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 appended to this document as follows:

- Annex A: BSA Comments on National Cybersecurity Bill (October 12, 2018)
- Annex B: Joint Industry Comments on the Cybersecurity Bill – Supplemental (May 21, 2018);
- Annex C: Joint Industry Comments on the Cybersecurity Bill (April 17, 2018); and
- Annex D: 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.

Annex A:
BSA Comments on the Cybersecurity Bill
(October 12, 2018)

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 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 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 Framework[3] 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 to 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

วันที่ 12 ตุลาคม 2561

นางสาวอัจฉรินทร์ พัฒนพันธ์ชัย
ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
120 หมู่ที่ 3 ชั้น 6-9 ศูนย์ราชการเฉลิมพระเกียรติ
ถนนแจ้งวัฒนะ ทุ่งสองห้อง
หลักสี่ กรุงเทพมหานคร 10210

เรื่อง ความเห็นเกี่ยวกับร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ....

เรียนท่านปลัดกระทรวง

<u>ความนำและคำชี้แจงเรื่องส่วนได้เสียในร่างพระราชบัญญัติ</u>

บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์ (“**บีเอสเอ**”)[1] ขอขอบคุณกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำหรับโอกาสให้มีการเสนอความเห็นเกี่ยวกับร่างร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.... (“**ร่าง พ.ร.บ.**”) ที่ได้ลงประกาศในเว็บไซต์ www.lawamendment.go.th เมื่อวันที่ 27 กันยายน 2018

[1] บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์ (www.bsa.org) เป็นหน่วยงานชั้นนำที่ทำหน้าที่เป็นผู้แทนในการรักษาสิทธิประโยชน์ของอุตสาหกรรมซอฟต์แวร์ในทั่วโลกต่อรัฐบาลและในตลาดระดับสากล สมาชิกของบีเอสเอเป็นบริษัทต่างๆ ที่สร้างสรรค์นวัตกรรมที่ทันสมัยที่สุดของโลก ซึ่งนำเสนอโซลูชั่นซอฟต์แวร์ที่ผลักดันให้เศรษฐกิจเติบโตและปรับปรุงคุณภาพชีวิตในยุคปัจจุบัน บีเอสเอมีสำนักงานใหญ่ตั้งอยู่ที่กรุงวอชิงตัน ดี.ซี. และมีการดำเนินการในกว่า 60 ประเทศทั่วโลก โดยเป็นผู้ริเริ่มโครงการส่งเสริมการปฏิบัติตามกฎหมายเพื่อรณรงค์การใช้ซอฟต์แวร์ที่ถูกกฎหมาย และสนับสนุนนโยบายสาธารณะที่ส่งเสริมให้มีการสร้างสรรค์นวัตกรรมเทคโนโลยีและขับเคลื่อนให้เศรษฐกิจดิจิทัลเติบโต

สมาชิกของบีเอสเอรวมถึงบริษัท 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.

บีเอสเอเป็นผู้กระทำการแทนบริษัทซอฟต์แวร์ชั้นนำระดับโลก โดยมีสมาชิกเป็นบริษัทแนวหน้าด้านนวัตกรรมที่ขับเคลื่อนด้วยข้อมูล และด้านการพัฒนาความก้าวหน้าในเชิงนวัตกรรม ให้แก่เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence (AI)) เครื่องจักรสมองกล (Marchin Learning) เทคโนโลยีคลาวด์เพื่อใช้ในการวิเคราะห์ และ Internet of Things (IoT) ซึ่งเป็นสิ่งที่ขับเคลื่อนเศรษฐกิจข้อมูลข่าวสารในทั่วโลกและทำให้มนุษย์มีความเป็นอยู่ในชีวิตประจำวันที่ดีขึ้น สมาชิกของเราได้รับความไว้วางใจจากลูกค้าในการจัดให้มีเทคโนโลยีรักษาความปลอดภัยที่สำคัญเพื่อปกป้องพวกเขาจากภัยคุกคามทางไซเบอร์ ภัยคุกคามเหล่านี้อาจเกิดขึ้นจากผู้ประสงค์ร้ายที่มีวัตถุประสงค์แตกต่างกันไป ซึ่งรวมถึงผู้ที่ต้องการขโมยอัตลักษณ์ของเรา ทำร้ายบุคคลที่เรารัก เอาไปซึ่งความลับที่มีค่าในทางการค้า หรือเป็นภัยต่อความมั่นคงของชาติ

จากการทำงานอย่างใกล้ชิดร่วมกับรัฐบาลทั่วโลกเพื่อพัฒนานโยบายและกฎหมายเพื่อความมั่นคงปลอดภัยไซเบอร์ ทำให้บีเอสเอมองเห็นความเป็นไปได้ที่กฎหมายและกฎระเบียบเพื่อความมั่นคงปลอดภัยไซเบอร์จะทำหน้าที่สำคัญสองอย่างไปพร้อมกัน ได้แก่ หน้าที่ในส่วนของการป้องกันและจัดการความเสี่ยงภัยไซเบอร์ และหน้าที่ในส่วนของการคุ้มครองความเป็นส่วนตัวและสิทธิเสรีภาพของพลเมือง ดังนั้น บีเอสเอจึงได้พัฒนากรอบนโยบายสากลว่าด้วยเรื่องความมั่นคงปลอดภัยไซเบอร์[2] (กรอบนโยบาย) รวมถึงรูปแบบของนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุม ซึ่งประเทศต่างๆ สามารถนำไปเป็นต้นแบบได้ นอกจากนี้ บีเอสเอขอแนะนำให้รัฐบาลไทยและกระทรวงฯ อ้างอิงถึงแนวทางปฏิบัติสากลที่ดีอื่นๆ เช่น National Institute of Standards and Technology's Cybersecurity Framework[3] ในขณะที่พิจารณาเรื่องกฎระเบียบและอื่นๆ เพื่อการบังคับใช้กฎหมาย ภายหลังจากที่ร่าง พ.ร.บ. มีผลบังคับใช้แล้ว

สมาชิกของบีเอสเอจึงเป็นผู้มีส่วนได้เสียโดยตรงในการที่รัฐบาลไทยจะเสนอร่าง พ.ร.บ. ฉบับนี้ โดยบีเอสเอ ร่วมกับสภาธุรกิสหรัฐอเมริกาและอาเซียน (US-ASEAN Business Council) ได้เสนอความเห็นเกี่ยวกับร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับก่อนหน้านี้ รายละเอียดปรากฏตามเอกสารที่แนบมาพร้อมกันนี้

- ภาคผนวก เอ: ความเห็นร่วมจากภาคอุตสาหกรรมต่อร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (17 เมษายน 2561)
- ภาคผนวก บี: ความเห็นร่วมจากภาคอุตสาหกรรมต่อร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (21 พฤษภาคม 2561)
- ภาคผนวก ซี: ความเห็นของบีเอสเอต่อร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (6 พฤษภาคม 2558)

---

[2] กรอบนโยบายสากลว่าด้วยเรื่องความมั่นคงปลอดภัยไซเบอร์ https://bsacybersecurity.bsa.org/wp-content/uploads/2018/04/BSA_cybersecurity-policy.pdf. สำหรับข้อมูลเพิ่มเติม https://bsacybersecurity.bsa.org/

[3] The *Framework for Enhancing Critical Infrastructure Cybersecurity, Version 1.1* ที่ได้ให้แนวทางเพื่อส่งเสริมความมั่นคงปลอดภัยของโครงสร้างพื้นฐานสำคัญและเครือข่าย สำหรับข้อมูลเพิ่มเติม https://www.nist.gov/cyberframework.

บีเอสเอขอแสดงความชื่นชมต่อกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมอีกครั้งหนึ่งมาในโอกาสนี้สำหรับความพยายามครั้งสำคัญที่ดำเนินการเพื่อให้แน่ใจว่าประเทศไทยมีความพร้อมที่จะระงับยับยั้งและจัดการกับภัยคุกคามไซเบอร์ เนื่องจากภัยคุกคามไซเบอร์มีความซับซ้อนและมีอันตรายขึ้นทุกวัน ความเสี่ยงที่เกิดจากนโยบายระดับประเทศที่กำหนดขึ้นอย่างไม่เพียงพอหรือไม่มีประสิทธิภาพในการรับมือกับภัยคุกคามไซเบอร์จึงอาจก่อให้เกิดความเสียหายอย่างใหญ่หลวงได้

<u>ความเห็นอย่างละเอียด</u>

ร่าง พ.ร.บ. ฉบับปัจจุบันมีการแก้ไขเพิ่มเติมร่างฉบับก่อนในประเด็นที่สำคัญ และได้รวมหลักการพื้นฐานอันจะทำให้กฎหมายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์บังคับใช้ได้อย่างมีประสิทธิภาพเพื่อประโยชน์ของชาวไทย โดยเฉพาะเพื่อปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure (CII)) ทำให้เห็นได้ชัดเจนว่าเรื่องนี้เป็นวัตถุประสงค์หลักของรัฐบาลไทย อย่างไรก็ดี ร่าง พ.ร.บ. ฉบับปัจจุบันยังคงมีบทบัญญัติในหลายเรื่องที่อาจสร้างภาระเกินควรและอาจสร้างความกำกวมในแง่กฎหมายต่ออุตสาหกรรมเทคโนโลยี โดยเฉพาะการตัดบทบัญญัติที่กำหนดให้การเข้าถึงข้อมูลต้องเป็นไปตามขั้นตอนที่ชอบด้วยกฎหมาย ในหนังสือฉบับนี้ บีเอสเอขอเรียนเสนอความเห็นและแสดงข้อกังวลในเรื่องต่อไปนี้

- ความชัดเจนในขอบเขตการบังคับใช้ร่าง พ.ร.บ. ฉบับปัจจุบัน และความสัมพันธ์กับกฎหมาย กฎระเบียบ และกฎเกณฑ์อื่น
- กรรมการในคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและคณะกรรมการกำกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
- อำนาจของ กปช.
- อำนาจหน้าที่ในการสอดส่องดูแล
- ความรับผิดทางอาญา
- การรักษาความลับ
- การแบ่งปันข้อมูลข่าวสาร
- ประเด็นอื่นๆ

รายละเอียดมีดังนี้

เอ. ความชัดเจนในขอบเขตการบังคับใช้ร่าง พ.ร.บ. ฉบับปัจจุบัน และความสัมพันธ์กับกฎหมาย กฎระเบียบ และกฎเกณฑ์อื่น

บีเอสเอสนับสนุนการจำกัดขอบเขตของการแจ้งเตือน รายงาน จัดการ และรับมือกับสถานการณ์ (มาตรา 38-58) ในร่าง พ.ร.บ. ฉบับนี้ ที่ใช้เฉพาะกับระบบข้อมูลของหน่วยงานรัฐและหน่วยงานเอกชนที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure (CII)) (หรือ

หน่วยงานเอกชน) อย่างไรก็ตาม บีเอสเอเห็นว่าคำจำกัดความของ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure (CII)) ควรมีความชัดเจน ดังต่อไปนี้

1. **แนวคิดเกี่ยวกับ "โครงสร้างพื้นฐานสำคัญ"** (Critical infrastructure) **ควรสอดคล้องกันกับแนวทางสากล** และควรมีคำจำกัดความดังนี้

    - **"ทรัพย์สิน บริการ และระบบ ไม่ว่าที่จับต้องได้หรือเสมือนจริง ที่หากถูกทำลาย ถูกทำให้เสียหาย หรือไม่สามารถใช้การได้เป็นระยะเวลานานแล้ว จะส่งผลกระทบในวงกว้างต่อความมั่นคงของชาติ สาธารณสุข ความปลอดภัยของประชาชน ความมั่นคงด้านเศรษฐกิจของชาติ หรือการปฏิบัติงานหลักของหน่วยงานในระดับท้องถิ่นหรือระดับชาติ"**

    ด้วยเหตุนี้ กปช. จึงควรกำหนดว่าโครงสร้างพื้นฐานใดเป็นโครงสร้างพื้นฐานที่สำคัญ โดยพิจารณาจากความสำคัญ และความสำคัญของผลกระทบที่จะเกิดขึ้นกับประเทศไทย ความจำเป็นต่อระบบอื่นและระดับความเสี่ยง มิใช่พิจารณาจากภารกิจหรือบริการของแต่ละหน่วยงาน ตามที่กำหนดไว้ใน **มาตรา 43** การกำหนดให้หน่วยงานที่มีภารกิจหรือบริการในเจ็ดด้านเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นมีขอบเขตที่กว้างเกินไปโดยมิได้คำนึงถึงข้อเท็จจริงว่า ภายในแต่ละหน่วยงานมีโครงสร้างพื้นฐานเพียงบางประการเท่านั้นที่เป็นโครงสร้างพื้นฐานที่สำคัญ

2. **ต้องมีความชัดเจนเกี่ยวกับองค์กร ที่เป็น "หน่วยงานเอกชน" ที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure (CII))** เพราะในบางสถานการณ์ อาจมีองค์กรที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure (CII)) อันเดียวกันมากกว่าหนึ่งแห่ง เช่น กรณีของการมอบหมายให้องค์กรภายนอกปฏิบัติงานบางส่วน (Outsource) บีเอสเอจึงขอแนะนำให้มีการกำหนดความชัดเจนเกี่ยวกับหน่วยงานเอกชนที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure (CII)) และขอเสนอแนวคิดดังนี้

