December 13, 2018

Respectfully to: **Ministry of Public Security**
Department of Cybersecurity, and Prevention of Crimes Using High Technology

Attention: **Lt. General Nguyen Minh Chinh**
Director

BSA COMMENTS ON THE DRAFT DECREE IMPLEMENTING LAW ON CYBERSECURITY

A. Introduction and Statement of Interest

BSA | The Software Alliance (**BSA**)[1] thanks the Ministry of Public Security (**MPS**) for the opportunity to submit comments on the draft decree implementing Law on Cybersecurity ("**Draft Decree**" and "**LOCS**" respectively). We offer the following comments in the hope that they will be helpful as the MPS and the Department of Cybersecurity, and Prevention of High Technology Crimes are finalizing the Draft Decree and considering potential amendments to the LOCS in the future.

Our members have a significant interest in Vietnam's LOCS and its corresponding draft decrees. BSA has previously provided comments (hyperlinked where available) as follows:

(i) Annex A: Joint Association Comments on the Implementing Guidelines for the Vietnamese Law on Cybersecurity (September 3, 2018)
(ii) Annex B: Joint Industry Comments on May 24 Revised Draft Law on Cybersecurity (May 28, 2018);
(iii) Annex C: Joint Industry Comments on Draft Law on Cybersecurity (February 26, 2018); and
(iv) Annex D: Joint Industry Comments on Draft Law on Cybersecurity (August 8, 2017).

We acknowledge and recognize the important effort that MPS and the Department of Cybersecurity and Prevention of High Technology Crimes have undertaken to ensure that Vietnam is prepared to deter and manage cybersecurity threats. However, an excessively broad

[1] 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, 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.

BSA's members include: Adobe, Akamai, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, Box, CA Technologies, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, SAS Institute, Siemens PLM Software, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, and Workday.

implementation of the LOCS – particularly in relation to data localization, local office requirements and law enforcement access to information – remains an ineffective method for achieving this goal and will have a chilling effect on innovation and investments.

As stated in our previous submission of 28 May 2018, it is imperative that the Government of Vietnam provides a flexible approach that accommodates a wide range of sectors and also recognizes and incorporates the regional data transfer mechanisms in existence today. Providing a regulatory regime that is both predictable and sufficiently flexible to allow for the adoption of cutting-edge IT products and services will ultimately yield the best security outcomes. We offer below a series of recommendations to help meet these objectives.

Data localization provisions are not in the spirit of Vietnam's commitments within the Comprehensive and Progressive Agreement for Trans Pacific Partnership (**CPTPP**), in which parties agreed to prohibit forced localization. These provisions also raise concerns relative to Vietnam's commitments under the General Agreement on Trade in Services (**GATS**) to permit cross border trade in services in numerous sectors without any limitations or restrictions. Those commitments include numerous services in which the cross-border transfer of data either is integral to, or comprises, the cross-border service at issue, with the result that Vietnam's proposed restrictions would breach Vietnam's GATS commitments and negate their value. The provisions also raise concerns relative to Vietnam's commitments to afford national treatment to foreign services and service suppliers.

Finally, as an APEC Member Economy, Vietnam should not foreclose the possibility of taking part in the APEC Cross-Border Privacy Rules System (**CBPR**) in the future. As the Member Economy Ministers recognized in 1998, "Regulatory systems that unnecessarily restrict [information] flow or place burdens on it have adverse implications for global business, economies and individuals."

Disrupting global data flows through data localization undermines cybersecurity significantly. Data security is ultimately not dependent on the physical location of the data or the location of the infrastructure supporting it. Businesses consider many factors when deciding where to locate digital infrastructure, for example in optimizing Internet speed and access, developing redundancy and backup capabilities, and the deployment of state-of-the-art security solutions. The draft decree restricts the ability of businesses to make decisions based on such considerations. Given the complexity and sensitivity of the subject matter, we strongly encourage the MPS not to rush into implementing all aspects of the LOCS, particularly relating to data localization and local office requirements, and to thoroughly consider all issues at play, including the implications and possible unintended consequences of the Draft Decree.

