Information Technology Industry Council

July 10, 2013

Ministry of Information and Communications
18 Nguyen Du
Hanoi, Vietnam

RE: Comments on Vietnam's Draft Law on Information Security, version 2.22

Dear Sir/Madam:

The Information Technology Industry Council (ITI) appreciates the opportunity to provide general input on the Republic of Vietnam's Draft Law on Information Security version 2.22, released on May 22, 2013. ITI is a voice, advocate, and thought leader for the global information and communications technology (ICT) industry. ITI's members[1] comprise the world's leading technology companies, with headquarters worldwide.

ITI commends the Government of Vietnam for undertaking the challenging task of seeking to improve cybersecurity.[2] Policymakers globally are intensely working on cybersecurity policies and laws in recognition of the evolving challenges to security in cyberspace. Throughout all of these efforts, ITI works closely and consistently with policymakers, providing substantive input and ideas and helping them to better understand the most effective approaches to improving cybersecurity. However, we believe certain proposed actions in the draft law, if not revised or implemented carefully, would present serious challenges to reaching the intended goal. In addition, we believe that certain provisions relating to personal information might hinder the ability of industry to innovate and to engage in the necessary transactions to offer optimal products and services.

Our comments below are not intended to be a comprehensive section-by-section analysis of the draft law. Rather, we make some general comments, as well as more specific comments with respect to certain sections.

General comments

Overly broad scope: The law includes a variety of separate issues that we believe should not be addressed in one law. The law's provisions touch on cybersecurity, personal information, and content/filtering. In lieu of combining these in one law—an approach we believe is unprecedented globally—Vietnam should separate the three main themes and seek extensive dialogues on how to approach them with all interested experts and other stakeholders.

Cybersecurity: Cybersecurity is rightly a priority for all governments. The ICT industry shares the goal with governments of improving cybersecurity, and therefore our interests are fundamentally aligned in this area. As both producers and users of cybersecurity products and services, ITI's members have extensive experience working with governments around the world

[1] See attached list of ITI member companies.
[2] Many of the topics Vietnam includes as "information security" topics are those we term broadly to be cybersecurity, hence our use of that term throughout this document.

on cybersecurity policy. Further, ITI members are global companies located in various countries. Most ITI member companies service the global market and have complex supply chains in which products are developed, made, and assembled in multiple countries across the world. As a result, ITI members understand the impact of international policies on security innovation and the need for governments' policies to be globally compatible.

We believe there are helpful things the Government of Vietnam can do, but to be effective, any governments' efforts to enhance cybersecurity must follow a set of principles that ITI and our member companies developed to guide all policymakers in this area.[3] Any efforts to improve cybersecurity must:
1) Leverage public-private partnerships and build upon existing initiatives and resource commitments;
2) Reflect the borderless, interconnected, and global nature of today's cyber environment;
3) Be able to adapt rapidly to emerging threats, technologies, and business models;
4) Be based on effective risk management;
5) Focus on raising public awareness; and
6) More directly focus on bad actors and their threats.

ITI concurs with portions of Vietnam's draft law, noted below. At the same time, it is imperative that Vietnam establish a globally compatible cybersecurity policy approach that considers cybersecurity, innovation, and trade. The current cyber-threat environment evolves rapidly and requires a complex and layered approach to security that varies greatly across industry sectors. Further, businesses must adapt their risk management strategies faster than regulatory processes can move, and a static compliance approach risks encouraging some firms to invest only in meeting requirements that are outmoded before they can be published. A one-size-fits-all approach also could divert scarce security resources from areas requiring greater investment towards areas with lower priority. These outcomes could decrease Vietnam's security.

Personal information: Regarding personal information, we believe that laws relating to personal information can both provide the necessary protections to personal information, while at the same time allow industry to utilize personal information that fosters innovation and enables the provision of the products and services that consumers expect.