    - หน่วยงานเอกชนที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure (CII)) หมายถึงองค์กรที่มีอำนาจควบคุมเหนือโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือมีหน้าที่รับผิดชอบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และเป็นเจ้าของสินทรัพย์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศในทางกฎหมาย
    - ในสถานการณ์ที่มีองค์กรที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศมากกว่าหนึ่งองค์กร คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ("กปช.") ควรปรึกษากับหน่วยงานที่ทำหน้าที่กำกับดูแลของแต่ละหน่วยงาน เพื่อกำหนดความชัดเจนเกี่ยวกับองค์กรเหล่านั้น

3. **ความชัดเจนเรื่องความรับผิดชอบของ "หน่วยงานเอกชน" ที่ปฏิบัติงานเกี่ยวกับโครงสร้าง**

พื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure (CII)) ที่ต้องทำให้แน่ใจว่าคู่ค้าของตนทำตามข้อกำหนดที่จำเป็นด้านการความมั่นคงปลอดภัย
หน่วยงานเอกชนที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรยังคงมีหน้าที่รับผิดชอบโดยรวมในเรื่องความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และร่าง พ.ร.บ. ฉบับปัจจุบันไม่ควรกำหนดความรับผิดให้กับคู่ค้าที่เป็นองค์กรภายนอกของหน่วยงานเอกชนที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และควรกำหนดให้ชัดเจนว่าหน่วยงานเอกชนที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถสร้างข้อกำหนดที่จำเป็นเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในสัญญาที่ทำกับคู่ค้าที่เป็นองค์กรภายนอกของตนได้

4. **ความชัดเจนเรื่องการบังคับใช้ร่าง พ.ร.บ. ฉบับปัจจุบัน กับกฎหมายอื่นที่มีอยู่แล้วในแต่ละหน่วยงาน** เช่น กฎหมาย กฎระเบียบ และกฎเกณฑ์ ของธนาคารแห่งประเทศไทย สำนักงานกำกับหลักทรัพย์และตลาดหลักทรัพย์แห่งประเทศไทย สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เป็นต้น โดยเฉพาะไม่ชัดเจนเกี่ยวกับเรื่องการรายงานที่จะซ้ำซ้อนระหว่างคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (“กปช.”) กับหน่วยงานที่ทำหน้าที่กำกับดูแลของแต่ละหน่วยงานหรือไม่ บีเอสเอขอแนะนำให้กระทรวงฯ เพิ่มบทบัญญัติในร่าง พ.ร.บ. เพื่อสร้างความชัดเจนในเรื่องนี้

บี. กรรมการในคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและคณะกรรมการกำกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ในหนังสือเสนอความเห็นของบีเอสเอต่อร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ปี 2558 และปี 2561 บีเอสเอได้เน้นในประเด็นที่ว่า คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (“**กปช.**”) ควรประกอบด้วยกรรมการที่มาจากหลายที่มามากขึ้น โดยรวมถึงกรรมการที่จะปกป้องผลประโยชน์ในเรื่องความเป็นส่วนตัวและเสรีภาพของบุคคลด้วย เช่น กรรมการที่แต่งตั้งมาจากคณะกรรมการสิทธิมนุษยชนและสำนักงานผู้ตรวจการแผ่นดิน นอกจากนี้ บีเอสเอขอเรียนเสนอว่าการดำเนินการในเรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ควรมีหน่วยงานของรัฐบาลพลเรือนเป็นผู้มีหน้าที่รับผิดชอบเป็นหลัก เนื่องจากภัยคุกคามทางไซเบอร์อาจส่งผลกระทบต่อผลประโยชน์ทางด้านเศรษฐกิจทั้งในระดับชาติและระดับนานาชาติได้ในวงกว้าง กปช. จึงควรมีกรรมการที่จะดูแลรักษาผลประโยชน์ดังกล่าวอยู่ด้วย นอกจากนี้ บีเอสเอขอเรียนเสนอให้ กปช. มีกรรมการที่มาจากภาคอุตสาหกรรมด้วย เพื่อให้มีมุมมองที่รอบด้านขึ้น อีกทั้งเป็นการส่งเสริมความร่วมมือระหว่างภาครัฐกับภาคเอกชน อันจะนำไปสู่วิธีปฏิบัติที่เป็นไปอย่างมีประสิทธิภาพสูงสุด

ในร่าง พ.ร.บ. ฉบับปัจจุบัน กปช. ก็ยังคงไม่มีกรรมการที่จะดูแลรักษาผลประโยชน์ในเรื่องความเป็นส่วนตัวและเสรีภาพของประชาชน ด้วยเหตุนี้ กรรมการยังมีแต่กรรมการที่เป็นผู้บังคับใช้กฎหมายและกรรมการที่เป็นผู้รักษาความมั่นคงของประเทศ โดยมีรัฐมนตรีว่าการกระทรวงกลาโหมเป็นรองประธานกรรมการ

อนึ่ง **มาตรา 19** ของร่าง พ.ร.บ. ฉบับปัจจุบัน ได้บัญญัติเพิ่มเติมเกี่ยวกับคณะกรรมการกำกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (**คณะกรรมการกำกับสำนักงาน**) ซึ่งมีกรรมการที่มาจากฝ่ายพลเรือนเป็นส่วนใหญ่ โดยมีปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นประธานกรรมการ บีเอสเอเห็นว่าคณะกรรมการกำกับสำนักงานควรมีกรรมการที่มาจากหลากหลายหน่วยงานเช่นกัน โดยมาจากทั้งภาคประชาชนและภาคเอกชน

ซี. การมีอำนาจอย่างกว้างขวางของ กปช.

บีเอสเอยังคงเห็นด้วยที่มาตรา 9 แห่งร่างพระราชบัญญัติฯ กำหนดให้ กปช. มีอำนาจหน้าที่เป็นศูนย์กลางในการประสานงานระหว่างหน่วยงานเพื่อรับมือกับภัยคุกคามไซเบอร์และสถานการณ์ด้านภัยคุกคามไซเบอร์ การกำหนดให้มีหน่วยงานระดับประเทศเพียงหน่วยงานเดียวทำหน้าที่เป็นหน่วยงานหลักที่มีความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะทำให้เกิดความชัดเจน มีความสอดคล้องและเป็นไปในทิศทางเดียวกันในการเตรียมความพร้อมของรัฐบาลในการรับมือกับภัยคุกคามและปัญหาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ นอกจากนี้ บีเอสเอยังการเปลี่ยนแปลงในทางที่ดีของการใช้อำนาจของ กปช. ที่จำกัดให้ใช้เฉพาะในสถานการณ์ “การจู่โจมทางไซเบอร์ที่ร้ายแรง” (มาตรา 56-58) อย่างไรก็ตาม บีเอสเอยังคงมีความกังวลเรื่องขอบเขตอำนาจของ กปช. อยู่

1. **อำนาจของ กปช. ควรใช้เฉพาะกับหน่วยงานเอกชนที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยจำกัดเฉพาะบริษัทที่จัดตั้งขึ้นในประเทศไทยและเป็นผู้ประกอบกิจการหรือเป็นผู้ควบคุมโครงสร้างพื้นฐานที่สำคัญในประเทศไทยเท่านั้น** องค์กรระหว่างประเทศที่มีสำนักงานตั้งอยู่ในประเทศไทย อาจมีโครงสร้างพื้นฐานและระบบเทคโนโลยีสารสนเทศโดยทั้งหมดมีที่ตั้งอยู่นอกประเทศไทย จึงจำเป็นที่ร่าง พ.ร.บ. ต้องสร้างความชัดเจนว่า “คอมพิวเตอร์” และ “ระบบคอมพิวเตอร์” โดยทั้งหมดมีที่ตั้งอยู่นอกประเทศไทย ไม่ได้เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อหลีกเลี่ยงความขัดแย้งกันระหว่างกฎหมายระหว่างประเทศที่อาจจะเกิดขึ้น
2. **การให้อำนาจที่กว้างขวางตามมาตรา 56 ถึงมาตรา 58 ในกรณี “ภัยคุกคามทางไซเบอร์ซึ่งอยู่ในระดับร้ายแรง” ควรต้องให้คำจำกัดความในลักษณะที่สอดคล้องกับวิธีปฏิบัติที่ดีของสากล**

ในประเด็นนี้ บีเอสเอขอเรียนย้ำว่าควรให้คำจำกัดความดังนี้

- “ภัยคุกคามทางไซเบอร์ซึ่งอยู่ในระดับร้ายแรง” หมายความว่า **“เหตุภัยคุกคามทางไซเบอร์ที่ทำให้ (i) มีการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือมีการถูกปฏิเสธไม่ให้เข้าถึงข้อมูล หรือมีการทำลาย ลบ ปรับเปลี่ยน หรือระงับข้อมูลที่จำเป็นต่อการทำงานของโครงสร้างพื้นฐานที่สำคัญ หรือ (ii) การควบคุมการปฏิบัติการหรือการควบคุมทางเทคนิคที่จำเป็นต่อความปลอดภัยหรือการทำงานของโครงสร้างพื้นฐานที่สำคัญถูกโจมตี”**

นอกจากนี้ บีเอสเอขอเรียนเสนอคำจำกัดความของ “ภัยคุกคามทางไซเบอร์” ดังนี้

- “ภัยคุกคามทางไซเบอร์” หมายความว่า **“เหตุการณ์ที่โดยตั้งใจเพื่อก่อให้เกิดผลกระทบที่ร้ายแรงต่อความมั่นคงปลอดภัย การมีอยู่ การรักษาความลับ หรือความสมบูรณ์ของระบบสารสนเทศ หรือข้อมูลที่ถูกเก็บไว้ หรือที่ถูกประมวลผลโดยระบบสารสนเทศ หรือที่ถูกส่งต่อไปยังระบบสารสนเทศ”**

นอกจากนี้ ร่าง พ.ร.บ. ฉบับนี้ ควรระบุเหตุการณ์ใดที่เรียกว่าร้ายแรง เพื่อความชัดเจนในเรื่องการใช้อำนาจสืบสวน

3. **การกำหนดขอบเขตอำนาจของ กปช. ก่อให้เกิดหน้าที่ในส่วนของหน่วยงานเอกชน (มาตรา 38, 40, 44-45 และ 53-58)** การให้อำนาจแก่ กปช. อย่างกว้างขวาง อาจส่งผลกระทบต่อการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของภาคพลเรือน และอาจบั่นทอนความร่วมมือจากภาคเอกชนเพื่อป้องกันความเสี่ยงที่จะมีต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดังนั้น ควรกำหนดและจำกัดอำนาจที่ให้แก่ กปช. ให้มีความชัดเจนยิ่งขึ้น รวมถึงให้มีการตรวจสอบโดยหน่วยงานอิสระและการตรวจสอบความชอบด้วยกฎหมายโดยศาล อีกทั้งหน่วยงานเอกชนควรมีโอกาสอย่างเต็มที่ในการโต้แย้งคำสั่งและมีสิทธิยื่นอุทธรณ์ต่อศาลหากไม่เห็นพ้องด้วยกับคำวินิจฉัย นอกจากนี้ บทบัญญัติที่จำกัดอำนาจบางประการโดยกำหนดให้ต้องได้รับคำสั่งศาลก่อนดำเนินการ (เว้นแต่ในกรณีจำเป็นเร่งด่วน) นั้นถูกตัดออกไปจากร่างพระราชบัญญัติฉบับนี้ บีเอสเอจึงขอเรียนว่าควรจำกัดอำนาจโดยกำหนดให้ต้องได้รับคำสั่งศาลก่อนดำเนินการเช่นเดิม นอกจากนี้ การใช้อำนาจของ กปช. ควรต้องมีการตรวจสอบโดยหน่วยงานอิสระและการตรวจสอบความชอบด้วยกฎหมายโดยศาลในหลายกรณีมากขึ้น เนื่องจากเป็นเรื่องที่เกี่ยวข้องกับ “หน่วยงานเอกชน”

โดยเฉพาะบทบัญญัติในมาตรา 46 มีลักษณะที่กว้างมาก และดูเหมือนจะสวนทางกับร่างพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคลของกระทรวงฯ และแนวทางปฏิบัติสากล ร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลที่ได้รับการแก้ไขเมื่อเร็วๆ นี้ เพื่อให้สอดรับกับหลักการของกฎหมาย General Data Protection Regulation (GDPR) ของสหภาพยุโรป แต่ระดับของการคุ้มครองเจ้าของข้อมูลภายใต้ร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ กลับไม่สอดคล้องกันกับหลักการของ GDPR ยิ่งไปกว่านั้น ในย่อหน้าที่ 2 ของมาตรา 46 กลับสร้างความเป็นโมฆะให้แก่กฎหมายทั้งหมดที่อาจใช้ได้กับหน่วยงานเอกชน รวมถึงความเป็นโมฆะของสัญญาที่ถูกใช้เป็นเครื่องมือที่สมควรในเรื่องการเปิดเผยข้อมูลและคุ้มครองเจ้าของข้อมูลและสิทธิในเชิงพาณิชย์ นับเป็นเรื่องที่สวนทางกับแนวทางปฏิบัติสากลที่ดีในการคุ้มครองข้อมูลส่วนบุคคล และเกือบจะเป็นไปไม่ได้ในการบังคับใช้ โดยเฉพาะหากหน่วยงานเอกชนมีหน้าที่ต้องปฏิบัติตามกฎหมายของประเทศอื่น