In this submission, we highlight provisions in the Draft Decree that raise the most serious concerns amongst our members. In this regard, we urge the MPS to consider further clarifying the Draft Decree as the implementation of the LOCS will have implications on the growth of the digital economy of Vietnam. To summarize, our comments focus on the following:

(i) Data localization and local office requirements under Chapter V of the Draft Decree should be subject to clear and defined limits that include due-process and appeal mechanisms;
(ii) Information systems that are not "critical to national security" should be clearly excluded from requirements under Article 19 of the Draft Decree and due-process and appeal mechanisms for "sudden audits" should be introduced; and
(iii) Inclusion of specific review or appraisal procedures as well as clear exemptions to conditions on cybersecurity assurance for equipment, hardware and software that are components of the information systems critical to national security under Article 14 of the Draft Decree.

B. Comments and Recommendations

1. Data localization and local office requirements under Chapter V of the Draft Decree should be subject to clear and defined limits that include due-process and appeal mechanisms

Under Article 25 of the Draft Decree, onshore and offshore entities having all of the following parameters must localize data, and establish a local branch or representative office in Vietnam:

(i) Being providers of one of the services on telecommunications networks [and/or] the Internet [and/or] value-added services in cyberspace with the following business activities in Vietnam: Telecommunications services; Services of storing [and/or] sharing data in cyberspace; Providing national or international domain names to service users in Vietnam; E-commerce; Online payment; Payment Intermediary; Services of transportation connection via cyberspace; Social networks and social media; Online games; Electronic mails;

(ii) Engaging in collecting, exploiting, analyzing and processing various types of data specified in Article 24 of the Draft Decree;

(iii) Enabling the service users to conduct the acts stipulated in Article 8.1 and/or Article 8.2 of the LOCS; and

(iv) Violation of the provisions of Article 8.4, Article 26.2(a) or Article 26.2(b) of the LOCS.

The Minister of Public Security will have the discretion to request specific businesses meeting the conditions above to store data in Vietnam and set up a branch/representative office in Vietnam.

This definition is wide-ranging and can virtually capture all types of online services available in Vietnam through the Internet. The framework for implementation of data localization and local office requirements under Chapter V of the draft decree can be enhanced further and additional clarity can be provided as follows:

1.1. Articles 24, 25 and 26 of the Draft Decree should only be applied pursuant to violations relating to Article 8.1 or 8.2 and 8.4, 26.2(a) or 26.2(b) of the LOCS.

Based on the current draft, it remains unclear whether Article 25 applies only to businesses that meet all four (4) of the above parameters (Article 25.1) **and** have been requested by the Minister of Public Security (Article 25.2) to meet data localization and local office requirements.

BSA recommends that the implementation of data localization and local office requirements, be scoped narrowly – and only applied as necessary to achieve the aims of the LOCS. In this regard, MPS should amend the draft decree to clearly **limit the scope of applicability of Article 25.1 only to businesses that are found to be in violation of LOCS: (a) Articles 8.1 or 8.2; and (b) Articles 8.4, 26.2(a) or 26.2(b)**, as outlined in the current draft decree as key areas of concern for MPS. BSA also recommends **deleting Article 25.1(a) and (b), to make scope of applicability clear**.

In addition, we recommend that MPS further clarify that ***only businesses who own and control the data set out in Article 24 can knowingly and intentionally encourage activities that violate the above, and hence Article 25 should not apply to business that do not own or control data set out in Article 24***. For example, in the context of self-service IT infrastructure, the customers of cloud service providers tend to own and control the data; they choose what data to store and where to store it and are often fully responsible for implementing appropriate technical and organizational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. In such circumstances, cloud service providers do not have visibility into or knowledge of what content customers are uploading to their services, including whether that content constitutes data that would be in violation of Vietnamese laws.

Broad implementation of data localization and local office policies will negatively affect Vietnam's economic competitiveness as businesses across all sectors and of all sizes in Vietnam rely on and benefit from the seamless flow of data into and out of the country. Data localization expenses will

inevitably be passed along to consumers in the form of higher prices. Requiring local businesses to use local data centers will add costs that are particularly hard to absorb for small and medium sized businesses. Ultimately, these localization requirements may also undermine cybersecurity by forcing companies to divert funds that could otherwise be focused on enhancing network security.

