



October 12, 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 Lakxi 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 September 27, 2018 (**the Bill**).

BSA represents the global software industry. Our members are at the forefront of data-driven innovation, developing cutting-edge advancements in artificial intelligence (**AI**), machine learning, cloud-based analytics, and the Internet of Things (**IoT**) that drive the global information economy and improve our daily lives. Our members earn users' confidence by providing essential security technologies to protect them from cyber threats. These threats may be posed by a broad range of malicious actors including those who would steal our identities, harm our loved ones, steal commercially valuable secrets, or pose immediate danger to national security.

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

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.

(**Framework**), which sets out a recommended model for a comprehensive national cybersecurity policy.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 Framework³ and those outlined in BSA's Framework, when developing, implementing, and operationalizing cybersecurity-related rules and requirements.

Our members have a significant interest in Thailand's National Cybersecurity Bill. BSA, in collaboration with the US-ASEAN Business Council, provided comments to the previous versions of the Bill. These submissions are appended to this document as follows:

- Annex A: Joint Industry Comments on the Cybersecurity Bill (April 17, 2018);
- Annex B: Joint Industry Comments on the Cybersecurity Bill – Supplemental (May 21, 2018); and
- Annex C: BSA Comments on the Cyber Security Bill (May 6, 2015).

BSA wishes to once again commend the MDES for undertaking this important effort to ensure Thailand is prepared to deter and manage cybersecurity threats. As cybersecurity threats grow more sophisticated and dangerous, the risk of an insufficient or poorly calibrated national policy for countering cyber threats is potentially catastrophic.

Detailed Comments

The current version of the Bill contains significant improvements over previous versions and encapsulates the fundamental elements of an effective cybersecurity legislative framework for the Thai people. We recognize the importance of the Bill in providing the necessary legislative framework to protect critical information infrastructure (**CII**), and the current version makes it clear that this is the Government of Thailand's main policy objective. However, the Bill also includes several concerning provisions that distract the proposed legislation from its stated policy objective. For example, the removal of requirements for due process for information access threatens to create unreasonable burdens and legal uncertainty for the technology sector. The following summarizes our key concerns in this submission:

- Scope of Application and the Bill's Interaction with Other Laws;
- Composition of the National Cybersecurity Committee (**NCSC**) and the Supervisory Committee of the Office of the National Cybersecurity Committee (**Supervisory Committee**);
- Powers of the NCSC;
- Surveillance Authority;
- Criminal Liability;
- Confidentiality;
- Information Sharing;
- Additional Elements of a National Cybersecurity Policy

The following paragraphs provide detailed comments and recommendations for further review.

² 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/>.

³ 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>.

A. Scope of Application and the Bill's Interaction with Other Laws

BSA generally supports the revised scope of the current version of the Bill. Specifically, narrowly applying most of the provisions related to notification, reporting, management, and incident responses (Sections 38-58) only to information systems of state agencies and private sector companies (or **private agencies**) that carry out CII functions is a positive development. Nevertheless, the Bill can benefit from further clarifying the definition of CII and the scope of application of the Bill as follows:

1. **The concept of “critical infrastructure” should be consistent with international practice, and defined instead as:**
 - **“those assets, services, and systems, whether physical or virtual, which, if destroyed, degraded, or rendered unavailable for an extended period, would have a large-scale, debilitating impact on national security, public health, public safety, national economic security, or core local or national government functions.”**

Hence, specific critical infrastructure should be identified by the NCSC based on an analysis of criticality, interdependency, and risk, rather than simply defining as CII the information infrastructure in seven sectors broadly defined as critical infrastructure in Section 43, giving no regard for whether only specific critical infrastructure within each sector should be included. Furthermore, criticality should be considered with respect to the impact on Thailand.

2. **Organizations that are “private agencies” for CII should be more clearly delineated.** There could be scenarios where more than one party could fulfil the definition of a private agency for CII for the same CII, for example, if business operations are outsourced to third-party vendors. We recommend that a clear framework for designation of CII private agencies should be established and incorporate the following concepts:
 - CII private agencies should be identified only as those entities which have effective control over the CII or are responsible for the CII, and these would be the legal owners of the CII assets.
 - In situations where there is more than one such entity, NCSC should identify all such owners in consultation with the sectoral regulators.
3. **CII private agencies should be clearly responsible for ensuring that their vendors comply with security requirements.** CII private agencies should retain the ultimate responsibility for the cybersecurity of the CII and the Bill should not place liability on third-party vendors. The Bill should also make clear that CII private agencies can impose cybersecurity requirements contractually on their vendors.
4. **The interaction between the Bill and other sectoral laws should be clear.** It is currently unclear how the Bill would be implemented vis-à-vis other sectoral requirements, such as those from the Bank of Thailand, the Securities Exchange Commission, and the Office of Insurance Commission, among others. Specifically, it is unclear whether there would be duplicated reporting to the NCSC and the sector regulators, or whether the NCSC might issue instructions that potentially conflict with those from sector regulators. BSA urges that MDES includes provisions in the Bill to make the interaction between the Cybersecurity law and other sectoral laws clear.

B. Composition of the National Cybersecurity Committee and the Supervisory Committee of the Office of the National Cybersecurity Committee

In BSA's previous comments to previous versions of the Bill issued in 2015 and March 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. We also recommended that cybersecurity efforts be led by a civilian government organization. Due to the broad ramifications of cybersecurity incidents for Thailand's national and international economic interests, it is critical that these interests are well represented on the NCSC. 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 still does not include members that represent the interests of personal privacy and civil liberties of individuals. Therefore, there continues to be a heavy emphasis on law enforcement and defense within the NCSC, with the Minister of Defense being appointed as the Vice-Chairman of the NCSC.