บีเอสเอขอแนะนำให้แก้ไขปัญหาดังกล่าว **โดยกำหนดลักษณะของข้อมูลที่บัญญัติไว้ในมาตร 46 (1)-(3) ให้แคบลง และเพิ่มขั้นตอนตามกระบวนการยุติธรรมที่หน่วยงานเอกชนสามารถใช้สิทธิโต้แย้งที่มีอยู่ได้** นอกจากนี้ ขอแนะนำให้ลบทิ้งย่อหน้าที่ 2 ของมาตรา 46 ที่ระบุว่า **“หน่วยงานที่ได้รับหนังสือตามวรรคหนึ่ง ไม่อาจยกเอาหน้าที่ตามกฎหมายอื่น หรือตามสัญญามาเป็น**

ข้ออ้างเพื่อไม่เปิดเผยข้อมูล” ในกรณีนี้ การดำเนินการที่เป็นการปฏิบัติตามมาตรานี้ที่ทำโดยเจตนาสุจริต ไม่ควรถูกพิจารณาว่าเป็นการฝ่าฝืนกฎหมายหรือสัญญา

ตัวอย่างเช่น กปช. ควรมีอำนาจที่จะยึดเครื่องคอมพิวเตอร์โดยไม่ต้องมีคำสั่งศาลได้เฉพาะในกรณีมีภัยหรือเกิดเหตุการณ์คุกคามทางไซเบอร์ซึ่งอยู่ในระดับร้ายแรง ซึ่งเป็นสถานการณ์ที่มีความจำเป็นเร่งด่วน และไม่มีวิธีการใดที่เหมาะสมเพื่อให้บรรลุวัตถุประสงค์ของการสืบสวนได้ และควรทำการยึดเครื่องคอมพิวเตอร์ภายหลังจากที่มีการปรึกษาหารือกับองค์กรเอกชนและได้พิจารณาถึงความสำคัญของเครื่องคอมพิวเตอร์ที่มีต่อธุรกิจและความจำเป็นในการปฏิบัติงานขององค์กรเอกชนนั้นแล้ว กล่าวคือการยึดเครื่องคอมพิวเตอร์ควรต้องมีความจำเป็นมากกว่าผลเสียหายร้ายแรงที่จะมีต่อองค์กรเอกชนนั้น

4. **การกำหนดหน้าที่แก่หน่วยงานเอกชนตลอดร่างพระราชบัญญัติฯ ควรจำกัดเฉพาะหน้าที่ตามสมควรและทำได้จริงในทางปฏิบัติ** บีเอสเอยังคงมีความกังวลเนื่องจากร่างพระราชบัญญัติฯ นี้กำหนดหน้าที่แก่หน่วยงานเอกชน (เช่น มาตรา 56 และมาตรา 58) อันทำให้หน่วยงานเอกชนต้องดำเนินการบางประการเมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ซึ่งอาจไม่ได้อยู่ภายใต้การควบคุมของตน หรืออาจเป็นหน้าที่เกินสมควร ไม่สามารถปฏิบัติได้จริง หรือไม่ได้สัดส่วน

การปฏิบัติตามกฎหมายใดๆ ที่หน่วยงานเอกชนต้องดำเนินการ (รวมถึง การดำเนินการ การจัดใช้เข้าถึงข้อมูล การให้ข้อมูล และ/หรือ การให้เอกสาร รายงาน เป็นต้น) ต้องเป็นให้เป็นไปตามคำสั่งศาลหรือหมายศาลที่มีสภาพบังคับและเป็นไปตามกระบวนการยุติธรรม นอกจากนี้ ร่าง พ.ร.บ. ฉบับปัจจุบันควรต้องระบุรายละเอียดและขอบเขตของการร้องขอให้เฉพาะเจาะจงและชัดเจน และเป็นการร้องขอเฉพาะกับข้อมูลหรือเอกสารที่หน่วยงานเอกชนมีอำนาจควบคุมในลักษณะที่สมเหตุสมผลในเชิงพาณิชย์และเหมาะสมในสถานการณ์นั้นๆ คำแนะนำเหล่านี้เกิดจากสภาพความเป็นจริงในเชิงพาณิชย์ที่หน่วยงานเอกชนไม่ได้อยู่ในสถานะเดียวกับหน่วยงานภาครัฐ และร่าง พ.ร.บ. ฉบับนี้ ไม่ควรสร้างข้อบังคับไม่สมควรให้แก่หน่วยงานเอกชน

ยกตัวอย่างเช่น การกระทำหลายอย่างที่กำหนดไว้ในมาตรา 57 และ 58 มีลักษณะที่ไม่สมเหตุสมผลหรือเป็นไปไม่ได้ในทางปฏิบัติสำหรับหน่วยงานเอกชน เพราะอาจทำให้เกิดการเปลี่ยนแปลงในพื้นฐานที่สำคัญของรูปแบบการดำเนินธุรกิจ เพียงเพื่อทำให้สามารถตอบสนองตามที่ร่าง พ.ร.บ. ฉบับปัจจุบันต้องการ และหากต้องทำเช่นนั้น อาจส่งผลกระทบต่อความสามารถในการดำเนินธุรกิจให้บริการแก่ลูกค้า ในขณะเดียวกัน มาตรา 58 (4) ที่ให้อำนาจเลขาธิการทำการทำการ “ยึดคอมพิวเตอร์หรืออุปกรณ์ใดๆ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ เพื่อการตรวจสอบหรือวิเคราะห์” ควรจำกัดหน้าที่ของหน่วยงานเอกชนเพียงเท่าที่จะกระทำได้ภายใต้อำนาจควบคุมของตน และความสมเหตุสมผลในเชิงพาณิชย์ในสถานการณ์นั้น

นอกจานนี้ การคาดหวังให้หน่วยงานเอกชนรายงานภัยคุกคามไซเบอร์ที่คาดการณ์ได้ เป็นเรื่องที่ไม่

สมเหตุสมผลหรือเป็นไปไม่ได้ **จึงควรลบมาตรา 51 ออกไปจากร่าง พ.ร.บ. ฉบับปัจจุบัน** เนื่องจากภัยคุกคามไซเบอร์ที่คาดการณ์ได้ว่าจะเกิด และต้นตอของภัยคุกคามดังกล่าวมีการเปลี่ยนแปลงอยู่ตลอดเวลา ในปัจจุบัน มีบริการบางอย่างที่ต้องเผชิญกับภัยคุกคามไซเบอร์มากมายอยู่ทุกวัน ส่วนใหญ่ของภัยคุกคามได้รับการป้องกันไปแล้ว ในขณะที่องค์กรสามารถมีมาตรการที่ถูกออกแบบมาเพื่อป้องกันภัยคุกคามไซเบอร์ได้ตามแนวทางปฏิบัติที่เกิดขึ้น การระบุว่าจะเกิดภัยคุกคามไซเบอร์อะไรบ้างทั้งหมด หรือการแจ้งภัยคุกคามไซเบอร์ทั้งหมด ที่มี “โอกาสจะเกิดขึ้น” ให้หน่วยงานที่มีอำนาจทราบ จึงเป็นไปไม่ได้ การแจ้งภัยคุกคามไซเบอร์ โดยปราศจากความเสี่ยงที่แท้จริง อาจทำให้เกิดจำนวนของการแจ้งที่มากเกินความจำเป็น นำไปสู่ภาระที่เกิดกว่าเหตุสำหรับหน่วยงานเอกชน และอาจทำให้หน่วยงานเอกชนเกิดข้อผิดพลาดในการแจ้งภัยคุกคามไซเบอร์ที่เป็นความเสี่ยงที่แท้จริงเมื่อถึงเวลาจริงๆ

ดังนั้น จึงจำเป็นที่ร่าง พ.ร.บ. ฉบับนี้ต้องเพิ่มบทบัญญัติที่รองรับความคล่องตัวของการทำงานของหน่วยงานเอกชนที่ต้องสมดุลย์ให้ได้สัดส่วนกับการใช้อำนาจ บีเอสเอขอแนะนำ กปช. ควรกำหนดมาตรการที่เหมาะสมสำหรับการสืบสวน สำหรับสถานการณ์ของภัยคุกคามทางไซเบอร์ซึ่งอยู่ในระดับร้ายแรง โดยปรึกษากับหน่วยงานที่ทำหน้าที่กำกับดูแลและหน่วยงานเอกชนที่ปฏิบัติงานเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

5. **มาตรา 56 ถึงมาตรา 58 อันเป็นเรื่องภัยคุกคามทางไซเบอร์ซึ่งอยู่ในระดับร้ายแรง ควรจำกัดเฉพาะหน่วยงานที่*ได้รับผลกระทบโดยตรง*จากภัยคุกคามนั้น** เพื่อที่จะได้หลีกเลี่ยงไม่ให้ตีความได้ว่าหน่วยงานเอกชน*ที่ไม่ได้รับผลกระทบ*จะต้องมีหน้าที่ตามมาตรานี้

ดี. อำนาจในการสอดส่องดูแล

บีเอสเอมีความกังวลเป็นอย่างยิ่งในเรื่องที่ร่าง พ.ร.บ. ฉบับปัจจุบัน ไม่มีบทบัญญัติที่กำหนดให้ต้องได้รับคำสั่งศาลก่อนเข้าถึงข้อมูลการติดต่อสื่อสารของหน่วยงานเอกชน จึงขอแนะนำดังต่อไปนี้

1. **บีเอสเอแนะนำว่าเป็นเรื่องจำเป็นอย่างยิ่งที่ร่าง พ.ร.บ. ฉบับปัจจุบัน ต้องมีคำสั่งศาลก่อนเข้าถึงข้อมูลการติดต่อสื่อสารของหน่วยงานเอกชน** การใช้อำนาจให้ได้มาซึ่งข้อมูล (รวมถึงการยึดสินทรัพย์) ควรดำเนินอยู่ภายใต้เครื่องมือทางกฎหมาย มิเช่นนั่น จะไม่มีการบันทึกเกี่ยวกับเหตุการณ์ที่เกิดขึ้น ขอบเขต วัตถุประสงค์ บริบท หรือระยะเวลา มุมมองของบีเอสเอคือควรต้องมีเอกสาร เช่น หมายศาล หรือ “เอกสารชั่วคราวในกรณีฉุกเฉิน” ที่กำหนดกระบวนการของการให้ได้มาซึ่งข้อมูล

   การที่กฎหมายไม่มีบทบัญญัติที่กำหนดให้ดำเนินการตามขั้นตอนที่ชอบด้วยกฎหมายทำให้เกิดการละเมิดความเป็นส่วนตัวของลูกค้าของหน่วยงานเอกชนนั้น และจะลดความเชื่อมั่นของผู้บริโภค เนื่องจากผู้ประกอบธุรกิจไม่อาจรับรองได้ว่าจะไม่มีผู้ใดเข้าถึงข้อมูลส่วนบุคคลหรือความลับทางการค้าของผู้บริโภคโดยไม่ได้รับอนุญาต นอกจากนี้ การที่กฎหมายไม่มีบทบัญญัติที่กำหนดให้ดำเนินการ

ตามขั้นตอนที่ชอบด้วยกฎหมายอาจทำให้เกิดการขัดกันแห่งกฎหมายระหว่างประเทศ และสร้างปัญหาให้แก่องค์กรระหว่างประเทศในเรื่องการปฏิบัติตามกฎหมาย

2. **การยกเว้นไม่ต้องขอคำสั่งศาลจำเป็นต้องกำหนดเป็นลายลักษณ์อักษรที่ชัดเจน** บีเอสเอขอแนะนำว่าต้องกำหนด “กรณีเร่งด่วน” ที่ได้รับการยกเว้นให้ชัดเจนว่าเป็นกรณีที่อาจเป็นสาเหตุของภัยต่อความมั่นคงของประเทศ
3. **องค์รอิสระควรเข้ามากำกับดูแลการใช้อำนาของ กปช.** เช่น คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ตามที่กำหนดในพระราชบัญญัติการคุ้มครองข้อมูลส่วนบุคคล และคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลควรมีอำนาจในการตรวจสอบการใช้อำนาจของ กปช. ในการเข้าถึงข้อมูลของหน่วยงานเอกชน เพื่อทำให้มั่นใจว่ามีการถ่วงดุลระหว่างการคุ้มครองสิทธิส่วนบุคคลกับความจำเป็นในการสอดส่องดูแล
4. นอกจากนี้ บีเอสเอขอแนะนำให้**เพิ่มเติมบทบัญญัติที่เกี่ยวกับขั้นตอนสำหรับการเข้าถึงและให้ได้มาซึ่งข้อมูล** ขั้นตอนเหล่านั้นได้แก่
    - **คำสั่ง คำบัญชาการ หรือคำขอทั้งหมด เพื่อให้ได้มาซึ่งข้อมูล หรือความช่วยเหลือ ควรมีข้อจำกัด กล่าวคือ ใช้เฉพาะกับสถานการณ์ที่เป็นความเสี่ยงที่จะทำให้เกิดความเสียหายในระดับร้ายแรง** บีเอสเอแนะนำว่าควรต้องพิจารณาผลกระทบต่อชุมชน ภาคธุรกิจ และควรต้องมีข้อพิจารณาในทางปฏิบัติอื่นๆ เพื่อถ่วงดุลความเสียหายดังกล่าวที่อาจเกิดขึ้น หากไม่มีข้อจำกัดและการดูแล จะทำให้องค์กรที่ตกเป็นเหยื่อของการจู่โจม หรือถูกละเมิดข้อมูล เข้าใจว่าเป็นหน้าที่ที่ต้องให้ข้อมูลตามคำสั่ง มากกว่าเข้าใจว่าหน่วยงานรัฐกำลังส่งเสริมให้เกิดความร่วมมือ
    - **การขอข้อมูลจากหน่วยงานเอกชนควรมีกรณียกเว้นและควรต้องแจ้งให้บุคคลภายนอกที่ได้รับผลกระทบทราบ** บีเอสเอขอเรียนเสนอว่า บุคคลภายนอกที่เป็นเจ้าของข้อมูลที่ถูกเปิดเผยควรมีสิทธิได้รับแจ้งก่อนที่จะมีการเปิดเผยข้อมูลนั้นเพื่อให้บุคคลภายนอกดังกล่าวได้มีโอกาสคัดค้านการเปิดเผยข้อมูล
    - **ควรกำหนดให้คำสั่งศาลมีผลเพียงช่วงระยะเวลาหนึ่ง** บีเอสเอขอเรียนเสนอว่า คำสั่งศาลไม่ควรมีผลบังคับโดยไม่จำกัดระยะเวลา เนื่องจากอาจก่อให้เกิดความไม่ชัดเจนมากขึ้นต่อหน่วยงานเอกชน