1.2. Data localization and local office requirements should be implemented as a last resort with the inclusion of due-process and appeal mechanisms

We would also recommend that MPS make clear that ***only where businesses are found to be in violation of the above will MPS consider requesting businesses with infringing activity to implement data localization and local office requirements***. In such circumstances, imposition of data localization and local office requirements should be viewed as a last resort, and due-process and appeals mechanisms should be provided as an avenue for recourse and appeal. Related to the above, we make the following recommendations:

(i) **Businesses should not be subject to data localization and local office requirements if they can comply with requests for lawful access to data**. We recommend that MPS make clear that businesses which are already able to make data available to the MPS or provide access to the data, as requested under an instrument of law, will not be subject to data localization and local office requirements.

(ii) **Due-process and court orders should be required for the implementation data localization and local office requirements**. The applicable data to be localized and the nature and activity required for local office/representative set-up should be precisely defined and limited by independent oversight and judicial review. Businesses should be notified, offered the opportunity to carry out rectification actions, and afforded clear opportunities to contest orders and rights to appeal adverse decisions in Court, prior to data localization and local office requirements being triggered. Furthermore, such requirements should be served on the violating business, that has control over the applicable data, rather than on their third-party vendors or data processors. Direct serving of orders on third-party vendors and data processors could place them in an untenable situation of needing to breach contractual agreements they have with their customers or their legal obligations under other jurisdictions.

(iii) **Court orders should be subject to a right of appeal**. A corresponding right to appeal should be provided in all cases of compelled actions related to data localization and the set-up of a local office. The compelled actions could be overly prescriptive and onerous for businesses or technically infeasible, or may not be directly related to the violation. Hence providing an avenue for appeal in such situations is essential.

1.3. Limiting the scope of applicable data to be stored in Vietnam under Article 24

Article 24 currently imposes a local storage requirement on a very broad scope of data. We understand that the concern of the MPS is about data sovereignty and making data available and accessible in Vietnam to maintain national security. However, requiring a broad scope of personal data of service users to be stored in Vietnam is disproportionate to this concern, and unnecessary and burdensome to the service providers.

The larger the scope of data subject to such requirement is, the larger the burden and the cost that the service providers have to bear. Meanwhile, certain types of personal data, data generated by service users in Vietnam and data regarding the relationships of the service users in Vietnam may not need to be stored locally to be accessible. Developing a joint agreement/framework or code of conduct with international businesses may be a better option for the MPS and the business environment.

In addition, data localization requirements have the effect of undermining cybersecurity efforts. The risk of cybersecurity attacks and breaches on data that is stored in Vietnam could increase,

because centrally stored information can provide an attractive target to malicious actors, who understand that breaching systems of localised data could yield complete sets of data. By contrast, using cloud systems to distribute data storage globally improves the ability to compartmentalize data sets, improving the chances that a breach in one location will not lead to access to the entirety of any data set.

If ultimately, the MPS has to rely on data localization requirements because a service provider does not provide access or make data available, we recommend that the MPS implement the data localization requirements narrowly and only where necessary as follows:

(i) ***The scope of data subject to local storage requirement should be limited to information that is essential for MPS' purposes***. This could include data relating to investigations of or violations to Article 8.1 or 8.2 and 8.4, 26.2(a) or 26.2(b) of the LOCS. Data localization requirements should not provide MPS with carte blanche powers to request for *all data* listed under Article 24 to be stored in Vietnam, without a clear purpose;

(ii) ***Datasets that could have significant impact to individuals if breached should be excluded from Article 24.*** Given the increased cybersecurity risk that is posed by localization of data, MPS should also consider excluding datasets that could have significant impact to an individual if a cyberattack or data breach were to occur, from data localization requirements. For example, information such as identity card number, credit card number, health status, medical records and biometry should be excluded from Article 24, as a data breach involving these types of data could result in significant harm to individuals;