Section 19 of the Bill includes a Supervisory Committee with civilian-focused designations, including the Permanent Secretary of MDES as Chairperson. **BSA supports the involvement of civilian-focused agencies but urges that the Supervisory Committee should likewise include representation from civil society and private sector stakeholders.**

C. Powers of the NCSC

BSA remains supportive of empowering the NCSC to act as a centralized coordinator for inter-agency responses to cyber-attacks and cyber incidents, pursuant to Section 9 of the Bill. Tasking a single national body with lead responsibility for cybersecurity ensures clarity, coherence, and coordination in the government's preparedness for and response to cybersecurity threats and challenges. Furthermore, BSA also acknowledges the limitation in Sections 56-58 of the NCSC's broad authorities to circumstances involving only "severe cyber-attacks". However, it is not appropriate for the responsibilities of private agencies that carry out CII functions to be the same as state agencies and BSA suggests introducing limits that more appropriately reflect the difference in responsibilities and roles that state agencies and private agencies should play in managing cybersecurity. BSA's concerns relating to the scope of NCSC powers follow:

1. **The NCSC's powers should only apply to CII providers that operate or control critical infrastructure in Thailand.** Multinational organizations with offices in Thailand may be supported by infrastructure and IT system located wholly outside of Thailand. The Bill must be clear that "computers" and "computer systems" located wholly outside of Thailand should not be designated as CIIs due to potential conflicts with other countries' regulatory regimes.
2. **The broad powers in Sections 56-58 triggered by "severe cyber-attack" should be defined according to international best practices.** We continue to recommend defining a "severe cyber-attack" as follows:
 - **"a cyber incident resulting in: (i) the unauthorized or denial of access to or damage, deletion, alteration, or suppression of data that is essential to the operation of critical infrastructure; or (ii) the defeat of an operational control or technical control that is essential to the security or operation of critical infrastructure."**

We also recommend including a definition for “cyber-attack” as follows:

- **“an action intended to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transitioning an information system.”**

Furthermore, the Bill should more clearly specify the severity thresholds for the exercise of investigative powers to provide clarity on the scenarios in which they could be used.

3. **Limits should be introduced to NCSC’s powers requiring private agencies to take action (Sections 38, 40, 44, 45-50, 53-58).** The overly broad powers granted to the NCSC have the potential to run contrary to the aims of protecting civil CII and could discourage private sector collaboration in addressing threats to CII. Hence, the powers granted to the NCSC should be more precisely defined and limited by independent oversight and judicial review. Private agencies should be afforded clear opportunities to contest orders and rights to appeal adverse decisions in Court. Further, it appears that previous limits on certain powers that required court orders (except in urgent circumstances) have been removed from the current version of the Bill. **We strongly urge that these limits requiring court orders be reinstated. In addition, we urge that independent oversight and judicial review should apply more broadly to all NCSC powers when exercised in relation to “private agencies”.**

In particular, the stipulations under Section 46 are overly broad and appear to contradict Thailand’s Personal Data Protection Bill issued by the MDES as well as internationally-established best practices. Thailand’s Personal Data Protection Bill was recently revised in order to align with principles from the European Union’s General Data Protection Regulation (**GDPR**), but the level of protection afforded to data subjects under the draft Cybersecurity Bill is inconsistent with the protections they ought to have under the GDPR data privacy principles. The second paragraph under Section 46 goes so far as to seek to nullify all laws that may be applicable to a private agency and contracts used to ensure proper means of information disclosure and appropriate protection of data subjects and commercial rights. This not only goes against internationally recognized best practices in data protection, but would also be near impossible to enforce, particularly if a private agency is subject to laws outside of Thailand that would contradict their responsibility under this Section 46.

We recommend that this inconsistency be addressed by **narrowing the range of data covered in Section 46.1-3, and by incorporating a judicial process by which private agencies can have an opportunity to assert any contradictory rights they may have.** In addition, we recommend **removing paragraph two of Section 46** that states “...agencies receiving the letter under paragraph one shall not claim that they have a duty under other laws or under contracts, in order to prevent themselves from disclosing such information. In this regard, an undertaking in compliance with this Section executed in good faith shall not be deemed to violate laws or contracts.”

In addition, even in instances where the NCSC seeks to authorize the seizure of a computer *without* judicial determination – for example in the event of a severe cybersecurity threat or incident, where there are urgent circumstances – the NCSC should ensure that there is no less disruptive method of achieving the purpose of the investigation. Furthermore, such seizures should be done after consultation with the private agency and having considered the importance of the computer to the business and operational needs of the private agency and that the benefit of seizure outweighs the detriment caused to the private agency.

4. **Baseline threshold throughout the current version of the Bill for obligations imposed on private agencies, should be restricted to actions which are *reasonable and practical*.**

We remain concerned that certain obligations on private agencies under the current version of the Bill (including, for example, under Sections 56 and 58) require them to take certain actions in the event of a cyber incident which may not be within their control, or which may be unreasonable, impractical, or disproportionate in the circumstances.

Any obligations on private agencies (including to take actions, provide physical or logical access, provide information, and/or provide documents, report, etc.) must be only pursuant to a valid and binding judicial order or warrant. Additionally, the Bill should specify that such requests must be specific and clear in scope, pertain only to information or documents over which the private agency exercises control, commercially reasonable, and proportionate in the circumstances. These suggested changes account for the commercial realities that private agencies are not in the same position as government agencies and the Bill should not create commercially unsustainable or disproportionate obligations on them.