5. **กฎหมายลำดับรอง กฎเกณฑ์อื่น หรือข้อบังคับ ควรต้องทำผ่านกระบวนการรับฟังความคิดเห็นก่อนเสมอ** และควรประกาศใช้พร้อมกันกับร่าง พ.ร.บ. ฉบับนี้

อี. ความรับผิดทางอาญา

บีเอสเอเห็นว่า มาตรา 62 และมาตรา 63 แห่งร่างพระราชบัญญัติฯ ได้กำหนดโทษทางอาญาสำหรับการกระทำที่ฝ่าฝืนร่างพระราชบัญญัติฯ ในเรื่องนี้ บีเอสเอเห็นว่า การดำเนินคดีอาญาควรจำกัดเฉพาะในกรณีที่ผู้กระทำผิดก่อกวน ทำให้เสียหาย หรือก่อให้เกิดปัญหาต่อโลกไซเบอร์ด้วยเจตนาทุจริตเท่านั้น
บีเอสเอเห็นว่า **การกำหนดโทษทางอาญาต่อหน่วยงานเอกชนที่ไม่ปฏิบัติตามคำขอของ กปช. ตามมาตรา 57 และมาตรา 58 นั้นเป็นบทลงโทษที่รุนแรงเกินควร** และไม่ควรมีโทษทางอาญาสำหรับการกระทำความผิดโดยไม่ตั้งใจ หรือเนื่องจากเหตุผลทางเทคนิค อันอาจทำให้บริษัทต่างชาติระงับแผนที่จะเข้ามาประกอบธุรกิจในประเทศไทยหากมีความเสี่ยงว่าบุคลากรของตนจะต้องมีความรับผิดทางอาญาสำหรับการกระทำความผิดโดยไม่ได้จงใจหรือการกระทำความผิดเพียงเล็กน้อย

เอฟ. การรักษาความลับ

บีเอสเอเห็นว่าบทบัญญัติที่เกี่ยวกับการรักษาความลับถูกลบทิ้งไปจากร่าง พ.ร.บ. ฉบับนี้ จึงขอเรียนเสนอเช่นเดิมว่า ร่างพระราชบัญญัติฯ ควรมีบทบัญญัติเพิ่มเติมที่ชัดเจนในเรื่องการรักษาความลับของข้อมูลที่อ่อนไหวและข้อมูลส่วนบุคคล ซึ่งรวมถึงการกำหนดหน้าที่ที่ชัดเจนของพนักงานเจ้าหน้าที่ในการปกป้องและรักษาความลับของข้อมูลดังกล่าว รวมถึงการกำหนดหน้าที่และขั้นตอนในการขอความยินยอม และวิธีใช้ เปิดเผย เก็บ และกำจัดข้อมูลดังกล่าวเมื่อไม่จำเป็นแล้วตามวัตถุประสงค์ทางกฎหมายของผู้ออกคำสั่ง

นอกจากนี้ ควรกำหนด**ประเภทของข้อมูลที่ได้รับการยกเว้นไม่ต้องเปิดเผย** เช่นข้อมูลที่ได้รับสิทธิพิเศษ หรือข้อมูลที่จะก่อให้เกิดการละเมิดสิทธิอื่น เช่นข้อมูลส่วนบุคคล หรือละเมิดสิทธิในทรัพย์สินทางปัญญาหรือความลับทางการค้า

ควรกำหนดให้เจ้าพนักงานของ กปช. มีความรับผิดทางอาญาด้วยหากมีการนำข้อมูลดังกล่าวไปใช้ในทางที่มิชอบด้วยเช่นกัน

จี. การแบ่งปันข้อมูลข่าวสาร

บีเอสเอเห็นว่า การแบ่งปันข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ ช่องโหว่ และเหตุทางไซเบอร์ ต่อผู้ที่ได้รับผลกระทบ ตลอดจนหน่วยงานอื่นๆ เพื่อป้องกันการโจมตี เป็นเรื่องที่สำคัญต่อการส่งเสริมการรักษาความมั่นคงปลอดภัยทางไซเบอร์
บีเอสเอขอเรียนย้ำว่า ร่างพระราชบัญญัติฯ ควรสนับสนุนให้มีการจัดทำนโยบายที่มีประสิทธิภาพในเรื่องการแบ่งปันข้อมูลข่าวสารระหว่างภาครัฐและเอกชน ระหว่างหน่วยงานเอกชนด้วยกัน และระหว่างหน่วยงานของรัฐด้วยกัน นอกจากนี้ นโยบายเรื่องการแบ่งปันข้อมูลข่าวสารควรมีข้อจำกัดเกี่ยวกับความรับผิดของหน่วยงานที่เป็นผู้แบ่งปันข้อมูลข่าวสาร โดยที่ยังคงสามารถปกป้องความเป็นส่วนตัวของผู้ที่ได้รับผลกระทบจากการแบ่งปันข้อมูลข่าวสาร อำนวยความสะดวกในการแบ่งปันข้อมูลข่าวสารหลายทาง ส่งเสริมให้ดำเนินการอย่างทันท่วงที และทำให้แน่ใจว่าข้อมูลข่าวสารที่ได้รับไปนั้นจะใช้เพื่อส่งเสริมการรักษาความมั่นคงปลอดภัยทางไซเบอร์เท่านั้น

เอช. ระยะเวลาของการบังคับใช้กฎหมาย

รัฐบาลควรกำหนดระยะเวลาอันสมควรระหว่างการประกาศใช้และการบังคับใช้กฎหมาย ซึ่งจะทำให้เกิดประโยชน์มากกว่ากับบุคคล องค์กรธุรกิจ และรัฐบาลเอง นอกจากนี้ รัฐบาลยังออกแนวทางในการปฏิบัติตามกฎหมายใหม่นี้ ในช่วงระยะเวลาระหว่างการประกาศใช้และการบังคับใช้กฎหมาย รวมถึงองค์กรธุรกิจสามารถเตรียมตัวเพื่อประเมินความพร้อมในการปฏิบัติตามกฎหมายใหม่ที่กำลังจะมีการบังคับใช้โดยทั่วไป ในประเทศอื่น ระยะเวลาการประกาศใช้และการบังคับใช้กฎหมายว่าด้วยเรื่องการป้องกันภัยไซเบอร์จะอยู่ที่ 2 ปี **บีเอสเอขอแนะนำให้กระทรวงฯ ให้ระยะเวลาไม่น้อยกว่า 2 ปี ก่อนที่จะมีการบังคับใช้กฎหมาย**

ไอ. แง่มุมอื่น ๆ ของนโยบายด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ

นอกจากนี้ บีเอสเอขอเรียนย้ำว่า นโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยควรครอบคลุมประเด็นที่สำคัญอื่นๆ ด้วย เช่น การปฏิบัติตามแนวทางในการจัดซื้อเทคโนโลยีและซอฟต์แวร์ของภาครัฐ การให้การสนับสนุนจากรัฐบาลอย่างเต็มที่ในด้านการวิจัยและพัฒนาเทคโนโลยีสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ โครงการให้ความรู้เพื่อเพิ่มความตระหนักรู้ การฝึกอบรม และการจัดทำนโยบายต่างประเทศให้ครอบคลุมถึงเรื่องการประสานความร่วมมือในการรักษาความมั่นคงปลอดภัยไซเบอร์ บีเอสเอขอสนับสนุนให้รัฐบาลไทยพิจารณาเพิ่มเติมประเด็นที่สำคัญเหล่านี้ไว้ในระเบียบข้อบังคับที่ออกโดยอาศัยร่างพระราชบัญญัตินี้

<u>บทสรุปและการดำเนินการขั้นต่อไป</u>

บีเอสเอขอแสดงความชื่นชมรัฐบาลไทยอีกครั้งสำหรับความพยายามในการปกป้องโครงสร้างพื้นฐานจากภัยคุกคามทางไซเบอร์และการก่ออาชญากรรมทางไซเบอร์ อย่างไรก็ดี บีเอสเอใคร่ขอความอนุเคราะห์ให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมพิจารณาประเด็นที่ได้เรียนเสนอไว้ข้างต้น เพื่อที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมจะสามารถจัดทำนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ ซึ่งคำนึงถึงเรื่องความเสี่ยงเป็นหลักและสอดคล้องกับแนวปฏิบัติในระดับสากล อันจะช่วยเสริมสร้างความเชื่อมั่นระหว่างภาครัฐและเอกชน และยกระดับความมั่นคงปลอดภัยของข้อมูลและโครงสร้างพื้นฐาน

นอกจากนี้ รัฐบาลควรเน้นย้ำเรื่องการป้องกันและการลดความเสี่ยงภัยไซเบอร์ โดยส่งเสริมให้องค์กรปฏิบัติตามวิธีปฏิบัติที่ดีที่มีอยู่แล้ว หรือมีแนวทางป้องกันภัยไซเบอร์ที่ดี เช่น การใช้ซอฟต์แวร์ที่มีสัญญาอนุญาตให้ใช้สิทธิและได้รับบริการความช่วยเหลือจากบริษัทซอฟต์แวร์ รวมถึงการใช้ฮาร์ดแวร์ด้วย ที่ต้องได้รับบริการอัพเดทด้านความปลอดภัยอย่างสม่ำเสมอ ตลอดจนไปถึงการป้องกันเครือข่ายที่มีประสิทธิภาพ ขั้นตอนการรับมือกับสถานการณ์ที่เกิดขึ้น การจัดการลดความเสี่ยง

บีเอสเอยินดีจะหารือกับท่านในเรื่องนี้เพิ่มเติมได้ทุกเมื่อ หากท่านมีข้อสงสัยหรือความเห็นประการใด กรุณาติดต่อ**นางสาววารุณี รัชตพัฒนากุล ผู้จัดการประจำประเทศไทยแห่งบีเอสเอ ได้ที่**

varuneer@bsa.org **หรือที่หมายเลข +668-1840-0591** บีเอสเอขอขอบพระคุณที่ท่านสละเวลาพิจารณาในเรื่องนี้

ขอแสดงความนับถือ

เจเร็ด แร้กแลนด์
ผู้อำนวยการอาวุโส ฝ่ายนโยบาย ภูมิภาคเอเชียแปซิฟิก
บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์

สำเนาถึง
ดร.พิเชฐ ดุรงคเวโรจน์ รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
นางสุรางคณา วายุภาพ ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

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:

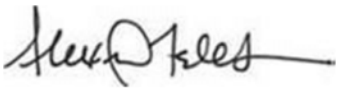
- The composition of the National Cyber Security Committee (**"NCSC"**) would benefit from the inclusion of **industry representatives**.
- The 2018 Bill should only apply to **"private agencies" incorporated in Thailand that operate or control critical infrastructure** (as defined in our April 17, 2018 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)	• 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	• 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
		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". • Sections 36 and 37 are broadly worded to apply to *all* private agencies, even where they may not be affected by a cyber incident.	but we urge that independent oversight and judicial review should apply more broadly to NCSC powers as they relate to "private agencies". • 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 *reasonable* and *practical.* • 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 *directly impacted* by the "significant cyber incident" (as defined in our earlier submission). This would avoid any suggestion that private agencies which are *not* 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 *actual and anticipated* cyber-attacks.	• The requirement to notify of *every actual or anticipated* 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 *anticipated* 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)	• 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 /	In addition to our earlier recommendations in relation to Section 47 of the 2018 Bill, we would like to add the following comments: • **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
		relevant guidelines, and assist under certain circumstances, *without a court order*. 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. • Regulated entities do not have rights to contest orders and a failure to comply could result in serious penalties.	• **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)	• 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.	• 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.