The Asia-Pacific Economic Cooperation (APEC) forum, in which the Republic of Vietnam is a member economy, has developed a Privacy Framework that includes principles that promote a flexible approach to information privacy protection and avoids the creation of unnecessary barriers to information flows.[4] We are concerned that the draft law does not allow for the flexibility that the APEC Privacy Framework endorses. We encourage using the APEC Privacy Framework as a resource in the development of any privacy-related laws.

[3] See The IT Industry's Cybersecurity Principles for Industry and Government, http://www.itic.org/dotAsset/191e377f-b458-4e3d-aced-e856a9b3aebe.pdf
[4] See APEC Privacy Framework at http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

A number of the provisions relating to personal information in the draft law are ambiguous in that it is unclear what requirements companies are being expected to follow. Other provisions mandate certain requirements, without any exceptions. Exceptions are necessary to take into account the different ways in which information is used and shared.

Any modern data protection law should be flexible and focus on outcomes rather than prescribe a rigid set of rules organizations must follow to achieve these outcomes. This is necessary to promote the rapid innovation necessary for competitiveness and economic growth.

Content/filtering: We are not commenting on the provisions of this draft law that relate to the appropriateness of disseminating information that may fall into certain categories on the Internet.

Chapter I- GENERAL PROVISIONS

Article 2: Applicable entity
This states that the law will apply to local or foreign individuals or organizations "directly participating in or related to information security in Vietnam." It is unclear what this means and therefore to whom the law applies.

Article 5: Principles of information security
Item 1) requires individuals and organizations to ensure security on the Internet. Security can never be 100% ensured whether in cyberspace or otherwise. Security is about risk management and taking measures appropriate to the value and consequences of the information in question. Neither is security an end state. Rather, it is a means to advance trust in various technologies that comprise the cyber infrastructure. Industry takes seriously its responsibility to improve security on the Internet but should be encouraged to do so in partnership with governments globally.

Item 2) requires individuals and organizations to inform any information security "infringement or incident" to related competent authorities. As currently drafted, the bill does not describe a threshold for reporting, which could cause unnecessary reporting from sources of little importance to the country thus leading to an overload of unnecessary and unusual information. In cases where incidents rise to the level of importance that reporting is necessary, having undefined parameters may harm both the reputation and security of the victim companies. In many cases public disclosure of an incident could further weaken the security posture of the victim and unnecessarily expose proprietary and other confidential information.

Article 6: State's policies on information security
Overall, we support the emphasis here on training, human resources, growing the market for information security product and service imports, and creating a competitive environment for information security activities, including research and development (R&D). Although we also support the proposal in item 3) to promote technical measures and technology, we are concerned that later in the law Articles 36-38 indicate that the government of Vietnam plans to create its own technical standards. See our comments below on those articles.

Article 7: International cooperation on information security

We strongly support Vietnam's plans to engage in international cooperation on information security. Cyberspace is a global and interconnected domain that spans geographic borders and national jurisdictions. To support the growth, operation, maintenance, and security of this domain, ICT companies continually innovate and invest in the development of globally deployable products and services. Further, cyberspace's stakeholders - consumers, businesses, governments, and infrastructure owners and operators - seek a consistent, secure experience in cyberspace. Thus, efforts to improve cybersecurity should reflect cyberspace's borderless nature and be based on globally accepted standards, best practices, and assurance programs. We urge Vietnam to join discussions with other governments about promoting global approaches.

Chapter II- INFORMATION SECURITY ON INTERNET

Article 9: Category of information system

We support governments categorizing their own information technology systems for the purposes of determining appropriate security controls. We understand that the Government of Vietnam is interested in learning best practices in this area.

In the United States federal computer systems are categorized by a legal definition as either national security or non-national security systems.[5] The U.S. Federal Information Security Management Act (FISMA) of 2002 mandates that U.S. federal non-national security computer systems must use computer security standards developed by the National Institute of Standards and Technology (NIST). NIST's standards are developed in an open, transparent manner using extensive stakeholder input, including public comment processes. In addition, the U.S. Office of Management and Budget (OMB), in its annual reporting instructions, mandates that U.S. federal agencies must use NIST's computer security standards as well as guidelines.[6] The National Security Agency (NSA) is responsible for writing standards for national security systems.