For example, many of the actions listed in Sections 57 and 58 are not reasonable or practical for private agencies to act on, as they may involve fundamental changes to their business model in order to be able to respond, and in doing so, they may affect their ability to continue to provide services at scale to other customers. One notable example is Section 58.1 which gives the Secretary-General the power to “confiscate any computer or equipment that has reasonable grounds to believe it is related to a cyber-attack for inspection or analysis.” **Private agencies’ obligations should be limited to taking actions which are within their control and commercially reasonable within the circumstances to implement.**

It is also not reasonable or practical to expect private agencies to report anticipated cyber-attacks. **The requirement to report “in the event a cyber-attack is likely to occur” in Section 51 should be removed.** The types of cyber-attacks and sources of those attacks are constantly evolving. In this environment, certain services are subjected to thousands (or more) attacks every day, most of which are successfully defended. While organizations can have measures in place designed to protect against cyber-attacks using the latest industry practices, it is simply not possible to identify every threat or to notify authorities of every attack “likely to occur”. Moreover, notification in the absence of established risk may create “notification fatigue,” leading to undue inconvenience for private agencies as well as the possibility that private agencies will fail to take appropriate action in response to notifications that indicate a real risk of harm.

Hence, there is a need for the Bill to include provisions that balance the need for operational expediency with safeguards that ensure NCSC actions are proportionate and judicious. **We recommend that for severe cybersecurity threats or incidents occurring on CII systems, the NCSC should determine the appropriate measures to take during investigations in consultation with the sector regulator and CII private agency.**

5. **Sections 56-58 should be limited to only those entities which are *directly impacted* by severe cyber-attacks.** This would avoid any suggestion that private agencies which are *not* impacted would be subject to these obligations.

D. Surveillance authority

BSA is very concerned that the current version of the Bill has removed the requirement for a court order authorizing access to a private agency’s communications information. In this regard, BSA submits the following recommendations:

1. **BSA strongly recommends that the requirement for a court order authorizing access to communications information be reinstated.** All compelled 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. The Thai legal system should provide a document such as a warrant or a “temporary emergency document” that would define the requirements of the provision or seizure of information.

Without adequate due process safeguards, surveillance 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. 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 organizations.

2. **Any exception to obtaining a court order should be precisely-worded.** We recommend that the “urgency” exception should be limited to situations where there is a probable cause of harm to national security.
3. **An independent body should have oversight over the NCSC’s powers.** We again recommend that an independent body, such as the Personal Data Protection Committee that is proposed by the Personal Data Protection Bill, 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.
4. **Additional requirements should be included in the process for requesting access to and obtaining such information.** These include:
 - **As a pre-qualifier, all orders, commands, or requests for information or assistance must be clear in scope, reasonable in the circumstances, and limited to situations where there is a significant risk of serious harm.** We recommend that any such harm should be balanced against other criteria, such as the impact on the community and commercial and other practical considerations. Without the inclusion of such limits and safeguards, compelled information sharing tends to result in minimum essential compliance statements from organizations that are victims of attack or breach rather than robust efforts of collaboration.
 - **Requests for information from a private agency should be subject to exemptions and notification to affected third parties.** We suggest that third parties whose information may be disclosed in this process have a right to be informed in advance in case they wish to contest such disclosure.
 - **Court orders issued should only be valid for a limited period of time.** We recommend that the court order’s period of validity not be open-ended since this would create greater uncertainty for private agencies.
5. **Related sub-regulations and additional rules should undergo a public consultation process before being issued.**

E. Criminal Liability

BSA observes that Sections 62 and 63 of the Bill continue to impose criminal liability for several types of breaches. We continue to recommend that criminal prosecution should only be imposed on those that, with criminal intent, seek to disrupt, degrade, or destabilize cyberspace.

Imposing criminal liability on private agencies that do not comply with the NCSC’s requests

under Section 57 and 58 is excessive. At a minimum, the provisions should be clarified to ensure that private agencies cannot be criminally liable in instances where the failure to comply with an NCSC request is unintentional and/or due to technical constraints, such as a lack of time or technical complications. This position could deter international companies from establishing a presence in Thailand if there is a risk their personnel are exposed to criminal liability for inadvertent or minor breaches.

F. Confidentiality

We note that language in the previous draft of the Bill mentioning confidentiality has been removed from the current version. BSA continues to recommend that the Bill should contain additional specific provisions dealing with the protection of confidentiality of sensitive or personal information. These provisions should include specific obligations on authorities to protect and maintain the confidentiality of such information, including requirements and procedures for obtaining consent and how such information may be used, disclosed, stored, and disposed after it is no longer required by the regulator for its legitimate supervisory purposes.

There should also be **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.

In addition, **NCSC officers should also be held criminally liable should they misuse such information.**

G. Information Sharing

The ability to share information about cybersecurity threats, vulnerability, and cyber incidents with affected parties and other entities with the means to defend against attacks is essential to promoting cybersecurity.

We repeat our recommendation that the current version of the Bill should support the development of robust information sharing policies between the government and the private sector, among private entities, and among government entities. Further, information sharing policies should include limitations on potential liability for sharing entities, protections for the privacy of those affected by the shared information, incentives for facilitating timely and multi-directional information sharing, , and requirements that information is used only to promote cybersecurity.