(คำแปล)

(กระดาษหัวจดหมายของบีเอสเอ) *(สภาธุรกิจสหรัฐอเมริกา-อาเซียน)*

วันที่ 21 พฤษภาคม 2561

นางสาวอัจฉรินทร์ พัฒนพันธ์ชัย
ปลัดกระทรวง
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
120 หมู่ที่ 3 ชั้น 6-9
ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550
ถนนแจ้งวัฒนะ
ทุ่งสองห้อง หลักสี่ กรุงเทพมหานคร 10210

เรื่อง ความเห็นเพิ่มเติมของภาคอุตสาหกรรมในเรื่องร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

เรียนท่านปลัดกระทรวง

ตามที่ บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์ (“**บีเอสเอ**”) และสภาธุรกิจสหรัฐอเมริกา-อาเซียน (“**สภาธุรกิจฯ**”) ได้เรียนเสนอความเห็นในเรื่องร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ตามหนังสือลงวันที่ 17 เมษายน 2561 ที่ผ่านมา (สำเนาหนังสือปรากฏอยู่ในภาคผนวก บี ของหนังสือฉบับนี้) นั้น

จากการศึกษาร่าง พ.ร.บ. ปี 2561 และการหารือกับกลุ่มสมาชิกเพิ่มเติม บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอความเห็นเพิ่มเติมจากความเห็นที่อ้างถึงข้างต้นมาตามภาคผนวก เอ ของหนังสือฉบับนี้ ซึ่งมีเนื้อหาโดยสรุปดังปรากฏด้านล่างนี้ บีเอสเอและสภาธุรกิจฯ ใคร่ขอความอนุเคราะห์ให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมพิจารณาความเห็นเพิ่มเติมดังกล่าวประกอบกับความเห็นที่ได้เรียนเสนอไว้เมื่อครั้งก่อนด้วยจักเป็นพระคุณยิ่ง

เนื้อหาของความเห็นเพิ่มเติมจากความเห็นตามหนังสือฉบับลงวันที่ 17 เมษายน 2561 สามารถกล่าวโดยสรุปได้ดังนี้

- การกำหนดให้มีกรรมการที่เป็น**ผู้แทนจากภาคอุตสาหกรรม**จะเป็นประโยชน์ต่อคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (“**กปช.**”)
- ร่าง พ.ร.บ. ปี 2561 ควรใช้บังคับกับ “**หน่วยงานเอกชน**” **ที่จัดตั้งขึ้นในประเทศไทยและเป็นผู้ประกอบกิจการหรือเป็นผู้ควบคุมโครงสร้างพื้นฐานที่สำคัญ (ตามคำจำกัดความที่ได้เรียน**

เสนอไว้ในหนังสือฉบับวันที่ 17 เมษายน 2561) เท่านั้น และควรกำหนดหน้าที่ให้กับหน่วยงานเอกชนดังกล่าวไว้อย่างชัดเจน โดยจำกัดเฉพาะแต่เพียงหน้าที่ที่**มีความเหมาะสม**และ**สามารถปฏิบัติได้จริง**

- **หน้าที่ในการรายงาน**ควรจำกัดเฉพาะกรณี**เหตุภัยคุกคามทางไซเบอร์ที่สำคัญซึ่งได้เกิดขึ้นแล้ว** เท่านั้น โดยไม่รวมถึงเหตุภัยคุกคามทางไซเบอร์ที่ไม่มีความสำคัญ หรือเหตุภัยคุกคามทางไซเบอร์ที่ “คาด” ว่าจะเกิดขึ้น
- การใช้อำนาจในการเข้าถึง**ข้อมูลและเครื่องมือ**ควรเป็นไปอย่าง**ได้สัดส่วน**และมีมาตรการ**ตรวจสอบและถ่วงดุล**ที่เหมาะสม **ซึ่งรวมถึงการตรวจสอบความชอบด้วยกฎหมายโดยศาลและสิทธิในการโต้แย้งหรืออุทธรณ์คำสั่ง**
- ควรมี**หน่วยงานกำกับดูแลเพียงหน่วยงานเดียว**ที่มีอำนาจหน้าที่ในการตรวจสอบดูแลและบังคับใช้กฎหมายตามร่าง พ.ร.บ. ปี 2561
- ร่าง พ.ร.บ. ปี 2561 ควรบัญญัติในเรื่อง**การรักษาความลับและการคุ้มครองความเป็นส่วนตัว**ไว้อย่างชัดแจ้งด้วย
- ร่าง พ.ร.บ. ปี 2561 ควรส่งเสริมให้มีการ**แบ่งปันข้อมูลข่าวสาร ซึ่งรวมถึงโดยการจำกัด**ความรับผิดที่เกิดขึ้นจากการแบ่งปันข้อมูลข่าวสารไว้อย่างเหมาะสม

บีเอสเอและสภาธุรกิจฯ ขอแสดงความชื่นชมต่อกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมอีกครั้งหนึ่งมาในโอกาสนี้ที่ได้เปิดรับฟังความคิดเห็นจากภาคเอกชนและผู้มีส่วนได้เสียอื่นๆ ในการจัดทำกฎหมายนี้ และขอสนับสนุนให้ยังคงมีการเปิดโอกาสให้มีการสื่อสารและหารือกับภาคเอกชนต่อไป โดยเฉพาะอย่างยิ่ง ในการจัดทำระเบียบและประกาศต่างๆ หรือข้อกำหนดเพิ่มเติมใดๆ ที่ออกตามร่าง พ.ร.บ. ปี 2561 นี้ ควรมีขั้นตอนการหารือกับภาคเอกชนเช่นกัน เพื่อให้เกิดความชัดเจนและความสอดคล้องกัน

บีเอสเอและสภาธุรกิจฯ ยินดีจะหารือกับท่านในเรื่องนี้เพิ่มเติมได้ทุกเมื่อเช่นเคย หากท่านมีข้อสงสัยหรือความเห็นประการใด กรุณาติดต่อโดยตรงไปที่ afeldman@usasean.org หรือที่หมายเลข 202-375-4393 หรือที่ jaredr@bsa.org หรือที่หมายเลข +65-6292-9609 หรือติดต่อ**นางสาววารุณี รัชตพัฒนากุล ผู้จัดการประจำประเทศไทยแห่งบีเอสเอ ได้ที่** varuneer@bsa.org **หรือที่หมายเลข +668-1840-0591 หรือนางสาวเอลล่า ดวงแก้ว ผู้จัดการประจำประเทศไทยแห่งสภาธุรกิจสหรัฐอเมริกา-อาเซียน ที่** eduangkaew@usasean.org **หรือที่หมายเลข 202-440-3642**

บีเอสเอและสภาธุรกิจฯ ขอขอบพระคุณที่ท่านสละเวลาพิจารณาในเรื่องนี้

ขอแสดงความนับถือ

(ลายมือชื่อ)

อเล็กซานเดอร์ ซี. เฟล์ดแมน
ประธานและประธานเจ้าหน้าที่บริหาร
ภูมิภาคเอเชีย
สภาธุรกิจสหรัฐอเมริกา-อาเซียน

(ลายมือชื่อ)

จาเร็ด แร้กแลนด์
ผู้อำนวยการอาวุโส ฝ่ายนโยบาย
ภูมิภาคเอเชีย แปซิฟิก
บีเอสเอ I พันธมิตรธุรกิจซอฟต์แวร์

สำเนาถึง

1. ดร.พิเชฐ ดุรงคเวโรจน์ รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
2. นางสุรางคณา วายุภาพ ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ภาคผนวก เอ – ความเห็นเพิ่มเติมเกี่ยวกับร่าง พ.ร.บ. ปี 2561

บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอความเห็นเพิ่มเติมเกี่ยวกับร่าง พ.ร.บ. ปี 2561 ตามที่ปรากฏในตารางด้านล่างนี้ เพื่อประกอบความเห็นที่ได้เรียนเสนอไว้ก่อนหน้านี้ ตามหนังสือลงวันที่ 17 เมษายน 2561 (ภาคผนวก บี)

ข้อ	เรื่อง	รายละเอียด	ความเห็นของบีเอสเอและสภาธุรกิจฯ
เอ. กรรมการในคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ			
1.	**กรรมการใน กปช.** (มาตรา 6)	แม้ร่าง พ.ร.บ. ปี 2561 จะได้มีการกำหนดให้แต่งตั้งกรรมการจากหน่วยงานที่หลากหลายมากขึ้นแล้ว แต่ยังไม่มีกรรมการรายใดที่เป็นผู้แทนจากภาคอุตสาหกรรม	จากความเห็นที่ได้เรียนเสนอไว้ในครั้งก่อนว่า กปช. ควรประกอบด้วยกรรมการที่แต่งตั้งมาจากคณะกรรมการสิทธิมนุษยชนและสำนักงานผู้ตรวจการแผ่นดินด้วยนั้น บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอเพิ่มเติมว่า กปช. ควรประกอบด้วยกรรมการที่มาจากภาคอุตสาหกรรมด้วย ซึ่งไม่เพียงแต่จะช่วยให้คณะกรรมการมีมุมมองที่รอบด้านมากขึ้นเท่านั้น แต่ยังช่วยเสริมสร้างการประสานความร่วมมือระหว่างภาครัฐและเอกชน อันจะนำไปสู่การปฏิบัติที่ก่อให้เกิดประสิทธิภาพสูงสุดด้วย
บี. อำนาจของ กปช.			
2.	**คำจำกัดความของ “หน่วยงานเอกชน” และความจำเป็นในการกำหนดหลักเกณฑ์ที่เหมาะสม**	ร่าง พ.ร.บ. ปี 2561 ประสงค์จะกำกับดูแล “หน่วยงานเอกชน” ซึ่งได้แก่หน่วยงานที่จัดตั้งขึ้น ไม่ว่าจะเป็นการดำเนินงานที่แสวงหากำไร หรือที่ไม่แสวงหากำไร ทั้งนี้ ไม่ว่าจะจดทะเบียนเป็นนิติบุคคลหรือไม่ก็ตาม คำจำกัดความของ “หน่วยงานเอกชน” ดังกล่าวนี้อาจกว้างเกินไปสำหรับเรื่องการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และควรกำหนดให้แคบลงกว่านี้	บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า ในกฎหมายนี้ คำจำกัดความของ “หน่วยงานเอกชน” ควรจำกัดอยู่ที่บริษัทที่จัดตั้งขึ้นในประเทศไทยซึ่งเป็นผู้ประกอบกิจการหรือเป็นผู้ควบคุม “โครงสร้างพื้นฐานที่สำคัญ” (ตามคำจำกัดความที่ได้เรียนเสนอไว้ในหนังสือฉบับก่อน) ในประเทศไทยเท่านั้น

ข้อ	เรื่อง	รายละเอียด	ความเห็นของบีเอสเอและสภาธุรกิจฯ
	(มาตรา 3, 36 และ 37)		
3.	**หน้าที่ในการบังคับบัญชาและสั่งการให้หน่วยงานต่าง ๆ ปฏิบัติงาน** (มาตรา 33, 34, 36 และ 37)	• อำนาจของ กปช. ในการบังคับบัญชาและสั่งการหน่วยงานเอกชนตามมาตรา 33 และในการสั่งการให้หน่วยงานเอกชน “กระทำการหรืองดเว้นกระทำการอย่างใดอย่างหนึ่ง” ตามมาตรา 37 มีข้อจำกัดอยู่เพียงเล็กน้อย • ตามมาตรา 34 กปช. มีดุลพินิจอย่างกว้างขวางในการมีมติว่าหน่วยงานเอกชนไม่ปฏิบัติตามพระราชบัญญัตินี้ หรือปฏิบัติการโดยขัดหรือแย้งกับแนวทางที่กำหนด หรือในการแจ้งให้แก้ไข ยกเลิก หรือยุติการดำเนินการดังกล่าว ซึ่งหากไม่ดำเนินการภายในเวลาที่กำหนด คณะรัฐมนตรีจะเป็นผู้พิจารณาสั่งการต่อไปตามดุลพินิจที่มีอย่างกว้างขวาง • บทบัญญัติในมาตรา 36 และมาตรา 37 ใช้ถ้อยคำที่กว้างเกินไปโดยบังคับใช้กับหน่วยงานเอกชน *ทั้งหมด* แม้กระทั่งหน่วยงานที่ไม่ได้รับผลกระทบจากเหตุภัยคุกคามทางไซเบอร์	• ควรกำหนดและจำกัดอำนาจที่ให้แก่ กปช. และหน่วยงานที่ได้รับแต่งตั้งให้มีความชัดเจนยิ่งขึ้น รวมถึงให้มีการตรวจสอบโดยหน่วยงานอิสระและการตรวจสอบความชอบด้วยกฎหมายโดยศาล อีกทั้งหน่วยงานเอกชนและบุคคลภายนอกควรมีโอกาสอย่างเต็มที่ในการโต้แย้งคำสั่งและยื่นอุทธรณ์ต่อศาลหากไม่เห็นพ้องด้วยกับคำวินิจฉัย บีเอสเอและสภาธุรกิจฯ ทราบว่าตาม ร่าง พ.ร.บ. ปี 2561 นั้น จำเป็นต้องขอคำสั่งศาลก่อนใช้อำนาจบางประการ (เว้นแต่กรณีจำเป็นเร่งด่วน) อย่างไรก็ดี บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า การใช้อำนาจของ กปช. ควรต้องมีการตรวจสอบโดยหน่วยงานอิสระและการตรวจสอบความชอบด้วยกฎหมายโดยศาลในหลายกรณีมากขึ้น เนื่องจากเป็นเรื่องที่เกี่ยวข้องกับ “หน่วยงานเอกชน” • มาตรา 34 ควรแก้ไขให้มีการระบุให้ชัดเจนว่า กปช. มีอำนาจบังคับบัญชาหรือสั่งการหน่วยงานเอกชนให้ดำเนินการอย่างไรได้บ้าง ทั้งนี้ เพื่อที่จะได้มีหลักเกณฑ์ที่ชัดเจน เพื่อให้ทุกฝ่ายมีความเข้าใจและสามารถปฏิบัติตามได้อย่างถูกต้อง อันจะนำไปสู่ความชัดเจนในเรื่องการรักษาความมั่นคงไซเบอร์ในประเทศไทย • บีเอสเอและสภาธุรกิจฯ มีความกังวลว่า ตามร่าง พ.ร.บ. ปี 2561 (รวมถึงหน้าที่ตามมาตรา 36 และมาตรา 37 เป็นต้น) หน่วยงานเอกชนมีหน้าที่ต้องดำเนินการบางประการในกรณีที่เกิดเหตุภัยคุกคามทางไซเบอร์ที่อาจ