The U.S. Government does not categorize information systems used by the private sector, nor does the U.S. Government mandate particular security standards on the private sector based on information system type. The NIST standards and guidelines referenced above are mandatory only for U.S. federal computer systems considered "non-national security," as noted above. NIST's standards are not mandatory for U.S. state or local governments or the private sector.

Article 10: Scope of information system protection

We appreciate that Vietnam seeks to manage information systems security risks. However, Article 10 would provide authority to the government to develop regulations regarding design, construction, management, operation, use, upgrades, and cancellation of information systems and to apply related measures. We urge the Government of Vietnam to undertake a broad dialogue

[5] This definition was most recently included in the U.S. Federal Information System Management Act (FISMA) of 2002 (see http://csrc.nist.gov/policies/FISMA- final.pdf). This categorization is not by agency, but by computer system. Even a national security-related agency, such as the U.S. Department of Defense (DOD) or the Department of Homeland Security (DHS), will have both national security and non-national security computer systems. The level of security for each type of system is distinct. The vast majority of U.S. federal computer systems are "non-national security."

[6] See http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf, p. 5.

with industry to further discuss and refine the need for such regulations. For Vietnam, it is very important that the industry and the market be allowed to innovate, develop and deploy the security technologies most appropriate to their needs.

Article 12: Responsibility to protect crucial information system at national level
We support Vietnam's goal to strengthen the security of its government information systems. See our comments on Article 9 above for a description of the U.S. approach in this area.

Article 13: Responsibility to protect crucial information system at ministerial, industrial, and local level
While we support Vietnam's goal to strengthen the security of ministerial government information systems, we urge Vietnam not to impose broad requirements on industry owned and operated systems. Per our general comments on p. 2, the cyber-threat environment evolves rapidly, and risks and risk management approaches vary widely across sectors.

Article 14: Classification and protection of information
This Article would require organizations and individuals to classify their information based on importance and to have "suitable protection methods." Similar to our comments on Article 13, we urge the Government of Vietnam not to impose specific requirements on private enterprises or individuals. Cybersecurity efforts must be dynamic and flexible to effectively leverage new technologies and business models and address new, ever-changing threats. Further, governments are unlikely best placed to know what steps should be taken.

Instead of a regulatory approach, Vietnam should seek to raise awareness among its business and citizens about what they can do to improve cybersecurity. Cyberspace's stakeholders - consumers, businesses, governments, and infrastructure owners and operators - need to know how to reduce risks to their property, reputations, and operations. However, many stakeholders are not aware of and also do not adequately utilize the range of tools available to them to do so, such as information sharing, risk management models, technology, training, and globally accepted security standards, guidelines and best practices. Raising awareness so that cyberspace's stakeholders can use these tools is critical to improving cybersecurity.

Article 16: Response in case of network incident
This article contains a number of unclear requirements related to responding to network incidents- for example, the terms quickly, accurately, effectively, and timely are not defined.

Chapter III- PERSONAL INFORMATION PROTECTION

Article 27: Responsibilities of organization handling personal information
1. This provision appears to require all businesses to publish their policies on handling and protection personal information. However, when a company does not interact directly with the consumer, such publication should not be necessary. Companies operating purely in a business-to-business capacity should not be subject to the same publication requirement with regard to their policies with respect to personal information.

2. It is unclear what is meant by "not establishing the consent default mechanism." This appears to be some restriction on how consent can be obtained, but greater clarity is necessary. Further, (b) appears to not permit obtaining consent for new uses of information. Companies should be permitted to seek consent for new planned uses of information.

3. This provision does not allow for sharing unless "consent" has been obtained. First, it is unclear how "consent" must be obtained. Further, a strict prohibition on the sharing of information does not allow for sharing that may be necessary. For example, companies may need to share information for fraud detection and prevention, identity verification, the improvement of analysis services, and to respond to law enforcement requests.