(iii) ***Only a copy of the relevant data should be stored in Vietnam***. MPS should make clear in its Draft Decree that additional copies of data listed in Article 24 can also be stored outside of Vietnam, so that companies can draw on this information for analysis and correlation, especially for timely access to global sources of ongoing threat information and the ability to synthesize the collected information into actionable intelligence for security products and services;

(iv) ***Request for the data to be stored in Vietnam should be specific and obtained under an instrument of the law*.** This would ensure that there is a record of the event and an explanation of its scope, purpose, context, and timescale;

(v) ***Companies should not be required to collect additional data.*** In addition, it needs to be recognized that not all companies collect the same personal data. Hence, MPS should make clear that businesses will not be required to collect unnecessary personal or other data, superfluous to the requirements of their business model; and

(vi) ***Data processors or vendors should not be responsible for collecting, retaining or storing copies of a "service user's" information.*** The Draft Decree does not define the term "service users in Vietnam" and the parameters to be considered as "service users in Vietnam". The term "service users" should be clarified as "service users" of the data controller, hence making it clear that there is no expectation for vendors or service providers of data controllers to collect, retain and store copies of the data controllers' "service user's" information in Vietnam.

1.4. The scope of "service providers" subject to Article 25.1 should be narrowed and clarified

Article 26.3 of the LOCS provides that local and foreign "*providers of services on telecommunication networks on the Internet and value-added services in cyberspace in Vietnam*"

("**Cyberspace Service Providers**") would be subject to data localization and local office requirements. Article 2.1[2] and Article 25.1(a) of the Draft Decree collectively defines Cyberspace providers as businesses that operate commercially to provide one of the following services in Vietnam:

1. Telecommunication services;
2. Data storing and sharing on cyberspace;
3. Services providing national or international domain names to service users in Vietnam;
4. E-commerce;
5. Online payment;
6. Payment intermediary;
7. Connecting transportation on cyberspace;
8. Social networks and social media;
9. Online games;
10. E-mail.

Pursuant to Article 25.1, the scope of businesses that qualify as a "Cyberspace Service Provider" remains extremely broad and unclear. Article 25 fails to recognize the relationships that businesses have with their vendors and data processors, and the corresponding application of Article 25 on each party. Vendors and data processors that are processing data and information on behalf of other businesses (i.e. data controllers) generally do not have visibility over their client's data. Therefore, they would not be in a position to determine whether a data controller has stored data on the service that would result in the application of the LOCS and the Draft Decree. For example, cloud service providers may not know if a data user has stored personal data on a cloud service. Hence, ***we recommend MPS exclude businesses that are processing data and information on behalf of other businesses (i.e. data controllers)***.

In addition, the categories identified in the list above when read with other laws (for example the Telecommunications Law) are duplicative and confusing. We have identified the following categories of businesses that would benefit from further clarification:

(i) It is unclear which services are considered "Data storing and sharing on cyberspace".
(ii) It is unclear which services are considered "e-commerce" under the Draft Decree, and whether such terminology refers to other relevant regulations (such Decree No. 52/2013/ND-CP and/or Decree No. 09/2018/ND-CP).

Due to this lack of definition, some services listed above may overlap with each other, such as telecommunication services and e-mail. We note for example that an e-mail service is a telecommunication value-added service. Given so, we recommend that the MPS narrow the list of businesses that would qualify as "Cyberspace Service Providers". ***Specifically, we recommend that the MPS remove Category 2 and Category 10 (i.e., data storing and sharing on cyberspace; and e-mail services) to avoid confusion and duplication***.

We further recommend that the MPS clearly define each service listed in Article 25.1 of the Draft Decree. Preferably, these services should be aligned with the definitions and categories that are provided in existing regulations. For example, telecommunication services and value-added telecom services are defined in the Telecommunications Law and Circular No. 05/2012/TT-BTTT.

1.5. Retention periods under Article 26

Article 26 specifies a retention period but is unclear on whether it applies to businesses subject to data localization and local office requirements only, or to *all* businesses in general. The is because storage period of "system logs" as provided in Article 26 does not fall within any Article 24 category of data that is subject to data localization requirement. We also note that Article 26 states "data

[2] Under Article 2.1 of the Draft Decree, there is a drafting error that mistakenly refers to Article 24. The actual list of services enterprises provide is featured in Article 25.

retention period" rather than "data retention period in Vietnam".

