November 30, 2018

Ms. Ajarin Pattanapanchai
The Permanent Secretary
Ministry of Digital Economy and Society
120 Moo 3, 6-9 floor
The Government Complex Commemorating His Majesty
Chaeng Watthana Road,
Thung Song Hong, Khet Laksi Bangkok 10210

BSA COMMENTS ON NATIONAL CYBERSECURITY BILL

Dear Ms. Pattanapanchai,

Introduction and Statement of Interest

BSA | The Software Alliance (**BSA**)[1] thanks the Ministry of Digital Economy and Society (**MDES**) for the opportunity to provide our comments on the National Cybersecurity Bill that was posted on www.lawamendment.go.th for public consultation on November 16, 2018 (**the Bill**).

BSA commends the MDES for undertaking this important effort to ensure Thailand is prepared to deter and manage cybersecurity threats as well as having an open and responsive process to incorporate multi-stakeholder feedback into the draft Bill.

Our members have a significant interest in Thailand's National Cybersecurity Bill. In this regard, BSA has provided comments to the previous versions of the Bill. These submissions are linked to this document as follows:

- BSA Comments on National Cybersecurity Bill (October 12, 2018)
- Joint Industry Comments on the Cybersecurity Bill – Supplemental (May 21, 2018);
- Joint Industry Comments on the Cybersecurity Bill (April 17, 2018); and
- BSA Comments on the Cyber Security Bill (May 6, 2015).

[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.

Many of the comments described in the above listed submissions remain relevant for the current version issued for public comment on November 16, 2018. In addition, below we provide the following specific comments to the current bill.

Comments and Recommendations

The current version of the Bill contains improvements over previous versions and encapsulates fundamental elements of an effective cybersecurity legislative framework for the Thai people. These improvements include: the removal of circumstances for the authority of the Office of the National Cybersecurity Committee that could lead to potential conflict of interest (Section 18); the introduction of due process (Sections 58 – 59) and appeal mechanisms for information access (Section 47 and Section 60); as well as stronger protections for confidentiality (Sections 61 – 63). Nonetheless, the Bill can be improved to provide further clarity for software or technology service providers, providing services to Critical Information Infrastructure (**CII**) Agencies. The following paragraphs summarizes our concerns and provide recommendations for MDES' further review.

A. Framework for due-process and appeal mechanisms should be clearer and provide general avenues for recourse and appeals.

BSA generally supports the inclusion of due process and appeal mechanisms for both CII Agencies (Section 47) and other entities that receive authoritative instructions pursuant to Part 4 of the Bill in *Response to Cyber Attacks* (Section 60) for cyberattacks having a general level of impact. Furthermore, BSA welcomes the effort that MDES has made to differentiate between the different levels of impact for cyberattacks (Section 54) – general level, significant level, and critical level of impact – and creating a tiered framework for responding to the different levels of cyberattacks. Nonetheless, the framework for due process can be enhanced further and additional clarity can be provided as follows:

1. **Court orders should be served to CII agencies rather than their service providers**. The Bill should be clearer on the process by which entities are served with court orders. CII agencies retain the ultimate responsibility for the cybersecurity of the CII and the Bill should not place liability on third-party vendors. In addition, any CII agency can and likely would avail services from more than one third party vendors. Direct serving of orders on third-party vendors may also place them in an untenable situation of needing to breach contractual agreements they have with the CII agency customers (e.g. regarding confidentiality and data protection) or their legal obligations under other jurisdictions. Accordingly, any court order should therefore be served on CII agencies, who can then instruct their third-party vendors to take the necessary action or provide access to information as requested by the National Cybersecurity Committee (**NCSC**).

2. **Any exception to obtaining a court order should be precisely-worded.** We continue to recommend that the "urgency" exception for incidents with a "critical level of impact" (Section 59, paragraph 3) should be clearly limited to situations where there is a probable cause of harm to national security. In this regard, where the "urgency" exception applies, the Thai legal system should provide a corresponding document such as a warrant or a "temporary emergency document" that would define the requirements of the provision or seizure of information.

3. **Right to appeal an authoritative instruction should be extended to all cyberattacks, regardless of level of impact.** All compelled actions and information provisions (including seizures) 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 in *all* cases. In this regard, any exceptions, including the

"urgency" exception, should be well-defined and narrow.