H. Transition Period of the Law

It is critical for the Government to make any new cybersecurity law purely prospective and to provide a reasonable period of time between the enactment of the law and its effective date. Individuals, businesses, and government agencies will benefit more from an orderly transition than with one that is abrupt and requires catch-up under threat of enforcement. In addition, this transition will provide the time necessary for the Government to issue any compliance guidance for the law and for industry to prepare its compliance assessments. Therefore, **BSA recommends MDES to provide for a transition period before the law comes into effect of not less than two years after the law is issued.**

I. Additional Elements of a National Cybersecurity Policy

BSA also reiterates its recommendation that Thailand's national cybersecurity policy address other important issues, including the implementation of guidelines for government procurement of technology and software, strong government support for cybersecurity technology research and

development, educational campaigns to increase cybersecurity awareness and training, and the integration of cybersecurity cooperation into foreign policy. We encourage the Government of Thailand to address these important issues as part of the implementing regulations to the Bill, once enacted.

Conclusion and Next Steps

BSA applauds the Government of Thailand's efforts to protect infrastructure from cyberattacks and cyber criminals. However, we humbly request that MDES thoroughly consider the suggestions above. By doing so, we believe that MDES has an opportunity to deliver a robust, risk-based national cybersecurity policy that aligns with international best practices, fosters greater trust between the public and private sectors, and enhances the security of data and infrastructure.

The Government of Thailand can also place greater emphasis on pre-emptive protection and mitigation against cyberattacks by encouraging organizations to adopt industry best-practices for cybersecurity. For example, the use of supported and licensed software and hardware that receive constant security updates, in combination with effective network defences and incident response processes and mitigations, will encourage the development of robust cyber hygiene practices.

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 and Development Agency

Annex A:
Joint Industry Comments on the Cybersecurity Bill
(April 17, 2018)



April 17, 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

Re: Joint Industry Comments on the Cybersecurity Bill

Dear Ms. Pattanapanchai

1. Introduction and statement of interest

BSA | The Software Alliance (“**BSA**”)¹ and the US-ASEAN Business Council (**US-ABC**)² represent the leading US technology companies operating in Thailand. Our members are at the forefront of data-driven innovation, developing and offering essential software, security tools, communications devices, servers, and computers that drive the global information economy and improve our daily lives. Our members earn users’ confidence by providing essential security technologies to protect them from cyber threats. These threats may be posed by a broad range of malicious actors, including those who would steal our identities, harm our loved ones, steal commercially valuable secrets, or pose immediate danger to our nation’s security.

Our members thus have a significant interest in the Thai government’s plans to introduce the draft Cybersecurity Bill (the “**2018 Draft Bill**”).

BSA and US-ABC have worked closely with governments around the world in relation to the development of national cybersecurity policies and legislation. In doing so, we have witnessed first-hand the potential for such policy and legislation to effectively deter and manage cybersecurity threats whilst still protecting privacy and civil liberties of citizens.

¹ BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. BSA’s members include: Adobe, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, Box, CA Technologies, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatca, Intel, Microsoft, Okta, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation, and Workday.

² 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.

As a result of this experience, BSA has developed the International Cybersecurity Policy Framework (“**International Framework**”), which sets out a recommended model for a comprehensive national cybersecurity policy. US-ABC strongly supports this framework. We have included a copy of the International Framework with this letter.

In summary, the Framework recommends six overarching principles that should guide the development of a successful national cybersecurity policy, namely that policies should:

1. be aligned with internationally recognized standards;
2. be risk-based, outcome-focused, and technology neutral;
3. rely on market-driven mechanisms where possible;
4. be flexible and encourage innovation;
5. be rooted in public-private collaboration; and
6. be oriented to protect privacy.

2. Joint Industry Comments

BSA commented on an earlier draft of the Cybersecurity Bill in 2015 issued by Thailand's Electronic Transactions Development Agency (“**2015 Draft Bill**”). A copy of BSA's original response is set out in the Annex to this letter.

BSA, with US-ABC, wishes to once again commend the Ministry of Digital Economy and Society (“**MDES**”) for undertaking this important effort to ensure Thailand is prepared to deter and manage cybersecurity threats. As cybersecurity threats grow more sophisticated and dangerous, the risk of an insufficient or poorly calibrated national policy for countering cyber threats is potentially catastrophic.

Cybersecurity threats are global in nature, and so must be the response. BSA and US-ABC commend MDES and the Government of Thailand for soliciting input from the private sector and other interested stakeholders in the development of this law. We encourage continued open communication and consultation with the private sector, including global companies. As such, we suggest that the Cybersecurity Law make clear that references to cooperation with the private sector (e.g. Sections 5(4), 7(5), etc.) explicitly allow for and encourage cooperation with international companies.

BSA and US-ABC acknowledge and appreciate the efforts that have been made to address concerns raised in relation to the 2015 Draft Bill. However, most of our comments to the 2015 Draft Bill continue to apply to the 2018 Draft Bill. BSA therefore offers the following comments that are intended to help achieve the Bill's laudable objective of ensuring “prompt and unified action” in response to cybersecurity threats, while avoiding any unintended consequences.

A. Composition of the National Cybersecurity Committee

In BSA's previous comments to the 2015 Draft Bill, BSA highlighted that the proposed National Cybersecurity Committee (“**NCSC**”) should be expanded to include the National Human Rights Commission and the Office of the Ombudsman among its members to complement the perspectives of the existing security- and defense-centered members of the NCSC. This suggestion is aimed to ensure that concerns regarding personal privacy and civil liberties of individuals will be fully considered by the NCSC in any cybersecurity strategy or response it develops.

