6 May 2015

PRIVILEGED & CONFIDENTIAL

H.E. Dr. Vishnu Krue-ngam
Deputy Prime Minister
Office of the Deputy Prime Minister
Command Building 1,
Royal Thai Government House Office
Pisanulok Road, Dusit,
Bangkok 10300

Re: BSA Comments on the Cybersecurity Bill

Dear H.E. Dr. Vishnu Krue-ngam

BSA | The Software Alliance (BSA)[1] appreciates the opportunity to submit its comments to the Council of State with respect to the Cybersecurity (the "**Bill**"). The Government of Thailand should be commended for undertaking this important, forward looking effort to ensure the country is prepared to deter and to manage cybersecurity threats. An effective cybersecurity strategy must be built on a solid legal foundation that facilitates coordination between law enforcement, government agencies and the private sector. Of course, such coordination requires a culture of trust that is possible only when the appropriate safeguards and incentives are put into place. Security requirements must, for instance, be duly balanced with the need for protection of privacy and civil liberties. With these principles in mind, we are concerned that the Bill's surveillance provisions (Article 35) may result in unintended consequence, including the undermining of consumer confidence in Thailand's IT systems. BSA therefore offers the following comments that are intended to help achieve the Draft Cybersecurity Act's laudable objective of ensuring "prompt and unified action" in response to cybersecurity threats.

Section 6: The members of the National Cybersecurity Committee

The membership of the proposed National Cybersecurity Committee (the "**NCSC**") is comprised primarily of government entities involved in security and defense, e.g. the Ministry of Digital

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 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. BSA's members include: Adobe, Altium, ANSYS, Apple, ARM, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, Dell, IBM, Intel, Intuit, Microsoft, Minitab, Oracle, salesforce.com, Siemens PLM Software, Symantec, Tekla, The MathWorks, and Trend Micro.

300 Beach Road
#25-08 The Concourse
Singapore 199555

P +65 6292 2072
F +65 6292 369
W bsa.org

Regional Representative Office
UEN: S97RF0005K

Economy, the Ministry of Defense, and the Technology Crime Suppression Division of the Royal Thai Police. To balance out the perspectives of the NCSC and ensure that concerns regarding personal privacy and civil liberties are considered, the NCSC should also include members from the National Human Rights Commission and the Office of the Ombudsman. Having members with various backgrounds will ensure that the rights of individuals are not be inappropriately impacted.

Section 7-34: The broad power of the NCSC under the Bill

BSA supports the idea of the NCSC serving as the centralized facilitator in order to coordinate between all relevant government entities in case a cyber attack occurs. Pursuant to Section 7, the NCSC must, among other things, "prepare an operation plan for national cybersecurity." The Office of the NCSC is charged by Sections 27-28 to develop guidelines, measures, operation plans, and projects relating to cybersecurity. Because the NCSC is afforded broad authority to take action in connection with the cybersecurity plan and related guidelines, it is important that the Act provide clear guidance regarding what constitutes an actionable threat. For instance, upon the occurrence of the cyber attack, Section 33 states that the NCSC can order all government agencies to take any action in order to prevent or mitigate the damage that arises. Likewise, Section 34 extends the NCSC's power to be able to order a private agency to act or not do any act, and notify the NCSC of the results of such operation, on the basis that the threat may affect the financial and commercial stability or national security.

Despite the broad power of the NCSC under these Sections, there is no clear definition of the term "cyber attacks" nor is there a threshold for determining the level of risk necessary to justify NCSC actions. Similarly, the Bill lacks guidance for determining when a risk to "financial and commercial stability or national security" is severe enough to warrant the NCSC to compel action from private entities. Therefore, clear definitions of these broad terms should be incorporated into the Bill so that all affected entities under the Bill clearly understand the position and that there is no more ambiguity.

Section 35 (1) and (2): Government Requests for Information, Action

Section 35 (1) of the Bill empowers the officials assigned in writing by the secretary-general of the Office of the NCSC to be able to send letters to demand clarification, or call in any government agency or person to give a statement, send a written explanation, or send any account, document, or evidence, for inspection or for information, in order to comply with the Bill.

Section 35 (2) further empowers officials to send letters requesting that a government agency or private entity take "action to facilitate the actions and duties of the NCSC".