Providing the right to appeal *only* to cyberattacks with a "general level of impact" (Section 60) is disproportionate and does not provide sufficient levels of due process safeguards. Without adequate due process safeguards and avenues for appeals, requests for information can amount to an invasion of privacy that would undermine consumer trust as businesses cannot guarantee that personal data or confidential information will be protected from unauthorized access. Likewise, other compelled actions, such as requiring the monitoring 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.

Furthermore, imposition of such requirements without due process would result in a conflict of laws with other countries' regulatory regimes and create significant compliance challenges for international companies.

4. **An independent body should have oversight over the NCSC's powers.** We reiterate that an independent body be given the authority to monitor the NCSC's exercise of its powers to access private agency information to ensure privacy interests are adequately balanced with the need for surveillance.

B. Certification, standards, or codes of conduct must leverage existing best practices and global industry-led standards

Standards and best practices are most effective when developed in collaboration with the private sector, adopted on a voluntary basis, and recognized globally. Thailand should align any practices and standards it issues 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. Allowing CII operators to combat evolving cyber threats with evolving best practices and standards permits a more flexible, current, and risk-based approach to cybersecurity. This will also help realize economies of scale as well as readiness in line with the best of the world.

C. Composition of the National Cybersecurity Committee, National Committee on Cybersecurity Supervision, the National Committee on the Promotion of Critical Information Infrastructure, and other associated committees and sub-committees.

In BSA's comments on previous versions of the Bill issued in 2015 and in March and October 2018, BSA highlighted that the proposed NCSC should be expanded to include members that represent the interests of personal privacy and civil liberties of individuals, such as the National Human Rights Commission and the Office of the Ombudsman. In addition, BSA also recommended that the NCSC include members from industry, as this would ensure that a range of viewpoints were represented and enhance cooperation between the public and private sectors to drive best practices.

In the current version of the Bill, the NCSC and other proposed new associated committees and sub-committees still do not explicitly include members that represent the interests of industry, personal privacy, and civil liberties of individuals. Section 20 of the current Bill includes a Board of the Office of National Cybersecurity Committee (**Board**) with civilian-focused designations, including the Permanent Secretary of MDES as Chairperson. **BSA supports the involvement of civilian-focused agencies but urges that the Board and associated committees should likewise include representation from civil society and private sector stakeholders**.

D. Confidentiality

BSA supports the inclusion of criminal penalties for officials and inquirers that misuse information and data compelled pursuant to the powers specified under the Bill (Sections 61 – 63).

In addition, we continue to recommend the inclusion of **categories of information which are exempted from disclosure** such as 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.

E. Transition Period of the Law

We repeat our recommendation that the Government of Thailand make the proposed cybersecurity law purely prospective and provide a reasonable period of time between the enactment of the law and its effective date. **BSA recommends MDES to provide for a transition period *not less than two years after the law is issued before the law comes into effect*.**

Conclusion and Next Steps

BSA appreciates the Government of Thailand's open and consultative process for the development of the Cybersecurity law. We humbly request that MDES thoroughly consider the suggestions above.

To ensure consumers and businesses alike can trust in and reap the maximum benefits from data-driven innovations like artificial intelligence and Internet of Things, BSA's members provide essential security technologies to protect them from cyber threats. BSA has worked closely with governments around the world on cybersecurity policy and legislative development and encourages the Thai Government and MDES to take reference from international best practices[2] when developing, implementing, and operationalizing cybersecurity-related rules and requirements.

We remain open to further discussion with you at any time. Please feel free to contact **Ms. Varunee Ratchatapattanakul, BSA's Thailand Country Manager, 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,

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

Cc: Dr. Pichet Durongkaveroj, Minister of Digital Economy and Society
Mrs. Surangkana Wayuparb, Managing Director of Electronic Transactions Development Agency

[2] BSA encourages the Thai Government and MDES to take reference from international best practices, such as the National Institute of Standards and Technology's Cybersecurity Framework (https://www.nist.gov/cyberframework) and *BSA International Cybersecurity Policy Framework* at: https://bsacybersecurity.bsa.org/wp-content/uploads/2018/04/BSA_cybersecurity-policy.pdf.