Moreover, Article 24 and Article 26 are unclear as to whether this requirement means that such data must be stored exclusively in Vietnam, or only a copy of such data is required to be stored in Vietnam.

We recommend that the MPS remove the storage period relating to "system logs" from Article 26 and throughout Chapter 5 since "system log" is not a type of data subject to data localization requirements under Article 24. Furthermore, the title of Article 26 should be amended to "data retention period in Vietnam for data subject" to "data localization requirement".

We further recommend that the MPS make clear that the data localization requirement means that such data does not need to be stored exclusively in Vietnam (i.e. only a copy of such data is required to be stored in Vietnam).

1.6. Grace period under Article 29

Article 29 provides that businesses defined in Article 25 will have one (1) year to comply with the data localization and local office requirements from the time the MPS makes the relevant request. One (1) year is an insufficient amount of time for businesses to comply with the MPS's request to localize data and open local offices, considering the amount of time that would be required establish a physical presence in Vietnam.

Given so, we recommend that the MPS consider either of the following options:

(i) To lengthen the grace period to three (3) years and provide exemptions for businesses if the circumstances so require; or

(ii) To provide leeway to relevant businesses subject to data localization and local office requirements by allowing them to submit documents showing their commitment to comply with requirements, if the one (1) year deadline cannot be met.

2. Information systems that are not "critical to national security" should be clearly excluded from requirements under Article 19 of the Draft Decree and due-process and appeals mechanisms for "sudden audits" should be introduced

Article 19.2 of the Draft Decree provides the process and procedures for an unexpected cybersecurity audit including in circumstances where an audit is carried out information systems that are not "critical to national security" (i.e. pursuant to Article 24.1 of the LOCS). While Article 24.1 states that such audits can only be carried out if there is an act is that is "*violating the laws on cybersecurity that prejudices national security, or causes serious harm to social order and safety*", neither the Draft Decree nor the LOCS provide clarity on the exact circumstances when this would apply.

As it stands, these provisions raise cause for concern as they can be subject to broad interpretation that grant excessive power to local authorities to access information without having to show proper reason or authorization. Article 24 of the LOCS and Article 19 of the Draft Decree do not limit or specify the scope of information the *specialized cybersecurity protection forces* may access during the audit. A plain reading of this Article appears to suggest that the *specialized force* is entitled to a significant range of information in any kind of system of agencies and organizations in Vietnam (in the course of an audit as per above circumstance). Furthermore, the audited information would likely include personal data or trade secrets, which would be protected by relevant laws of Vietnam, such as the Civil Code and the Intellectual Property Law. Therefore, an authority's unreasonable access to the personal or business secrets of an information system could trigger a serious risk of the authority being deemed to have committed a violation of a citizen's privacy.

Given the above, we make the following recommendations:

(i) **Circumstances under which specialized cybersecurity protection forces are permitted to conduct audits, should be limited to situations concerning "material national security information systems" and that "results in circumstances that prejudices national security, or causes serious harm to social order and safety"**. Such circumstances should be clearly elaborated. In addition, the scope of information that the specialized cybersecurity protection *can access during an audit* should be limited to information that is relevant to the purposes of the audit;

(ii) **Some categories of information should be exempted from audit.** This includes privileged information or information which would violate other rights, such as personal information, or information that would be inconsistent with protecting intellectual property rights or trade secrets;

(iii) **An appeals mechanism should be created to review a "sudden audit" request. MPS should create a process to allow businesses to appeal an audit request**. Court orders should be served in all circumstances where a "sudden audit" is being compelled. All compelled actions should be obtained under an instrument of the law to ensure that there is a record of the event and an explanation of its scope, purpose, context, and timescale. A corresponding right to appeal should be provided. Without adequate due process safeguards and avenues for appeals compelled actions, such as requiring the audit of computer systems or de-activating functioning computers could be overly prescriptive and onerous for businesses or technically infeasible. Hence providing an avenue for appeal in such situations is essential. In situations where there are requests for "sudden audit" resulting in an exception to a court order, these exceptions should be precisely worded, and the Vietnamese legal system should provide a corresponding document such as a warrant or a "temporary emergency document" that would define the requirements of the audit clearly; and