To ensure that these broad powers are not potentially abused, it is essential for the Thai government to set out specific rules that define the type and scope of information the officials can request, and the circumstances under which the Office of the NCSC can compel a private sector actor to perform a specific action. Such rules should define who within the Office of the NCSC may make requests for information and impose handling restrictions to ensure that private information obtained by the NCSC is appropriately safeguarded. Moreover, exercise of these broad authorities should be strictly limited to circumstances where there is a specific and credible cybersecurity risk.

Section 35 (3): Surveillance Authority

Section 35 (3) empowers NCSC officials to access information communicated by post, telegraph, telephone, facsimile, computer, or electronic tool or equipment, or any information technology media, for the benefit of operations to secure cybersecurity. This broad delegation of surveillance authority provides NCSC with virtually unfettered access to communications networks, and thus raises significant privacy concerns. Section 35 (3) lacks the necessary balance between national security and data privacy as the government may exercise its discretion without judicial review, e.g. there is no clause which requires that a warrant be obtained from the court prior to accessing private communications. The statute simply provides that the officials may access such information if there is a written permission letter from the secretary-general of the Office of the NCSC.

From a commercial perspective, Section 35 (3) of the Bill is likely to hinder IT investment in Thailand. Any business with an IT system could be subject to Section 35 (3) of the Bill, from banking and financial to retail businesses. As such, providers cannot guarantee that their users' personal data, trade secrets, or stock purchase history can be kept confidential. As a result, IT businesses may refuse to use or invest in IT systems in Thailand, which will undermine the effort to turn Thailand into an IT hub for the ASEAN Economic Community.

The lack of checks and balances within Section 35(3) stands in contrast with Thailand's approach to data privacy in existing law and in the proposed Computer-Related Crimes Act. For instance, Section 25 of the Special Case Investigation Act B.E. 2547 (the" **Special Case Act**") contains similar authority to access private information if there is a reasonable ground to believe that any media has been used to commit a Special Case offence. Importantly, Section 25 of the Special Case Act requires the Special Case Inquiry Official to submit an ex parte application to obtain a criminal court order in order to access such information. Also, the court may grant permission for a period of no more than 90 days per each permission.
Likewise, under the proposed Computer-Related Crimes Act, law enforcement officials must obtain a court order in order to compel intermediaries to disclose the content of user communications.

Leading from this, it is suggested that Section 35 (3) of the Bill requires a court order to access private information and also that such order be valid only for a limited period of time. There should also be a probable cause of harm to national security before officials under the Bill could resort to Section 35. Finally, we recommend that an independent body, such as the Personal Data Protection Committee that is proposed by the Personal Data Protection Act, be given the authority to monitor the NCSC's usage of its powers under Section 35 (3) to ensure privacy interests are adequately balanced with the need for surveillance.

Conclusion

BSA appreciates the Thai government's attempt to protect any infrastructure from cyber attack and cyber terrorists, however, the official authority under the Bill should provide transparency and not undermine user privacy, which may adversely impact digital economy plans. Moreover, cooperation of the private sector in notifying the government when there is any security breach of their systems should be highlighted in order to prevent cyber attacks for the sake of national cybersecurity. Unfortunately, wide authority of the NCSC and/or the officials under the Bill may create fraud, mistrust and reduce cooperation of the private sector in notifying cybersecurity breaches. While the existence of Sections 5(4), 7(8), 17 (2), 17(3), and 18(3) seems to promote cooperation between the public and private sectors in preventing cyber attacks, the private sector may be reluctant to share information with the government for fear of the government requesting irrelevant information or intercepting their private communications via IT media.

Therefore, BSA humbly requests the Council of State to thoroughly consider the above for reasons of transparency and to create trust between the public and private sectors, while preserving national cybersecurity.

We remain open to further discussion with you at any time. Please feel free to contact **Ms. Varunee Ratchatapattanakul, BSA's Thailand Representative, at varuneer@bsa.org or +668-1840-0591** with any questions or comments which you might have.

Thank you for your time and consideration.

Yours sincerely,

Boon Poh Mok
Director, Policy, APAC
BSA │ The Software Alliance

Cc:
1. The Secretary-General, Office of the Council of State
2. Mrs. Surangkana Wayuparb, CEO, the Office of Electronic Transactions Development Agency (Public Organization)