26 February 2018

Respectfully to: Ministry of Public Security
Hanoi, Vietnam

Attention: Senior Lieutenant General To Lam
The Minister

Joint Industry Comments on Draft Law on Cybersecurity

ACT | The App Association, The American Chamber of Commerce Hanoi, BSA | The Software Alliance, The Computing Technology Industry Association (CompTIA), DIGITALEUROPE, The Information Technology Industry Council (ITI), 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 ("MPS") for the opportunity to submit comments on Draft 15 of the Law on Cybersecurity ("Draft Law").

Our organizations appreciate the opportunity to provide further comments alongside those already submitted on August 25 and October 31, 2017. We are encouraged by the positive amendments to Draft 15 as compared to the previous draft, such as the modifications to the server localization requirements and the whole-of-government approach indicated by the Ministry's ceding of some cybersecurity responsibilities to other authorities. We offer our support as the revision process continues.

With the shared goal of ensuring the stability and security of Vietnam's technology infrastructure, we are writing to share remaining concerns with the Draft Law, particularly those regarding data localization, content regulation, local representative office requirements, and the Draft Law's broad scope. As a collective of industry stakeholders, we hold cybersecurity as a top priority, and take an active role in ensuring the security of our products and services for all users.

Our recommendations on addressing cybersecurity challenges derive from expertise in developing solutions which raise cybersecurity standards for businesses of all sizes and in all sectors of the economy. In an effort to engage more closely with the Vietnamese government on cybersecurity legislation, we respectfully seek to offer additional constructive feedback on what we believe are unclear, or potentially harmful, provisions in the Draft Law.

Specifically, our comments are as follows:

- **Article 3(5)(d):** We recommend limiting the language of this clause so as not to include IoT, cloud computing, big data, or artificial intelligence systems within the scope of "national cyberspace infrastructure," as well as removing references to industry 4.0, including mixed real and virtual systems, cloud computing, big data, fast data, and artificial intelligence system. Other references to "national cyberspace infrastructure" impose an overly broad scope of restrictions on this infrastructure that might be helped in part by a narrower definition.

- **Articles 3(21), 22(1)**: Article 3(21) contains a definition for "*dangerous circumstances as to cybersecurity,*" while Article 22(1) lists out the actual "*dangerous circumstances as to cybersecurity.*" To avoid ambiguity in what constitutes "*dangerous circumstances as to cybersecurity,*" we recommend deleting Article 3(21) in its entirety, and amending the heading of Article 22(1) to read as follows: "For purposes of this Article 22, '*dangerous circumstances as to cybersecurity*' means any one or more of the following:"

- **Articles 5(5), 10(1-2), 11(2), 13(2) and 42(5)**: The Draft Law consistently references the need to take ex-ante measures to ensure secure systems before use. This requires industries to divert a large proportion of their resources towards averting a single, static vulnerability, and away from a myriad of evolving threats that are the source of most cyber-attacks. We recommend instead that 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.

- **Articles 6(1), 16(4), 27(2) and 41(2)(d)**: We recommend removing the requirement that companies take down (or otherwise "prevent" the posting of) content in the absence of a specific court order.

- **Article 7**: We strongly support the Draft Law's provisions for international cooperation on cybersecurity, given the transnational nature of the threat landscape. These efforts should extend to ensuring that the policy response to cybersecurity threats does not have a negative impact on trade or the attractiveness of the Vietnamese economy. As such, we recommend the addition of a sub-article to Article 7(2), which reads: *"The development of multilateral systems which facilitate the harmonization of cybersecurity protection measures that are required of owners and operators of information systems critical to national security."*

- **Articles 8, 16, 41**: The Draft Law obligates information system owners to "prevent, detect, fight against, or remove" certain content. The definitions of offensive speech and expression are broad and unclear, requiring content that does not meet the Draft Law's standards to be taken down within a short timeframe of 24 hours, but without detailing what type of content falls under this provision. References to "embarrassing or slanderous" content, as well as speech which restricts "social order and safety," appear arbitrary and difficult to interpret or regulate. We recommend removing phrases in these Articles and elsewhere in the Draft Law that refer to aspects of social order and content regulation in the definition of harms. Directions for content removal should be accompanied by court orders and specify the content in question deemed offensive.

- **Article 9, 11, 19**: Language concerning the methods of classification and criteria necessary for "information systems critical to national security" as well as formation and implementation of the "specialized force" and "List of Information Systems Critical to National Security" remains unclear. We recommend further clarification of the language in these articles, and the use of a third-party audit and assessment agent rather than the use of a "specialized force" or ad hoc cybersecurity audit and assessment, both of which appear unnecessary and excessive.

- **Article 9(2)(c):** This language is overly broad. Without clear definition of what constitutes "particularly important value," this clause can be interpreted to cover a wide range of information systems, well beyond the scope of "information systems critical to national security."

- **Article 9(2)(e):** The language here is vague. The term "e-government" captures many non-national security related information systems.

- **Article 9(2)(g):** Rather than designate entire sectors of the economy as "critical," it is important to delineate services that are vital and non-vital to the functioning of Vietnamese society. We recommend that the government narrow the focus of legislation to "*identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security*."

- **Article 11(5):** It is widely accepted that no network system can provide 100% security before an incident occurs; therefore, it is imperative that a network is highly resilient after a network attack or natural disaster takes place. Industry experts recommend that, in terms of legislative design, the mechanism should not overly depend on ex-ante security testing and assessment. We suggest that such requirements be focused on ensuring that products and services can be designed on principles of *identify, protect, detect, respond, and recover*, rather than impose measurements of security at any static moment in time.