ข้อ	เรื่อง	รายละเอียด	ความเห็นของบีเอสเอและสภาธุรกิจฯ
			ไม่ได้อยู่ภายใต้การควบคุมของหน่วยงานเอกชนนั้นแต่อย่างใด หรืออาจมีความไม่สมเหตุสมผล ไม่สามารถปฏิบัติได้จริง หรือไม่ได้สัดส่วนแก่กรณีด้วยเหตุนี้ บีเอสเอและสภาธุรกิจฯ จึงขอเรียนเสนอว่า ในร่าง พ.ร.บ. ปี 2561 ทั้งฉบับ (ไม่เพียงแต่เฉพาะบางมาตรา) การกำหนดหน้าที่แก่หน่วยงานเอกชนควรต้องจำกัดเฉพาะแต่เพียงหน้าที่ที่*มีความเหมาะสม*และ*สามารถนำไปปฏิบัติได้จริง*เท่านั้น • สำหรับมาตรา 36 และมาตรา 37 นอกเหนือจากความเห็นที่ได้เรียนเสนอไว้ก่อนหน้านี้ว่าควรใช้หลักเกณฑ์ในเรื่องเหตุภัยคุมคามทางไซเบอร์ที่สำคัญแล้ว บีเอสเอและสภาธุรกิจฯ มีความเห็นว่า ทั้งสองมาตรานี้ควรใช้บังคับเฉพาะกับหน่วยงานที่*ได้รับผลกระทบโดยตรง*จาก “เหตุภัยคุกคามทางไซเบอร์ที่สำคัญ” (ตามคำจำกัดความที่ได้เรียนเสนอไว้ในหนังสือฉบับก่อน) เท่านั้น เพื่อที่จะได้หลีกเลี่ยงไม่ให้ตีความได้ว่าหน่วยงานเอกชนที่*ไม่ได้รับผลกระทบ*จะต้องมีหน้าที่ตามมาตรานี้
ซี. หน้าที่ในการรายงานเหตุภัยคุกคามทางไซเบอร์			
4.	**หน้าที่ในการรายงาน** (มาตรา 35 และ 40)	มาตรา 35 กำหนดหน้าที่ในการรายงานทั้งใน*กรณีที่เกิดและคาดว่าจะเกิด*เหตุภัยคุกคามทางไซเบอร์	• กฎหมายไม่ควรกำหนดให้มีหน้าที่ต้องรายงาน*ทุกกรณีที่เกิดหรือคาดว่าจะเกิด*เหตุภัยคุกคามทางไซเบอร์ เนื่องจากประเภทของเหตุภัยคุกคามทางไซเบอร์และที่มาของเหตุดังกล่าวมีการเปลี่ยนแปลงอยู่ตลอดเวลา ด้วยเหตุนี้ บริการบางอย่างจึงอาจตกเป็นเป้าหมายของการโจมตีได้วันละหลายพันครั้ง (หรือกว่านั้น) ซึ่งส่วนใหญ่แล้วสามารถป้องกันได้สำเร็จ แม้ว่าองค์กรต่างๆ อาจจะมีมาตรการที่กำหนดขึ้นเพื่อป้องกันเหตุภัยคุกคามทางไซเบอร์โดยใช้วิธีการที่องค์กรต่างๆ ใช้กันอยู่ล่าสุด แต่การที่จะสามารถ

ข้อ	เรื่อง	รายละเอียด	ความเห็นของบีเอสเอและสภาธุรกิจฯ
			ระบุเหตุภัยคุกคามได้ทุกครั้งหรือรายงานให้พนักงานเจ้าหน้าที่ทราบทุกครั้งที่คาดว่าจะเกิดเหตุภัยคุกคามก็เป็นเรื่องที่ย่อมเป็นไปไม่ได้ นอกจากนี้หน้าที่ดังกล่าวจะสร้างภาระอย่างยิ่ง ในขณะที่พนักงานเจ้าหน้าที่ไม่สามารถนำข้อมูลไปใช้ประโยชน์ได้เท่าใดนัก เนื่องจากต้องประมวลผลรายงานกรณีที่คาดว่าจะเกิดเหตุภัยคุกคามซึ่งมีจำนวนมหาศาล ซึ่งส่วนใหญ่แล้วไม่ได้เกิดขึ้นจริง (หรืออาจป้องกันได้สำเร็จหรือไม่มีความเสี่ยงว่าจะมีความเสียหายเกิดขึ้นจริง) • บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอให้ใช้ถ้อยคำที่สอดคล้องกันตลอดทั้งฉบับ และกำหนดคำจำกัดความของ “เหตุภัยคุกคามทางไซเบอร์” และ “เหตุภัยคุกคามทางไซเบอร์ที่สำคัญ” ให้ชัดเจน (ตามที่ได้เรียนเสนอไว้ในหนังสือฉบับก่อน) • นอกจากนี้ บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า ควรกำหนดหน้าที่ในการรายงานเฉพาะในกรณีที่เข้า “หลักเกณฑ์ที่พิจารณาจากความสำคัญ” เช่น กรณีของเหตุภัยคุกคามทางไซเบอร์ที่สำคัญและมีความเสี่ยงอย่างแท้จริงว่าจะเกิดความเสียหายอย่างร้ายแรง • บีเอสเอและสภาธุรกิจฯ เชื่อว่า กฎหมายในเรื่องการรักษาความมั่นคงปลอดภัยทางไซเบอร์ควรมีขึ้นเพื่อสร้างสภาพแวดล้อมที่เอื้อต่อการแบ่งปันข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ มิใช่เพื่อบังคับให้รายงานทุกกรณีที่คาดว่าจะเกิดเหตุภัยคุกคามทางไซเบอร์ ความเห็นเรื่องนี้ในรายละเอียดปรากฏอยู่ในข้อ 8 ด้านล่าง

ข้อ	เรื่อง	รายละเอียด	ความเห็นของบีเอสเอและสภาธุรกิจฯ
ดี. อำนาจหน้าที่ในการสอดส่องดูแล			
5.	**การเข้าถึงข้อมูลและเครื่องมือ** (มาตรา 34, 36, 37, 43, 46 และ 47)	• มาตรา 43 ได้ให้อำนาจแก่เจ้าหน้าที่ของรัฐที่เกี่ยวข้องและสำนักงาน กปช. ในการขอให้มีการให้ข้อมูล สนับสนุนบุคลากร หรือใช้เครื่องมือทางอิเล็กทรอนิกส์ของหน่วยงานเอกชน โดย กปช. ต้องขอให้ศาลมีคำสั่งหากหน่วยงานเอกชนไม่ยินยอมให้ข้อมูล ให้การสนับสนุนบุคลากร หรือจัดให้ใช้เครื่องมือทางอิเล็กทรอนิกส์ • มาตรา 47 ให้อำนาจแก่เลขาธิการในการเรียกบุคคลมาให้ถ้อยคำ ส่งเอกสารหรือหลักฐาน หรือดำเนินการเพื่อประโยชน์แห่งการปฏิบัติหน้าที่ของ กปช. หรือเข้าถึงข้อมูลการติดต่อสื่อสาร (รวมถึงการติดต่อสื่อสารทางไปรษณีย์ โทรศัพท์ คอมพิวเตอร์ อุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศใด) ตามที่เรียนไว้ในหนังสือฉบับก่อนหน้านี้ แม้จะกำหนดให้เลขาธิการต้องขอคำสั่งศาลก่อนเข้าถึงข้อมูลการติดต่อสื่อสาร แต่ “กรณีจำเป็นเร่งด่วนหากไม่ดำเนินการในทันทีจะเกิดความเสียหายอย่างร้ายแรง” ที่เป็นข้อยกเว้นนั้นก็มีขอบเขตที่กว้าง นอกจากนี้ มาตรา 47 ได้ให้อำนาจแก่ กปช.	สำหรับมาตรา 47 แห่งร่าง พ.ร.บ. ปี 2561 บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอเพิ่มเติมดังนี้ • **การสั่งการ กำกับ หรือขอให้มีการให้ข้อมูลหรือการสนับสนุนใด ๆ ควรจำกัดเฉพาะในกรณีที่มีความเสี่ยงสูงว่าจะเกิดความเสียหายอย่างร้ายแรง** บีเอสเอและสภาธุรกิจฯ ขอเรียนว่า ความเสียหายดังกล่าวควรต้องพิจารณาร่วมกับหลักเกณฑ์อื่นด้วย เช่น ผลกระทบต่อชุมชน การพิจารณาในเชิงเศรษฐกิจ และการพิจารณาเรื่องความเป็นไปได้ในทางปฏิบัติ • **หน้าที่ตามมาตรา 34 ในการปฏิบัติตามคำสั่งของ กปช. ควรมีการกำหนดเวลาตามสมควรสำหรับการปฏิบัติดังกล่าว** ในทุกกรณีกำหนดเวลาดังกล่าวควรมีความเหมาะสมเมื่อพิจารณาจากปัจจัยทั้งหมดที่เกี่ยวข้อง เช่น ผลกระทบที่จะได้รับ ความสามารถของบริษัทในการดำเนินการตามคำสั่งได้จริง ค่าใช้จ่ายในการดำเนินการดังกล่าว และประโยชน์ที่จะได้รับจากการดำเนินการดังกล่าว ปัจจุบัน มาตรา 34 ให้อำนาจแก่ กปช. ในการกำหนดเวลาได้ตามดุลพินิจของ กปช. ซึ่งอาจไม่มีความเหมาะสม และการไม่ปฏิบัติตามคำสั่งนั้นอาจทำให้บริษัทที่เกี่ยวข้องได้รับโทษที่รุนแรงได้ • **การขอข้อมูลจากหน่วยงานเอกชนตามมาตรา 43 และ 47 ควรมีกรณียกเว้นและควรต้องแจ้งให้บุคคลภายนอกที่ได้รับผลกระทบทราบ** บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า บุคคลภายนอกที่เป็น

ข้อ	เรื่อง	รายละเอียด	ความเห็นของบีเอสเอและสภาธุรกิจฯ
		ในการเสนอให้หน่วยงานรัฐที่มีหน้าที่กำกับดูแลพิจารณาลงโทษหน่วยงานเอกชนที่ไม่ปฏิบัติตามคำสั่งของ กปช. “โดยใช้อำนาจตามกฎหมายประกาศ ข้อบังคับอื่นใดที่มีอยู่” • นอกจากนี้ มาตรา 34, 36, 37 และ 46 ได้ให้อำนาจแก่พนักงานเจ้าหน้าที่ในการสั่งการ ขอ และกำกับให้หน่วยงานเอกชนกระทำการหรืองดเว้นกระทำการอย่างใดอย่างหนึ่ง ปฏิบัติการตามร่าง พ.ร.บ. ปี 2561 นี้ หรือแนวทางที่เกี่ยวข้อง และให้ความช่วยเหลือในสถานการณ์อย่างใดอย่างหนึ่ง *โดยที่ไม่ต้องมีคำสั่งศาล* โดยมีข้อยกเว้นเพียงกรณีเดียวตามมาตรา 44 ที่ กปช. ต้องได้รับอนุญาตจากศาลหาก กปช. ต้องใช้เครื่องมือสื่อสาร เครื่องมือทางอิเล็กทรอนิกส์ หรือด้วยวิธีการอื่นใดเพื่อติดตามการก่อให้เกิดภัยคุกคามทางไซเบอร์อันมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลอื่น • หน่วยงานที่อยู่ภายใต้บังคับของกฎหมายนี้ไม่มีสิทธิโต้แย้งคำสั่ง อีกทั้งการไม่ปฏิบัติตามคำสั่งอาจทำให้ได้รับโทษที่รุนแรงได้	เจ้าของข้อมูลที่ถูกเปิดเผยตามมาตรานี้ควรมีสิทธิได้รับแจ้งก่อนที่จะมีการเปิดเผยข้อมูลนั้นเพื่อให้บุคคลภายนอกดังกล่าวได้มีโอกาสคัดค้านการเปิดเผยข้อมูล • **อำนาจในการเข้าถึงข้อมูลควรต้องมีการตรวจสอบและการถ่วงดุลตามควรเสมอ** เช่น การตรวจสอบความชอบด้วยกฎหมายโดยศาล (ได้แก่ การขอคำสั่งศาล) และสิทธิในการโต้แย้งคำสั่ง • **การพิจารณาลงโทษตามมาตรา 47 มีความไม่ชัดเจน** บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า มาตรา 47 ควรกำหนดโทษที่หน่วยงานเอกชนอาจได้รับให้ชัดเจน มิใช่เพียงแค่อ้างถึงกฎหมาย ประกาศ หรือข้อบังคับอื่นใด