4. This provision requires that in all instances, personal information must be updated, amended, or "cancelled" at the request of the individual. First, companies need to be able to closely examine these requests to ensure that they are in fact requests from the specific individual, and not a fraudulent actor. Further, there are circumstances under which "cancelling" (or "deleting") the information is not practical, considering other requirements to which the company may be subject. In addition, companies should have the option of de-identifying information as an alternative to deleting information.

5. This provision refers to a "storage time," but it is unclear what that means. Also, greater clarification is needed on what is considering an "invalid" purpose.

6. This provision refers to "insurance." Clarification is needed as to what this requires.

Article 28: Rights and obligations of subject of personal information

This Article appears to repeat provisions that appear in earlier articles. With respect to updating, amending, or removing information, companies need to be able to determine whether the request is actually coming from the actual individual. Also, in certain situations, updating or removing information may not be practical or feasible in light of other requirements.

Article 29: Obligation of state management agencies in online personal information protection

1. This provision appears to allow government agencies to enter the premises of companies for the purpose of examining and inspecting their processing personal information practices. Reasonable notice, at a minimum of 30 days, should be required prior to any on-site examination, and there should be limitations so that companies are not subject to examinations every year. Also, it is unclear which "state management agencies" will have the ability to conduct these examinations.

2. It is not clear what "informative channels" will require. Greater clarification is necessary.

3. This provision indicates that state management agencies can promulgate additional regulations and instructions. Greater clarification is necessary on the scope of these additional requirements.

Chapter IV – CRYPTOGRAPHY AND PRIVACY OF INFORMATION

Regarding this chapter, ITI concurs with the separate, specific comments submitted by the Semiconductor Industry Association (SIA).[7] We provide additional comments below.

This chapter's regulatory approach to cryptography in Vietnam's commercial market risks stymieing the growth of ICT, Internet, and e-commerce use in Vietnam. Cryptography is now the foundation of Internet and e-commerce development – and therefore economic growth. Thus, it also underpins security. Vietnam's proposed approach to cryptography, in which licenses and certification are required and the Government will control levels of encryption used, will result in less cybersecurity- the opposite of Vietnam's intentions in this law.

Recent market trends have driven the use of encryption in everyday commercial ICT products, including tablets, smartphones, computers, software, and web browsers. In fact, nearly all ICT products contain cryptographic capabilities. The vast majority of businesses use encryption for email and database security, data transfer, and online payments. Consumers use it to protect and secure their personal information held in smartphones or computing tablets or on the web. Governments use it to provide secure services online. An approach based on the unrestricted import, use, manufacturing, and sale in Vietnam's commercial market of products with cryptographic capabilities will ensure its consumers and businesses access to the best products and technologies available in the global marketplace for security and privacy in and across a variety of ICT products and systems. In addition, access to leading-edge technologies is the best defense against online crime, fraud, and theft. In short, a global and cooperative approach to encryption will create an environment in which Vietnam's consumers and businesses have trust in online commerce, which is fundamental to increased Internet and e-commerce use.

Chapter V - TECHNICAL STANDARDS AND NORMS MANAGEMENT IN INFORMATION SECURITY

This entire chapter contains numerous requirements related to standards and norms, including that hardware and software comply with technical standards established by Vietnam's Ministry of Information and Communications. Under this structure, it appears that companies must attest to a given product's compliance with security standards and norms, and that Vietnam will issue lists of products that need to meet info security regulations.

We urge Vietnam not to establish its own technical security standards. ITI strongly cautions all governments not to set compulsory security standards for the commercial market– whether ones vendors must follow as they build their products or services, or standards that would guide consumers when purchasing ICT products and services or conducting business with companies. Such an approach could encourage some firms to invest only in meeting static standards or best practices that are outmoded before they can even be published or cause organizations to divert scarce resources away from areas requiring greater investment towards areas with lower priority. To maintain (rather than restrain) innovation and to prevent the development of single points of

[7] See Semiconductor Industry Association (SIA), "Comments Submitted RE: Draft 2.22 Law on Information Security, Issued by National Assembly, Socialist Republic of Vietnam."

failure, any standards lists should be purely indicative, their use entirely voluntary, and they should always allow organizations to adopt alternative solutions. Defining new, Vietnam-centric standards has many downsides as they may conflict with global standards currently used, such as the Common Criteria and 3GPP, or set new trade barriers.