BSA and US-ABC acknowledge that Section 6 of the 2018 Draft Bill has expanded the composition of the NCSC, with the addition of representatives from several ministries including transport, education, and public health. The inclusion of these members to the NCSC will undoubtedly increase the diversity of views and provide for a well-rounded national cybersecurity policy proposal to the Cabinet. Nevertheless, the NCSC still does not include members that represent the interests of personal privacy and civil liberties of individuals. As

such, there continues to be a heavy emphasis on law enforcement and defense within the NCSC, with the Minister of Defense being appointed as the Vice-Chairman of the NCSC.

We recommend cybersecurity efforts are not led solely by the Ministry of Defense, but are co- led by the Ministry of Digital Economy and Society. Due to the broad ramifications of cybersecurity incidents for Thailand’s national and international economic interests, civilian interests should be well represented on the NCSC.

B. Broad powers of the NCSC

Under Section 14 of the 2018 Draft Bill, the NCSC is empowered to act as a centralized coordinator for any inter-agency response to a cyber attack and cyber incident. BSA and US-ABC continue to support this approach. Tasking a single national body with lead responsibility for cybersecurity ensures clarity, coherence, and coordination in the government’s preparedness for and response to cybersecurity threats and challenges.

As part of its role as centralized coordinator, the NCSC is afforded broad authority to respond to actionable threats. For example, under Sections 36 and 37 of the 2018 Draft Bill, the NCSC has the power to direct private agencies³ to take actions in the event of a “cyber incident” and “cyber attack”. We acknowledge that an effort has been made, in line with our comments on the 2015 Draft Bill, to clarify that some of these powers are triggered only where “the services of computer networks, Internet, telecommunication networks, satellites, utilities, important public service” are affected. However, we remain concerned about the absence of clear parameters and trigger events relating to NCSC’s rights under these Sections.

- **The NCSC’s powers should only apply where “critical infrastructure” is affected.** The concept of “critical infrastructure” is used in cybersecurity regulations in many jurisdictions internationally and is an accepted qualifier for broad regulatory enforcement powers of the type seen in the 2018 Draft Bill. Consistent with international practice, we suggest defining:
 - critical infrastructure as **“those assets, services, and systems, whether physical or virtual, which, if destroyed, degraded, or rendered unavailable for an extended period, would have a large-scale, debilitating impact on national security, public health, public safety, national economic security, or core local or national government functions.”**

Specific critical infrastructure should be identified by the NCSC based on an analysis of criticality, interdependency, and risk.

- **The broad powers in Sections 36 and 37 should only be triggered by “significant cyber incidents”.** This would require two new definitions of “cyber incident” and “significant cyber incident”. Consistent with the International Framework, we recommend defining:
 - a “cyber incident” as **“a single, or series of, identified occurrence(s) of a system, service, or network indicating a possible breach of information security policy or failure of security controls, or a previously unknown situation that may be relevant to the security of the system, service, or network.”**
 - A “significant cyber incident” as **“a cyber incident resulting in: (i) the unauthorized or denial of access to or damage, deletion, alteration, or suppression of data that is essential to the operation of critical infrastructure; or (ii) the defeat of an operational control or technical**

³ “Private agencies” is a newly defined term in Section 3 meaning “organizations established by an assembly of individuals or a body of persons to run business either for profits or not for profits and either registered or not registered”.

control that is essential to the security or operation of critical infrastructure.”

C. Notification regime for cyber attacks

BSA and US-ABC are concerned that the new requirement for private agencies to notify the Secretary-General of any actual or anticipated cyber attacks in Section 35 is too broad. Overbroad thresholds for reporting can unintentionally inhibit cybersecurity by causing companies to over notify for any incident on their systems, leading to notification fatigue, increased costs, operational distractions, and difficulties identifying and addressing the most important incidents. We suggest limiting this notification regime to "significant cyber incidents" that impact "critical infrastructure", as described above.

D. Surveillance authority

BSA and US-ABC acknowledge that BSA's previous suggestions regarding the Secretary-General's surveillance authority in the 2015 Draft Bill have been incorporated to some extent in the 2018 Draft Bill. In particular, Section 47 of the 2018 Draft Bill provides that the Secretary-General may only access a private agency's communications information where it has first obtained a court order allowing it to do so. This court order requirement is excepted "in case of urgency where serious damages will be incurred if no immediate action is taken", allowing the Secretary-General to access the communications information first and file a report with the court later under urgent circumstances. Such a broad exception may introduce uncertainty in its application, possibly undermining consumer trust that businesses can generally guarantee that their users' personal data or confidential information will be protected from unauthorized access. To address these concerns, we recommend:

- **The court order issued should only be valid for a limited period of time.** We recommend that the court order's validity not be open-ended since this would create greater uncertainty for private agencies.
- **Any exception to obtaining a court order should be precisely-worded.** We recommend that the "urgency" exception should be clarified to situations where there is a probable cause of harm to national security.
- **An independent body should have oversight over the NCSC's powers in Section 47.** We again 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 exercise of its powers under Section 47 of the 2018 Draft Bill to ensure privacy interests are adequately balanced with the need for surveillance.

E. Criminal liability

BSA and US-ABC observe that Sections 53 to 56 of the 2018 Draft Bill now impose criminal liability for several breaches under the 2018 Draft Bill. We recommend that criminal prosecution should only be imposed on those that, with criminal intent, seek to disrupt, degrade, or destabilize cyberspace.