ข้อ	เรื่อง	รายละเอียด	ความเห็นของบีเอสเอและสภาธุรกิจฯ
เรื่องอื่น ๆ			
6.	**กฎหมายและเจ้าหน้าที่มีอำนาจซ้ำซ้อนกัน** (มาตรา 7, 14, 17 และ มาตรา 30 ถึง 52)	ร่าง พ.ร.บ. ปี 2561 ให้อำนาจแก่เจ้าหน้าที่หลายราย (รวมถึงกรรมการที่แต่งตั้งจากหลากหลายองค์กร รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และคณะรัฐมนตรี) ในการขอความร่วมมือและสั่งการให้หน่วยงานเอกชนกระทำการหรืองดเว้นกระทำการใดๆ ในสถานการณ์หนึ่งๆ	ตามร่าง พ.ร.บ. ปี 2561 อำนาจที่ให้แก่เจ้าหน้าที่หลายรายอาจทำให้มีการสั่งการที่ขัดแย้งกัน ซึ่งทำให้หน่วยงานเอกชนอาจต้องกลั่นกรองว่าจะดำเนินการอย่างไรกับคำสั่งต่างๆ ที่ได้รับจากเจ้าหน้าที่หลายราย โดยเฉพาะในกรณีเหตุภัยคุกคามทางไซเบอร์ที่จำเป็นต้องดำเนินการในทันที เนื่องจากการติดต่อเจ้าหน้าที่หลายรายย่อมทำให้เกิดความล่าช้าในการดำเนินการ ด้วยเหตุนี้ บีเอสเอและสภาธุรกิจฯ จึงขอเรียนเสนอให้มีหน่วยงานกำกับดูแลเพียงหน่วยงานเดียวที่มีอำนาจหน้าที่ในการตรวจสอบดูแลและบังคับใช้กฎหมายตามร่าง พ.ร.บ. ปี 2561 แทนการกำหนดให้หลายหน่วยงานมีอำนาจหน้าที่ดังกล่าว นอกจากนี้ อำนาจของหน่วยงานดังกล่าวต้องมีการควบคุมโดยมีกฎระเบียบที่โปร่งใสและมีกฎหมายที่กำหนดอำนาจของหน่วยงานนั้นไว้อย่างชัดเจน อีกทั้งมีการตรวจสอบโดยรัฐมนตรีและศาล
7.	**การรักษาความลับ** (มาตรา 48)	• นอกจากมาตรา 48 แล้ว ไม่มีบทบัญญัติอื่นใดในร่าง พ.ร.บ. ปี 2561 ที่กล่าวถึงเรื่องการรักษาความลับหรือการปกป้องความเป็นส่วนตัว • แม้มาตรา 48 จะกำหนดโทษสำหรับพนักงานเจ้าหน้าที่ที่เปิดเผยข้อมูลที่ได้มาโดยการใช้อำนาจของตน แต่การคุ้มครองดังกล่าวจำกัดแต่เพียงการเปิดเผยแก่บุคคลอื่น แต่ไม่ได้ห้ามการใช้ข้อมูลดังกล่าวโดยพนักงานเจ้าหน้าที่รายนั้นเองเพื่อประโยชน์ของตน	บีเอสเอและสภาธุรกิจฯ ขอเรียนว่า ร่าง พ.ร.บ. ปี 2561 ควรมีบทบัญญัติเพิ่มเติมที่ชัดเจนในเรื่องการรักษาความลับและการปกป้องข้อมูลส่วนบุคคล ซึ่งรวมถึงการกำหนดหน้าที่ที่ชัดเจนของพนักงานเจ้าหน้าที่ในการปกป้องและรักษาความลับของข้อมูลดังกล่าว รวมถึงการกำหนดหน้าที่และขั้นตอนในการขอความยินยอม และวิธีใช้ เปิดเผย เก็บ และกำจัดข้อมูลดังกล่าวเมื่อไม่จำเป็นแล้ว

ข้อ	เรื่อง	รายละเอียด	ความเห็นของบีเอสเอและสภาธุรกิจฯ
8.	**การแบ่งปันข้อมูลข่าวสาร** (ทั่วไป)	ร่าง พ.ร.บ. ปี 2561 ไม่มีการกล่าวถึงเรื่องการแบ่งปันข้อมูลไว้อย่างชัดแจ้ง	• บีเอสเอและสภาธุรกิจฯ เห็นว่า การแบ่งปันข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ ช่องโหว่ และเหตุทางไซเบอร์ ต่อผู้ที่ได้รับผลกระทบตลอดจนหน่วยงานอื่นๆ เพื่อป้องกันการโจมตี เป็นเรื่องที่สำคัญต่อการส่งเสริมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และเป็นวิธีที่น่าจะมีประสิทธิภาพมากกว่าการรายงานเหตุภัยคุกคามทางไซเบอร์ • เนื่องจากเป้าหมายของการโจมตีอาจเป็นได้ทั้งภาคเอกชนและหน่วยงานของรัฐทั่วประเทศ บีเอสเอและสภาธุรกิจฯ จึงขอเรียนเสนอว่า ร่าง พ.ร.บ. ปี 2561 ควรสนับสนุนให้มีการจัดทำนโยบายที่มีประสิทธิภาพในเรื่องการแบ่งปันข้อมูลข่าวสารระหว่างภาครัฐและเอกชน ระหว่างหน่วยงานเอกชนด้วยกัน และระหว่างหน่วยงานของรัฐด้วยกัน • บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า ร่าง พ.ร.บ. ปี 2561 และนโยบายเรื่องการแบ่งปันข้อมูลข่าวสารควรมีข้อจำกัดเกี่ยวกับความรับผิดที่หน่วยงานที่เป็นผู้แบ่งปันข้อมูลข่าวสารอาจมี โดยที่ยังคงสามารถปกป้องความเป็นส่วนตัวของผู้ที่ได้รับผลกระทบจากการแบ่งปันข้อมูลข่าวสาร อำนวยความสะดวกในการแบ่งปันข้อมูลข่าวสารหลายทาง ส่งเสริมให้ดำเนินการอย่างทันท่วงที และทำให้แน่ใจว่าข้อมูลข่าวสารที่ได้รับไปนั้นจะใช้เพื่อส่งเสริมการรักษาความมั่นคงปลอดภัยทางไซเบอร์เท่านั้น

Annex C:
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, Informatica, 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 agencies[3] 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** 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 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)

(คำแปล)

(กระดาษหัวจดหมายของบีเอสเอ) *(สภาธุรกิจสหรัฐอเมริกา-อาเซียน)*

วันที่ 17 เมษายน 2561

นางสาวอัจฉรินทร์ พัฒนพันธ์ชัย
ปลัดกระทรวง
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
120 หมู่ที่ 3 ชั้น 6-9
ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550
ถนนแจ้งวัฒนะ
ทุ่งสองห้อง หลักสี่ กรุงเทพมหานคร 10210

เรื่อง ความเห็นของภาคอุตสาหกรรมในเรื่องร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

เรียนท่านปลัดกระทรวง

1. ความนำและคำชี้แจงเรื่องส่วนได้เสียในร่างพระราชบัญญัติ

บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์ (“**บีเอสเอ**”)[1] และสภาธุรกิจสหรัฐอเมริกา-อาเซียน (**สภาธุรกิจฯ**)[2] เป็นผู้กระทำการแทนบริษัทอเมริกันชั้นนำด้านเทคโนโลยีที่ประกอบธุรกิจในประเทศไทย โดยมีสมาชิกเป็นบริษัทแนวหน้าด้านนวัตกรรมที่ขับเคลื่อนด้วยข้อมูล ผู้พัฒนาและนำเสนอผลิตภัณฑ์ซอฟต์แวร์ที่มีความสำคัญและจำเป็น เครื่องมือรักษาความปลอดภัย อุปกรณ์สื่อสาร เซิร์ฟเวอร์ และคอมพิวเตอร์ ซึ่งเป็น

[1] บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์ (www.bsa.org) เป็นหน่วยงานชั้นนำที่ทำหน้าที่เป็นผู้แทนในการรักษาสิทธิประโยชน์ของอุตสาหกรรมซอฟต์แวร์ในทั่วโลกต่อรัฐบาลและในตลาดระดับสากล สมาชิกของบีเอสเอรวมถึง Adobe, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, Box, CA Technologies, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Microsoft, Okta, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation และ Workday

[2] ตลอดกว่า 30 ปีที่ผ่านมา สภาธุรกิจสหรัฐอเมริกา-อาเซียนเป็นองค์กรชั้นนำที่ทำหน้าที่เป็นผู้แทนของบริษัทสหรัฐที่ดำเนินกิจการอยู่ในกลุ่มประเทศอาเซียนซึ่งเป็นประชาคมที่เติบโตขึ้นอย่างต่อเนื่อง สมาชิกของสภาธุรกิจฯ กว่า 150 ราย มีรายได้โดยรวมถึงกว่า 6 ล้านล้านดอลลาร์สหรัฐ และมีพนักงานกว่า 13 ล้านคนในทั่วโลก สมาชิกของสภาธุรกิจฯ ล้วนเป็นบริษัทสหรัฐขนาดใหญ่ที่สุดที่ดำเนินกิจการอยู่ในกลุ่มประเทศอาเซียน ซึ่งมีตั้งแต่บริษัทที่เพิ่งเข้ามายังภูมิภาคนี้ไปจนถึงบริษัทที่ดำเนินกิจการอยู่ในเอเชียตะวันออกเฉียงใต้เป็นเวลากว่า 100 ปีมาแล้ว สภาธุรกิจฯ มีสำนักงานอยู่ที่กรุงวอชิงตัน ดี.ซี., เมืองนิวยอร์ก รัฐนิวยอร์ก, กรุงเทพมหานคร ประเทศไทย, กรุงฮานอย เวียดนาม, กรุงจาการ์ตา อินโดนีเซีย, กรุงกัวลาลัมเปอร์ มาเลเซีย, กรุงมะนิลา ฟิลิปปินส์ และสิงคโปร์

สิ่งที่ขับเคลื่อนเศรษฐกิจข้อมูลข่าวสารในทั่วโลกและทำให้มนุษย์มีความเป็นอยู่ในชีวิตประจำวันที่ดีขึ้น สมาชิกของเราได้รับความไว้วางใจจากลูกค้าในการจัดให้เทคโนโลยีรักษาความปลอดภัยที่สำคัญเพื่อปกป้องจากภัยคุกคามทางไซเบอร์ ภัยคุกคามเหล่านี้อาจเกิดขึ้นจากผู้ประสงค์ร้ายที่มีวัตถุประสงค์แตกต่างกันไป ซึ่งรวมถึงผู้ที่ต้องการขโมยอัตลักษณ์ของเรา ทำร้ายบุคคลที่เรารัก เอาไปซึ่งความลับที่มีค่าในทางการค้า หรือเป็นภัยต่อความมั่นคงของชาติ

ด้วยเหตุที่เรียนมานี้ สมาชิกของเราจึงเป็นผู้มีส่วนได้เสียโดยตรงในการที่รัฐบาลไทยมีแผนจะเสนอร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (“**ร่าง พ.ร.บ. ปี 2561**”)

บีเอสเอและสภาธุรกิจฯ ได้ทำงานอย่างใกล้ชิดกับรัฐบาลในทั่วโลกในเรื่องเกี่ยวกับการพัฒนานโยบายและกฎหมายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศต่างๆ อันทำให้เราได้ประจักษ์ถึงศักยภาพของนโยบายและกฎหมายดังกล่าวที่จะระงับยับยั้งและจัดการกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ และสามารถปกป้องความเป็นส่วนตัวและเสรีภาพของประชาชนได้ในขณะเดียวกัน บีเอสเอได้นำประสบการณ์ดังกล่าวมาใช้ในการพัฒนากรอบนโยบายสากลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (“**กรอบนโยบายสากล**”) เพื่อเป็นแนวทางสำหรับจัดทำนโยบายระดับประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุมเนื้อหาอย่างครบถ้วน ซึ่งสภาธุรกิจฯ ก็ได้ให้การสนับสนุนกรอบนโยบายสากลดังกล่าวอย่างเต็มที่ รายละเอียดของกรอบนโยบายสากลดังกล่าวปรากฏตามสำเนาที่แนบมาพร้อมนี้

กล่าวโดยสรุป กรอบนโยบายสากลดังกล่าวนำเสนอหลักการ 6 ข้อ เพื่อใช้เป็นแนวทางในการจัดทำนโยบายระดับประเทศในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ กล่าวคือ นโยบายในเรื่องดังกล่าวควรมีลักษณะดังนี้

1. สอดคล้องกับมาตรฐานซึ่งเป็นที่ยอมรับในระดับสากล
2. คำนึงถึงเรื่องความเสี่ยงเป็นหลัก มุ่งเน้นที่ผล และเป็นกลางทางเทคโนโลยี
3. อาศัยกลไกที่ขับเคลื่อนด้วยการตลาดหากสามารถกระทำได้
4. มีความยืดหยุ่นและสนับสนุนให้มีการพัฒนานวัตกรรม
5. ส่งเสริมให้มีการประสานความร่วมมือระหว่างภาครัฐและเอกชน และ
6. มุ่งปกป้องความเป็นส่วนตัว

