical support, advertisement or payment support services to any organisations or individuals that post information containing any content against the State of the Socialist Republic of Vietnam, false or slanderous information on cyberspace.'*	Requiring that telecommunications/Internet service providers assess all clients and vendors in this regard places an undue burden on these sectors, and would no doubt have a dampening effect on foreign direct investment in Vietnam. As such, we recommend that this policy be removed.
Article 66.4	Responsibility of owners of information systems critical to the national security 4. *'When collecting or creating personal information and critical data, to store the same within the country. Where it is obligatory to provide any information out of the country, to assess security levels as regulated by the Ministry of Public Security or in accordance with legislation where it provides for this.'*	Server and data localization defeats the purpose of improving network efficiency and cost effectiveness through Internet-enabled services, such as cloud computing. Further, as fraud is not a local phenomenon, data localization will also hinder fraud prevention efforts as the building of 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. Server and data localization also increases product development cost by requiring equipment to be tailor-made for local markets, and therefore creates a market with unfair competition. In addition, the trends in global innovation and advanced technology development are increasingly moving toward hyper-scale architecture drawing on global data sets for advances such as artificial intelligence, deep learning, language processing, etc.

		Imposing requirements that make such services impractical in Vietnam will hamper economic growth and the development of globally competitive enterprises. Further, businesses which operate in multiple countries need to be able to transfer, store and process data across borders in order to provide goods and services to consumers, manage a global workforce and maintain supply chains, and to comply with financial reporting requirements. As such, we recommend that this section be removed.
Article 66.6	*"To undertake, or mandate any cybersecurity service providers to undertake, surveys and assessments in respect of their safety levels and responsiveness to risks at least twice a year, and at the same time to deliver reports on audits, assessments and improved remedies to the cybersecurity specialized agency under the Ministry of Public Security."*	Audit procedures are costly and time consuming – draining resources away from implementing 'best in class' cybersecurity practices. As such, we encourage the government to make them voluntary for private sector entities, such that they can undertake them at a frequency which is commensurate with their risk management procedures.
Article 69.2 d)	*"The responsibilities of the Ministry of Information and Communications in preventing and handling the information containing content against the State of the Socialist Republic of Vietnam or which infringe the legitimate rights and interests of organizations and individuals contrary to fine customs and practices in cyberspace include requiring foreign telecommunication and internet service providers to comply strictly with Vietnamese laws, register their business and locate their servers that contain Vietnamese users data in the territory of Vietnam."*	Data localization requirements undermine security by making it harder to aggregate information, which is essential for analyzing emerging cyber threats and fraud. Given that network risks are constantly changing, the preferred approach in promoting security is to pay attention to how the data is handled rather than where it is handled. Government should refrain from data and/or server localization requirement.

About the American Chamber of Commerce in Hanoi

Founded in 1994, the American Chamber of Commerce in Hanoi's mission is to increase trade and investment between the United States and Vietnam. AmCham supports the success of our members by promoting a healthy business environment in Vietnam, strengthening commercial ties, and providing high-quality business information and resources.

About BSA | The Software Alliance

BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

About CompTIA

The Computing Technology Industry Association (CompTIA) is a non-profit trade association serving as the voice of the information technology industry. With approximately 2,000 member companies, 3,000 academic and training partners, 100,000 registered users and more than two million IT certifications issued, CompTIA is dedicated to advancing industry growth through educational programs, market research, networking events, professional certifications and public policy advocacy.

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants a European Union that nurtures and supports digital technology industries, and that prospers from the jobs we provide, the innovation and economic benefits we deliver and the societal challenges we address. Our mission is to foster, on behalf of our members, a business, policy and regulatory environment in Europe that best realises our vision. We will achieve this by working as positive partners with the European Institutions and other European and global bodies and, through our national trade associations, the member states of Europe.

About Information Technology Industry Council

The Information Technology Industry Council (ITI) is the global voice of the tech sector, celebrating its 100th year in 2016 as the premier advocacy and policy organization for the world's leading innovation companies. We advocate for global policies that advance industry leadership, open access to new and emerging markets, promote e-commerce expansion, drive sustainability and efficiency, protect consumer choice, and enhance worldwide competitiveness of our member companies. Visit www.itic.org to learn more. Follow us on Twitter for the latest ITI news @ITI_TechTweets.

About Japan Electronics and Information Technology Industries Association

The Japan Electronics and Information Technology Industries Association (JEITA) was launched in 2000 through the consolidation of the EIAJ, originally formed in 1948, and JEIDA, which was set up in 1958. JEITA is Japan's leading ICT and electronics association, with around 400 members from Japan and abroad.

We have been working on a range of programs to promote data utilization, etc., with the aim of realizing "Society 5.0"—a world-leading super-smart society built on advanced information use.

About Semiconductor Industry Association

SIA | The Semiconductor Industry Association (www.semiconductors.org) is the voice of the U.S. semiconductor industry, which makes the global trillion dollar electronics industry possible. Its members make the microchips that control all modern electronics and enable the systems and products we use to work, communicate, travel, entertain, harness energy, treat illness, and make new scientific discoveries. SIA seeks to strengthen U.S. semiconductor manufacturing, design, and research by working with Congress, the Administration, foreign governments, and global industry stakeholders to encourage policies and regulations that fuel innovation, propel business and drive international competition.

About US-ASEAN Business Council

For over 30 years, the US-ASEAN Business Council has been the premier advocacy organization for US corporations operating within the dynamic Association of Southeast Asian Nations (ASEAN). Worldwide, the Council's 150+ membership generates over $6 trillion in revenue and employ more than 13 million people. Members include the largest US companies conducting business in ASEAN, and range from newcomers to the region to companies that have been working in Southeast Asia for over 100 years. The Council has offices in: Washington, DC; New York, NY; Bangkok, Thailand; Hanoi, Vietnam; Jakarta, Indonesia; Kuala Lumpur, Malaysia; Manila, Philippines; and Singapore.

About U.S. Chamber of Commerce

The U.S. Chamber of Commerce represents the interests of more than three million U.S. businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations. Its International Affairs Division includes more than 50 regional and policy experts and 23 country-specific business councils and initiatives. It also works closely with 116 American Chambers of Commerce abroad.