We consider that imposing criminal liability on private agencies that do not comply with the NCSC's requests under Section 47 is excessive. This position could deter international companies from establishing a presence in Thailand if there is a risk their personnel are exposed to criminal liability for inadvertent or minor breaches.

F. Other aspects of a national cybersecurity policy

BSA and US-ABC also recommend that Thailand's national cybersecurity policy address other

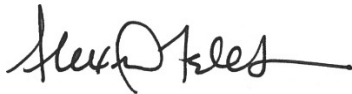
important issues including the implementation of guidelines for government procurement of technology and software, strong government support for cybersecurity technology research and development, educational campaigns to increase cybersecurity awareness and training, and the integration of cybersecurity cooperation into foreign policy. We encourage the Thai government to address these important issues as part of the implementing regulations to the 2018 Draft Bill and offer the International Framework and our international experience in these areas as a resource for developing the relevant policies.

3. Conclusion and Next Steps

BSA and US-ABC again applaud the Government of Thailand's efforts to protect infrastructure from cyber attacks and cyber criminals. However, we humbly request that MDES thoroughly consider the suggestions above. By doing so, we believe that MDES has an opportunity to deliver a robust, risk-based national cybersecurity policy that aligns with international best practices, fosters greater trust between the public and private sectors and enhances the security of data and infrastructure.

We remain open to further discussion with you at any time. Please feel free to contact us directly at afeldman@usasean.org or 202-375-4393, or jaredr@bsa.org or +65 6292 9609, or contact **Ms. Varunee Ratchatapattanakul, BSA's Thailand Country Manager, at varunee@bsa.org or +668-1840-0591, or Ms. Ella Duangkaew, US-ABC's Manager for Thailand, at eduangkaew@usasean.org or 202-440-3642** with any questions or comments which you might have. Thank you for your time and consideration.

Yours sincerely,



Alexander C. Feldman
President & CEO
US-ASEAN Business Council



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

CC:

1. Dr. Pichet Durongkaveroj, the Minister of the Ministry of Digital Economy and Society
2. Mrs. Surangkana Wayuparb, the Executive Director and Chief Executive of the Ministry of Digital Economy and Society's Electronic Transactions Development Agency (ETDA)

**Annex B:
Joint Industry Comments on the Cybersecurity Bill –
Supplemental (May 21, 2018)**



May 21, 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

Re: Joint Industry Comments on the Cybersecurity Bill – Supplemental

Dear Ms. Pattanapanchai

We refer to the April 17, 2018 BSA | The Software Alliance (“**BSA**”) and the US-ASEAN Business Council (“**US-ABC**”) submission in relation to the Cybersecurity Bill (“**2018 Bill**”). A copy of this submission is set out in Annex B to this letter.

After further study of the 2018 Bill and consultation with our members, we would like to supplement our original submission with these comments, summarized below and set out in further detail in Annex A to this letter. We humbly request that the Ministry of Digital Economy and Society (“**MDES**”) consider the additional comments in this letter alongside the suggestions made in our earlier submission.

In summary, our key additional recommendations, building on those set out in our April 17, 2018 submission, are as follows:

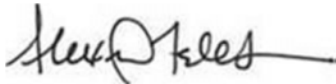
- The composition of the National Cyber Security Committee (“**NCSC**”) would benefit from the inclusion of **industry representatives**.
- The 2018 Bill should only apply to “**private agencies**” incorporated in Thailand that **operate or control critical infrastructure** (as defined in our April 17, 2018 comments), and obligations imposed on them should be expressly limited to those that are both **reasonable** and **practical**.
- The **notification obligations** should only apply to **actual significant cyber incidents**, and not to non-significant or “anticipated” incidents.
- Powers to access **information and facilities** should be **proportionate** and subject to appropriate **checks and balances**, including **judicial oversight and rights of contestation or appeal**.
- Supervisory and enforcement powers under the 2018 Bill should be administered by a **single regulatory authority**.
- The 2018 Bill should expressly cover **confidentiality and privacy concerns**.
- The 2018 Bill should promote **information sharing**, including by **establishing appropriate limitations on liability** for such information sharing activities.

We once again commend MDES and the Government of Thailand for soliciting input from the private sector and other interested stakeholders and continue to encourage such open communication and consultation. In particular, we would like to further recommend that the public consultation process extends to any sub-regulations or any other additional terms to be introduced under the 2018 Bill to ensure clarity and consistency.

As always, we remain open to further discussion with you at any time. Please feel free to contact us directly at afeldman@usasean.org or 202-375-4393, or jaredr@bsa.org or +65 6292 9609, or contact **Ms. Varunee Ratchatapattanakul, BSA's Thailand Country Manager, at varuneer@bsa.org or +668-1840-0591, or Ms. Ella Duangkaew, US-ABC's Manager for Thailand, at eduangkaew@usasean.org or 202-440-3642** with any questions or comments which you might have.

Thank you for your time and consideration.

Yours sincerely,



Alexander Feldman
President & CEO
US-ASEAN Business Council



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

Cc:

1. His Excellency Dr. Pichet Durongkaveroj, the Minister of the Ministry of Digital Economy and Society
2. Mrs. Surangkana Wayuparb, the Executive Director and Chief Executive of the Ministry of Digital Economy and Society's Electronic Transactions Development Agency (ETDA)

Annex A – Additional Feedback on the 2018 Bill

The table below sets out additional comments from BSA and US-ABC on the 2018 Bill. It supplements (and should be read alongside) the comments made in our submission of April 17, 2018, as set out in Annex B.