- **Article 11, 42(7)**: Audit procedures are very costly and time consuming. The proposal for "annual audits and assessments" would drain resources away from implementing best-in-class cybersecurity practices, towards legal compliance measures. We recommend that audits be conducted voluntarily by private sector entities, such that they can undertake them at a frequency which is commensurate with their risk management procedures.

- **Article 13:** The language used to describe cybersecurity qualification certifications, which must be obtained from MPS or the Ministry of National Defense depending on how critical the work is to national security, has changed from the previous draft. While Article 15 of Draft 14 described these certifications as a self-certifying procedure, the current Draft Law implies a more regulatory nature and mechanism. We recommend that requirements for these certifications revert to the one contemplated in Draft 14, such as a mechanism that is self-certifying with oversight from MPS. This would help ensure that products and services are designed with security in mind, without unnecessarily complicating the procedure. Additionally, we request detailed information on the "cybersecurity conditions" for information systems critical to national security, including any product security standards and certification requirements to be applied.

- **Article 14(1)**: Given broad international use of the National Institute for Standards and Technology (NIST) Cybersecurity Framework as a means for organizations to assess and improve their ability to identify, protect, detect, respond and recover from cyber-attacks, we recommend that this taxonomy be utilized in place of the existing language in Article 14 (1). This will provide

greater clarity to organizations in terms of what is required of them and, consequently, will facilitate compliance with the requirements.

- **Article 14(3)**: The resolution of cybersecurity incidents should be led by the owners or operators of information systems critical to national security themselves, since they have the requisite knowledge of the systems that they manage. We recommend that this language be adapted such that owners and operators shall take the lead, while MPS shall provide support, as requested.

- **Article 26:** Relating back to the definition of "national cyberspace infrastructure" contained in Article 3(5)(d), we urge the Vietnamese government to delete Article 26(1)(b) because it mandates localization of gateways and thus creates burdensome requirements for local providers.

- **Articles 27, 45**: We appreciate that the local office requirement was changed to a "local representative office requirement," but remain concerned that any such requirement will not enhance cybersecurity. A local representative office is typically not authorized to provide user data and does not have the capabilities to remove any content that does not comply with the regulations, as detailed above. We would especially recommend the deletion of Article 27(4)(c), as the suggested localization creates additional business costs and does not strengthen, but could actually weaken, the security of those systems.

- **Articles 27, 42, 48**: We recommend that Vietnam utilize global cloud infrastructure rather than store cloud-based data by jurisdiction. Not doing so creates both security and business concerns, which are outlined in more detail below.

    - Security Concerns:
        - Cloud services operated by global cloud services providers according to international best practices are typically more secure than local networks. Such service providers invest heavily to ensure their systems are secure, both physically and digitally. They also have visibility into cyber threats around the world, and ensure their cyber defenses are quickly updated against newly discovered threats. Network failures are less disruptive under a globally distributed network, as the free flow of data in the cloud ensures that data is still available on another network. Restricting the storage of user data geographically prevents Vietnam from benefitting from a more resilient, secure, and reliable system. Using local IT solutions that are out of date with global standards would work against the national security goals of this draft law.

    - Business Concerns:
        - Enterprises from every sector in Vietnam compete on the global scale, and as a result require cutting edge resources to remain attractive to a diverse customer base. Forced localization limits business capacity to access infrastructure and tools necessary to support business operations, employees, and networks around the world. Forced localization also inhibits global operations through

restricting the mobilization of user data from region to region. Increased costs for companies to comply with requirements to send data to specific locations undermine efficiency and productivity of these businesses and ultimately burden users, making technology more expensive and less secure.

- Data security furthermore depends on the quality controls and management processes rather than a server's physical location. Businesses choose to store data outside the country of operations to ensure data availability and security in the case of a natural disaster, power outage, or other emergencies. Geographic neutrality with regard to data storage enables all companies, particularly small ones, to employ cost-effective information security solutions. We recommend that the language used in Article 42(4), "*where it is obligatory to provide any information out of the country*," be changed to "*where the owner of the information systems considers it necessary to provide any information out of the country*" as well as "*to assess security levels*" changed to "*to conduct a self-security assessment based on security levels regulated by the Ministry of Public Security.*"

- **Articles 41(2)(d):** The requirement that telecom and Internet providers remove content recognized by the State for being "false or slanderous" within 24 hours is exceedingly strict. Content removals present an extremely complex set of legal and compliance processes that may often take longer than 24 hours for companies to resolve. In an effort to narrow the scope of the law, we strongly recommend that content regulation issues be addressed through a separate legislative instrument.

We are grateful for the opportunity to once again provide feedback on this important legislation, and we appreciate your engagement with the business community. Our organizations stand ready to work with your government to implement clear cybersecurity legislation that supports the continued development of Vietnam's digital economy. We would welcome a meeting to further discuss our concerns and alternative approaches that could better ensure Vietnam's cybersecurity.

About ACT | The App Association

ACT | The App Association (www.actonline.org) is an international grassroots non-profit trade association that represents thousands of small business software application development companies and technology firms located around the world. Alongside the rapid adoption of mobile technologies, our members have developed innovative applications and products that improve workplace productivity, accelerate academic achievement, monitor health, and support the global digital economy. The app ecosystem the App Association's members drive is worth more than $143 billion and serves as a key driver of the $8 trillion internet of things (IoT) revolution.

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 the Information Technology Industry Council
The Information Technology Industry Council (ITI) is the global voice of the tech sector and 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.

About the 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 the 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 the 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 the 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.