(iv) **Direct serving of orders on third-party vendors or data processors should be avoided.** Where the audit involves both businesses that operate the "material national security information systems" as well as their third-party vendors, direct serving of orders on third-party vendors should be avoided as it would place them in an untenable situation of needing to breach contractual agreements they have with the business operating "material national security information systems" (e.g. regarding confidentiality and data protection) or their legal obligations under other jurisdictions.

3. *Inclusion of specific review or appraisal procedures as well as clear exemptions to conditions on cybersecurity assurance for equipment, hardware and software that are components of the information systems critical to national security ("Critical Systems") under Article 14 of the Draft Decree*

Pursuant to Article 14 of the Draft Decree, equipment, hardware, and software that are components of the Critical Systems must, among others, be audited for cybersecurity to detect vulnerability, security flaw, malware, assuring compatibility with other components in the information systems critical to national security. In addition, the products that have been flagged for or "warned" of any possible cybersecurity risk by the *specialized cybersecurity protection forces* must not be used without remedial measures for handling and overcoming vulnerability, security flaws, and malware being put in place before use.

The Draft Decree contains no detail on any review or appraisal procedures, or any objective criteria to establish whether a specific product or service is fit for use in Critical Systems. Ambiguous review and appraisal procedures may result in non-transparent procurement procedures and discrimination between offshore suppliers and domestic suppliers. Furthermore, the requirement of audit of components and company equipment could result in forced access to privileged information or information which would violate other rights, such as personal information,

or would be inconsistent with protecting intellectual property rights or trade secrets. Given so, we make the following recommendations:

(i) The MPS should provide ***specific review or appraisal procedures*** as well as on any objective criteria to establish whether a specific product or service is fit for use in Critical Systems;

(ii) The MPS should include a ***clear exemption for information to be excluded from audit,*** including those that would be inconsistent with protecting intellectual property rights or trade secrets, as well as privileged information of information that would violate other rights; and

(iii) The MPS should consider the ***adoption of internationally-recognized certification systems such as the ISO/IEC 27034 or Common Criteria*** to assess and evaluate products that are deployed in critical systems rather than introducing a different approach.

C. Conclusion and Next Steps

We would like to thank the MPS again for the opportunity to comment on the Draft Decree. We appreciate MPS's kind consideration of our above comments.

BSA represents the global software industry. Our members are at the forefront of data-driven innovation, developing cutting-edge advancements in artificial intelligence, machine learning, and cloud-based analytics. Our members earn users' confidence by providing essential security technologies that protect against cyberthreats. By working closely with governments around the world on cybersecurity policy and legislative development, BSA has witnessed the potential for cybersecurity laws and regulations to both deter and manage cyberthreats while also protecting privacy and civil liberties of citizens.

Building on this experience, BSA has developed the International Cybersecurity Policy Framework (**Framework**), which sets out a recommended model for a comprehensive national cybersecurity policy.[3] BSA encourages the Vietnamese Government and MPS to take reference from international best practices, such as the National Institute of Standards and Technology's Cybersecurity Framework[4] and those outlined in BSA's Framework, when developing, implementing, and operationalizing cybersecurity-related rules and requirements.

For any questions or if any point of clarification is required on any part of this submission, please feel free to contact us. Thank you for your time and consideration.

Yours sincerely,

Jared Ragland, Ph.D.
Senior Director, Policy – APAC
BSA │ The Software Alliance

[3] The *BSA International Cybersecurity Policy Framework* at: https://bsacybersecurity.bsa.org/wp-content/uploads/2018/04/BSA_cybersecurity-policy.pdf. For more information, see https://bsacybersecurity.bsa.org/.

[4] The *Framework for Enhancing Critical Infrastructure Cybersecurity, Version 1.1* provides outcome-focused, risk-based guidelines to enhance cybersecurity of critical infrastructures and critical infrastructure networks. See https://www.nist.gov/cyberframework.