No.	Issue / reference	Description of issue	BSA and US-ABC comments
A. Composition of the National Cybersecurity Committee			
1.	Composition of the NCSC (Section 6)	While the 2018 Bill has expanded the composition of the NCSC, it does not include any industry members.	In addition to BSA and US-ABC’s recommendation in our earlier submission that the NCSC should be expanded to include the National Human Rights Commission and the Office of the Ombudsman, we further suggest that the NCSC include members from industry. Not only would this ensure that a range of viewpoints is represented, it would also help to enhance cooperation between the public and private sectors and drive best practices.
B. Powers of the NCSC			
2.	Definition of “private agencies” and need for a reasonableness threshold (Sections 3, 36, 37)	The 2018 Bill seeks to regulate “private agencies”, being any organizations established to run business, whether or not for profit, and whether or not they are registered. The current definition of “private agencies” appears to be too broad for the purpose of cybersecurity and should be narrowed accordingly.	We recommend that the definition of “private agency”, for purposes of this law, should be restricted to companies incorporated in Thailand that operate or control “critical infrastructure” (as defined in our earlier submission) in Thailand.
3.	Powers to give orders and require private agencies to take actions (Sections 33, 34, 36 and 37)	<ul style="list-style-type: none"> • There appear to be few limits to the power of the NCSC to give orders and instructions to private agencies under Sections 33 and 37, under which the NCSC may order private agencies “to act or omit any act”. • The NCSC has broad discretion under Section 34 to determine that a private 	<ul style="list-style-type: none"> • The powers granted to the NCSC and its delegated bodies should be more precisely defined and limited, including through independent oversight and judicial review. Private sector agencies and third parties should be afforded clear opportunities to contest orders and rights to appeal adverse decisions in Court. We recognize that certain powers do require court orders (except in urgent circumstances) under the 2018 Bill,

No.	Issue / reference	Description of issue	BSA and US-ABC comments
		<p>agency has failed to comply with the 2018 Bill or specified guidelines and to order the agency to rectify or terminate the action. If the agency fails to comply within the specified timeframe, the Cabinet has broad discretion to “consider appropriate instructions”.</p> <ul style="list-style-type: none"> Sections 36 and 37 are broadly worded to apply to <i>all</i> private agencies, even where they may not be affected by a cyber incident. 	<p>but we urge that independent oversight and judicial review should apply more broadly to NCSC powers as they relate to “private agencies”.</p> <ul style="list-style-type: none"> Section 34 should be amended to include greater specificity in terms of the types of actions or instructions which may be given to private agencies. Doing so would set clear parameters that all parties would understand and be able to work within, bringing greater certainty to the cybersecurity ecosystem in Thailand. We are also concerned that certain obligations on private agencies under the 2018 Bill (including, for example, under Sections 36 and 37) require them to take certain actions in the event of a cyber incident which may not be within their control, or which may be unreasonable, impractical, or disproportionate in the circumstances. We therefore recommend that, as a baseline threshold throughout the 2018 Bill (and not just in specific sections), the obligations imposed on private agencies should be restricted to actions which are <i>reasonable and practical</i>. In addition to the recommendation in our earlier submission that Sections 36 and 37 should only be triggered by significant cyber incidents, we also suggest that these sections only apply to entities which are <i>directly impacted</i> by the “significant cyber incident” (as defined in our earlier submission). This would avoid any suggestion that private agencies which are <i>not</i> impacted would be subject to these obligations.

No.	Issue / reference	Description of issue	BSA and US-ABC comments
C. Notification regime for cyber attacks			
4.	Notification requirements (Sections 35, 40)	The notification requirement under Section 35 seems to apply to all <i>actual and anticipated</i> cyber-attacks.	<ul style="list-style-type: none"> • The requirement to notify of <i>every actual or anticipated</i> cyber-attack should be removed. The types of cyber-attacks, and the sources of those attacks, are constantly evolving. In this environment, certain services are subjected to thousands (or more) attacks every day, most of which are successfully defended. While organizations can have measures in place designed to protect against cyber-attacks using the latest industry practices, it is simply not possible to identify every threat or to notify authorities of every <i>anticipated</i> attack. This would also create a very heavy burden and be of limited practical value for the authorities, who would be required to process vast numbers of notifications of “anticipated” attacks, many of which may never occur (or which may be successfully defended or pose no real risk of harm). • We recommend using consistent terminology and precise definitions of “cybersecurity incidents” and “significant cybersecurity incidents” (as defined in our earlier submission). • We further recommend that notification requirements are only applied to circumstances that meet a “materiality threshold” – e.g. significant cybersecurity incidents for which there is a real risk of serious harm. • Further, we believe that the role of cybersecurity regulation should be to facilitate an environment for sharing threat intelligence and information, rather than compelling disclosure of every anticipated cyber-attack. See further our comments in Item 8, below.