Globally developed security standards form the foundation of cybersecurity risk management. The ICT industry is committed to global standards because standardized security technologies, practices, and products deployed across the global digital infrastructure enable interoperability and assurance of security policies and controls, security innovation, efficient and effective use of private sector resources, and rapid response to cybersecurity challenges. Global standardization also restrains the emergence of multiple, conflicting security requirements in multiple jurisdictions, which could compromise cybersecurity. However, it is important to stress that there is no one "cybersecurity standard" or set of practices that is applicable across the board. Cybersecurity risk management is complex, including many moving parts, responsible parties, and standards. In addition, the global ICT industry continually establishes new standardization efforts addressing emerging cybersecurity risk concerns.

We urge the Government of Vietnam to take a leadership role in promoting the adoption of industry-led, voluntary, globally recognized cybersecurity standards and best practices, make the preservation and promotion of a global market a primary goal in any product assurance requirements, and avoid Vietnam-specific requirements. We also welcome and encourage Vietnam to participate in standards development activities, particularly in private fora and consortia. In addition, the Government of Vietnam might consider greater action in their own (public sector) use of voluntary, globally accepted standards or generally accepted industry practices for cybersecurity risk management. Indeed, government leadership can demonstrate such standards' importance and may be necessary to overcome economic disincentives to adoption of standards that yield benefits to the network as a whole.

We also are concerned that a list of products that must meet particular security regulations will hinder the growth of Vietnam's ICT market and cybersecurity. We seek additional information on Vietnam's intentions in this area.

Chapter VI – RESEARCH, DEVELOPMENT AND BUSINESS IN INFORMATION SECURITY

Articles 39-40: Research and development

We strongly agree that governments have a critical role in promoting and accelerating R&D of key cybersecurity technologies. We have long encouraged the U.S. Government to increase its R&D related to security, to help identify R&D gaps and direct resources to emerging security technologies, and to support industry's R&D, and we have the same recommendations for the Government of Vietnam. ITI also recommends that Vietnam seek out industry participation in developing strategies and setting priorities related the cybersecurity-related R&D. Further, Vietnam should promote public-private partnerships for cybersecurity R&D, particularly partnerships that include a multi-disciplinary approach involving the ICT hardware, software, and networking sectors. Finally, Vietnam also should determine if cross-border partnerships in R&D would be helpful. It is possible that some of Vietnam's trading partners—such as the

United States—are also interested in pursuing R&D in certain segments of cybersecurity. If so, joining forces to advance R&D will help all of us get to our goals more quickly.

Article 43: Business conditions of information security services

Item 1) requires providers of information security services "with use of civic crypto" to have licenses to provide these services. Items 3-5 also list numerous license and certification requirements. We urge Vietnam to limit such requirements, as they may hinder the development of Vietnam's information security service industry, which could lead to decreased security.

Article 45: Import license of information security products

We are concerned that a list of information security products that must obtain import licenses will hinder the growth of Vietnam's ICT market and cybersecurity. We seek additional information on Vietnam's intentions in this area.

Chapter VII – HUMAN RESOURCE DEVELOPMENT FOR INFORMATION SECURITY

We agree with the provisions in this chapter regarding education and training.

Conclusion

Please note that our comments are not exhaustive and we may have additional concerns or details. We would be pleased to meet with the Government of Vietnam to discuss our concerns as well as alternative solutions. Please consider ITI as a resource on these issues.

Thank you very much for your consideration.

Sincerely,

Danielle Kriz
Director, Global Cybersecurity Policy

Yael Weinman
Vice President, Global Privacy Policy and General Counsel

Innovation.
Insight.
Influence.

member companies