No.	Issue / reference	Description of issue	BSA and US-ABC comments
D. Surveillance authority			
5.	Access to information and facilities (Sections 34, 36, 37, 43, 46 and 47)	<ul style="list-style-type: none"> Section 43 authorizes relevant government authorities and the Office of the NCSC to request information, personnel or electronic devices of private agencies. However, the NCSC must obtain a court order if the private agency does not give its consent to provide the requested information, personnel or devices. Section 47 allows the Secretary-General to summon persons, documents or evidence, or take any steps required to facilitate the NCSC's actions, or access communications information (including as communicated by post, telephone, computer, electronic tools or other information technology media). As noted in our earlier submission, while the Secretary-General must first obtain a court order to access communications information, there is a broad exception "in case of urgency where serious damages will be incurred if no immediate action is taken". Section 47 also allows the NCSC to ask other government regulators to inflict penalties or sanctions on private agencies who do not obey NCSC orders, by "exercising the power of any laws, announcements or regulations". In addition, Sections 34, 36, 37 and 46 grant powers to the authorities to command, request and order private agencies to act, not to act, comply with the 2018 Bill / 	<p>In addition to our earlier recommendations in relation to Section 47 of the 2018 Bill, we would like to add the following comments:</p> <ul style="list-style-type: none"> All orders, commands or requests for information or assistance should be limited to situations where there is a significant risk of serious harm. We recommend that any such harm should be balanced against other criteria, such as the impact on the community, commercial and other practical considerations. The requirement in Section 34 to comply with the NCSC's directions should allow organizations a reasonable time period within which to do so. This should be a period of time that is reasonable in all of the circumstances, taking into account all relevant factors, such as the impact, the practical ability of the entity to take actions and the costs and benefits of taking those actions. Currently, Section 34 allows the NCSC to arbitrarily impose a time period that may not be reasonable and a breach of which could lead to serious consequences for the relevant entity. Requests for information from a private agency under Sections 43 and 47 should be subject to exemptions and notification to affected third parties. We suggest that third parties whose information may be disclosed in this process should have a right to be informed in advance in case they wish to contest such disclosure.

No.	Issue / reference	Description of issue	BSA and US-ABC comments
		<p>relevant guidelines, and assist under certain circumstances, <i>without a court order</i>. The only exception is under Section 44 where the NCSC is required to obtain a court order if it uses communications or electronic devices or other methods to detect cyber incidents which would affect a person's rights or freedom.</p> <ul style="list-style-type: none"> Regulated entities do not have rights to contest orders and a failure to comply could result in serious penalties. 	<ul style="list-style-type: none"> Powers to access information should always be subject to appropriate checks and balances. We recommend that this includes judicial oversight (i.e. court orders) and the right to contest orders. The penalties which could be inflicted under Section 47 are unclear. We suggest that Section 47 clearly defines the penalties to which a private agency could be subject, rather than referring to any other laws or regulations.
Additional recommendations			
6.	Overlapping laws and authorities (Sections 7, 14, 17, and 30 – 52)	The 2018 Bill authorizes several relevant authorities (including various constituents of the NCSC, the Minister of the MDES, and the Cabinet) to request cooperation and order private agencies to act, or not act, in certain circumstances.	The powers granted to different authorities under the 2018 Bill could create conflicts of command and potentially leave private agencies needing to reconcile multiple sets of instructions from different authorities. This would be a particular problem in case of cybersecurity incidents that require a prompt response, as dealing with multiple authorities would undoubtedly delay any response. We therefore recommend that there is a single regulatory authority with supervisory and enforcement powers under the 2018 Bill, as opposed to multiple authorities. The powers of that authority should be clearly regulated with transparent rules and governing documentation, and be subject to ministerial and judicial review.
7.	Confidentiality (Section 48)	<ul style="list-style-type: none"> Apart from Section 48, there are no specific provisions regarding confidentiality or privacy protection in the 2018 Bill. While Section 48 imposes penalties on the Officer who discloses information obtained from exercising his / her power, its 	We recommend that the 2018 Bill should contain additional specific provisions dealing with the protection of confidentiality of sensitive or personal information. These should include specific obligations on authorities to protect and maintain the confidentiality of such information, including requirements and procedures obtaining consent and how such information may be used, disclosed, stored, and disposed after it is no longer

No.	Issue / reference	Description of issue	BSA and US-ABC comments
		protection limits only disclosure to others, and does not prohibit the Officer's use of information for his / her own benefit.	required.
8.	Information sharing (General)	The 2018 Bill does not expressly deal with information sharing.	<ul style="list-style-type: none"> • BSA and US-ABC consider that the ability to share information about cybersecurity threats, vulnerability and cyber incidents with affected parties, as well as with other entities with the means to defend against attacks, is essential to promoting cybersecurity and can be more effective than incident reporting. • As attacks may be aimed at both private sector and government agencies across national borders, we recommend that the 2018 Bill supports the development of robust information sharing policies between the government and the private sector, among private entities, and among government entities. • We recommend that the 2018 Bill and information sharing policies should include limitations on potential liability for sharing entities, protecting the privacy of those affected by the shared information, facilitating multi-directional information sharing, encouraging timeliness, and ensuring that information is used only to promote cybersecurity.

Annex C:
BSA Comments on the Cyber Security Bill (May 6, 2015)



6 May 2015

PRIVILEGED & CONFIDENTIAL

The Secretary-General
Office of the Council of State
Phra Arthit Road, Phra Nakorn,
Bangkok 10200

Re: BSA Comments on the Cybersecurity Bill

Dear The Secretary-General

BSA | The Software Alliance (BSA)¹ appreciates the opportunity to submit its comments to the Council of State with respect to the Cybersecurity Bill (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 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

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.

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 varunee@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. H.E. Dr. Vishnu Krue-ngam, Deputy Prime Minister
2. Mrs. Surangkana Wayuparb, CEO, the Office of Electronic Transactions Development Agency (Public Organization)