2. <u>ความเห็นของภาคอุตสาหกรรม</u>

บีเอสเอได้เรียนเสนอความเห็นต่อร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับปี พ.ศ. 2558 ที่ออกโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์แห่งประเทศไทย (“**ร่าง พ.ร.บ. ปี 2558**”) รายละเอียดปรากฏตามสำเนาหนังสือแสดงความเห็นของบีเอสเอในภาคผนวกของหนังสือฉบับนี้

บีเอสเอและสภาธุรกิจฯ ขอแสดงความชื่นชมต่อกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมอีกครั้งหนึ่งมาในโอกาสนี้สำหรับความพยายามครั้งสำคัญที่ดำเนินการเพื่อให้แน่ใจว่าประเทศไทยมีความพร้อมที่จะระงับยับยั้งและจัดการกับภัยคุกคามไซเบอร์ เนื่องจากภัยคุกคามไซเบอร์มีความซับซ้อนและมีอันตรายขึ้นทุกวัน ความเสี่ยงที่เกิดจากนโยบายระดับประเทศที่กำหนดขึ้นอย่างไม่เพียงพอหรือไม่มีประสิทธิภาพในการรับมือกับภัยคุกคามไซเบอร์จึงอาจก่อให้เกิดความเสียหายอย่างใหญ่หลวงได้

ภัยคุกคามไซเบอร์โดยลักษณะแล้วเป็นเรื่องระดับโลก ดังนั้น การรับมือกับภัยคุกคามทางไซเบอร์จึงจำเป็นต้องดำเนินการในระดับโลกเช่นกัน บีเอสเอและสภาธุรกิจฯ ขอแสดงความชื่นชมต่อกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและรัฐบาลไทยที่เปิดรับฟังความคิดเห็นจากภาคเอกชนและผู้มีส่วนได้เสียอื่นๆ ในการจัดทำกฎหมายนี้ และขอสนับสนุนให้ยังคงมีการเปิดโอกาสให้มีการสื่อสารและหารือกับภาคเอกชนต่อไป ซึ่งรวมถึงบริษัทระดับโลก ด้วยเหตุนี้ ทางบีเอสเอและสภาธุรกิจฯ จึงขอเรียนเสนอให้กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ระบุให้ชัดเจนว่า บทบัญญัติที่กล่าวถึงการประสานความร่วมมือระหว่างภาครัฐและเอกชนนั้น (เช่น ตามมาตรา 5(4) และ มาตรา 7(5) เป็นต้น) เป็นการอนุญาตและส่งเสริมให้มีการประสานความร่วมมือกับเอกชนที่เป็นบริษัทที่ประกอบธุรกิจในหลายประเทศด้วย

บีเอสเอและสภาธุรกิจฯ ทราบและซาบซึ้งในความพยายามที่จะแก้ไขปัญหาของร่าง พ.ร.บ. ปี 2558 ตามที่ได้มีการเสนอความเห็นไว้ อย่างไรก็ดี ปัญหาส่วนใหญ่ของร่าง พ.ร.บ. ปี 2558 ก็ยังคงปรากฏอยู่ในร่าง พ.ร.บ. ปี 2561 นี้ บีเอสเอจึงขอเรียนเสนอความเห็นต่อไปนี้ด้วยเจตนาที่จะมีส่วนช่วยให้ร่างกฎหมายดังกล่าวบรรลุตามเจตนารมณ์อันดีที่จะกำหนดให้มี “การดำเนินการที่ทันท่วงทีและเป็นไปในทิศทางเดียวกัน” ต่อภัยคุกคามทางไซเบอร์ โดยไม่ก่อให้เกิดผลอันไม่พึงประสงค์

เอ. กรรมการในคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ในหนังสือเสนอความเห็นของบีเอสเอต่อร่าง พ.ร.บ. ปี 2558 บีเอสเอได้เน้นในประเด็นที่ว่า คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (“กปช.”) ควรประกอบด้วยกรรมการที่แต่งตั้งมาจากคณะกรรมการสิทธิมนุษยชนและสำนักงานผู้ตรวจการแผ่นดินด้วย เพื่อให้มีมุมมองที่รอบด้านขึ้นจากมุมมองของกรรมการของ กปช. ที่มาจากหน่วยงานด้านการรักษาความปลอดภัยและความมั่นคง ทั้งนี้ เพื่อให้แน่ใจว่า ในการจัดทำกลยุทธ์หรือแผนรับมือด้านความมั่นคงปลอดภัยไซเบอร์ กปช. จะพิจารณาประเด็นเรื่องความเป็นส่วนตัวและเสรีภาพของประชาชนในทุกมิติ

บีเอสเอและสภาธุรกิจฯ ทราบว่ามาตรา 6 แห่งร่าง พ.ร.บ. ปี 2561 ได้กำหนดให้กรรมการใน กปช. มาจากหลากหลายหน่วยงานมากขึ้น โดยมีผู้แทนจากหลายกระทรวง รวมถึงกระทรวงคมนาคม กระทรวงศึกษาธิการ และกระทรวงสาธารณสุข ซึ่งย่อมทำให้ได้มุมมองที่หลากหลายและสามารถจัดทำนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ผ่านการพิจารณาอย่างรอบด้านเพื่อเสนอต่อคณะรัฐมนตรีได้ อย่างไรก็ดี เนื่องจาก กปช. ไม่มีกรรมการที่จะดูแลรักษาผลประโยชน์ในเรื่องความเป็นส่วนตัวและเสรีภาพของประชาชน มุมมองของ กปช. จึงยังคงเน้นไปที่ประเด็นเรื่องการบังคับใช้กฎหมายและความมั่นคง โดยมีรัฐมนตรีว่าการกระทรวงกลาโหมเป็นรองประธาน กปช.

บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า คณะทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไม่ควรนำโดยรัฐมนตรีว่าการกระทรวงกลาโหมแต่เพียงผู้เดียว แต่ควรให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมมีส่วนร่วมในการนำคณะทำงานดังกล่าวด้วย เนื่องจากภัยคุกคามทางไซเบอร์อาจส่งผลกระทบต่อผลประโยชน์ทางด้านเศรษฐกิจทั้งในระดับชาติและระดับนานาชาติได้ในวงกว้าง กปช. จึงควรมีกรรมการที่จะดูแลรักษาผลประโยชน์ของประชาชนอยู่ด้วย

บี. การมีอำนาจอย่างกว้างขวางของ กปช.

ตามมาตรา 14 แห่งร่าง พ.ร.บ. ปี 2561 กปช. มีอำนาจหน้าที่เป็นศูนย์กลางในการประสานงานระหว่างหน่วยงานเพื่อรับมือกับภัยคุกคามไซเบอร์และสถานการณ์ด้านภัยคุกคามไซเบอร์ บีเอสเอและสภาธุรกิจฯ ยังคงเห็นด้วยในเรื่องนี้ การกำหนดให้มีหน่วยงานระดับประเทศเพียงหน่วยงานเดียวทำหน้าที่เป็นหน่วยงานหลักที่มีความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะทำให้เกิดความชัดเจน มีความสอดคล้อง และเป็นไปในทิศทางเดียวกันในการเตรียมความพร้อมของรัฐบาลในการรับมือกับภัยคุกคามและปัญหาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ในฐานะที่ กปช. เป็นศูนย์กลางในการประสานงานดังกล่าว กปช. จึงมีอำนาจอย่างกว้างขวางในการจัดการกับภัยคุกคามไซเบอร์ที่กฎหมายนี้กำหนดให้ต้องมีการดำเนินการอย่างหนึ่งอย่างใด ตัวอย่างเช่น ตามมาตรา 36 และมาตรา 37 แห่งร่าง พ.ร.บ. ปี 2561 กปช. มีอำนาจสั่งการให้หน่วยงานเอกชน[3]ดำเนินการอย่างหนึ่งอย่างใดเมื่อมีเหตุฉุกเฉินหรือภยันตรายอันเนื่องมาจากภัยคุกคามทางไซเบอร์ บีเอสเอและสภาธุรกิจฯ ตระหนักว่าได้มีความพยายามที่จะระบุให้ชัดเจนขึ้นว่า อำนาจเหล่านี้จะมีขึ้นเฉพาะในกรณีที่ “การให้บริการด้านระบบเครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม การให้บริการดาวเทียม ระบบกิจการสาธารณูปโภคพื้นฐาน ระบบกิจการสาธารณะสำคัญ” ได้รับผลกระทบเท่านั้น ซึ่งสอดคล้องกับความเห็นที่บีเอสเอได้ให้ไว้สำหรับร่าง พ.ร.บ. ปี 2558 อย่างไรก็ดี หลักเกณฑ์และกรณีที่ กปช. อาจใช้อำนาจตามมาตราเหล่านี้ได้ก็ยังไม่ได้มีการบัญญัติไว้อย่างชัดเจน

- **อำนาจของ กปช. ควรจำกัดให้มีเฉพาะในกรณีที่ “โครงสร้างพื้นฐานที่สำคัญ” ได้รับผลกระทบ** หลายประเทศได้นำเรื่อง “โครงสร้างพื้นฐานที่สำคัญ” มาใช้ในกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งเป็นกรณีที่ยอมรับได้ว่าหน่วยงานผู้บังคับใช้กฎหมายจะมีอำนาจอย่างกว้างขวาง ดังเช่นที่ปรากฏในร่าง พ.ร.บ. ปี 2561 ดังนั้น เพื่อให้สอดคล้องกับกฎหมายที่ใช้ในทั่วโลก บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอคำจำกัดความดังนี้
  - โครงสร้างพื้นฐานที่สำคัญ หมายความว่า **“ทรัพย์สิน บริการ และระบบ ไม่ว่าที่จับต้องได้หรือเสมือนจริง ที่หากถูกทำลาย ถูกทำให้เสียหาย หรือไม่สามารถใช้การได้เป็นระยะเวลานานแล้ว จะส่งผลกระทบในวงกว้างต่อความมั่นคงของชาติ สาธารณสุข ความปลอดภัยของประชาชน ความมั่นคงด้านเศรษฐกิจของชาติ หรือการปฏิบัติงานหลักของหน่วยงานในระดับท้องถิ่นหรือระดับชาติ”**

  ในการกำหนดว่าโครงสร้างใดเป็นโครงสร้างพื้นฐานที่สำคัญ บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า กปช. ควรพิจารณาจากความสำคัญ ความจำเป็น และความเสี่ยงที่เกี่ยวข้อง

[3] “หน่วยงานเอกชน” เป็นคำที่เพิ่มคำจำกัดความเข้ามาใหม่ในมาตรา 3 ซึ่งหมายความว่า “หน่วยงานที่จัดตั้งขึ้นจากการรวมตัวของบุคคล หรือคณะบุคคลเข้าด้วยกัน ไม่ว่าจะเป็นการดำเนินงานที่แสวงหากำไร หรือที่ไม่แสวงหากำไร ทั้งนี้ ไม่ว่าจะจดทะเบียนเป็นนิติบุคคลหรือไม่ก็ตาม”

- **การให้อำนาจที่กว้างขวางตามมาตรา 36 และมาตรา 37 ควรจำกัดเฉพาะในกรณี "เหตุภัยคุกคามทางไซเบอร์ที่สำคัญ"** ในเรื่องนี้ควรต้องให้คำจำกัดความทั้งคำว่า "เหตุภัยคุกคามทางไซเบอร์" และ "เหตุภัยคุกคามทางไซเบอร์ที่สำคัญ" ดังนั้น เพื่อให้สอดคล้องกับกรอบนโยบายสากล บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอคำจำกัดความดังนี้
  - "เหตุภัยคุกคามทางไซเบอร์" หมายความว่า **"เหตุการณ์ที่ระบุได้ ไม่ว่าจะเกิดขึ้นเพียงครั้งเดียวหรือหลายครั้ง ต่อระบบ บริการ หรือเครือข่าย ซึ่งแสดงให้เห็นได้ว่าอาจมีการกระทำอันเป็นการฝ่าฝืนนโยบายด้านการรักษาความมั่นคงปลอดภัยของสารสนเทศ หรือมีความบกพร่องในการรักษาความมั่นคงปลอดภัย หรือสถานการณ์ที่อาจมีความเกี่ยวข้องกับความปลอดภัยของระบบ บริการ หรือเครือข่าย ที่เกิดขึ้นมาก่อนหน้านี้แต่ไม่ทราบมาก่อน"**
  - "เหตุภัยคุกคามทางไซเบอร์ที่สำคัญ" หมายความว่า **"เหตุภัยคุกคามทางไซเบอร์ที่ทำให้ (1) มีการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือมีการถูกปฏิเสธไม่ให้เข้าถึงข้อมูล หรือมีการทำลาย ลบ ปรับเปลี่ยน หรือระงับข้อมูลที่จำเป็นต่อการทำงานของโครงสร้างพื้นฐานที่สำคัญ หรือ (2) การควบคุมการปฏิบัติการหรือการควบคุมทางเทคนิคที่จำเป็นต่อความปลอดภัยหรือการทำงานของโครงสร้างพื้นฐานที่สำคัญถูกโจมตี**

ซี. การรายงานเหตุภัยคุกคามทางไซเบอร์

บีเอสเอและสภาธุรกิจฯ มีความกังวลว่า บทบัญญัติที่กำหนดให้หน่วยงานเอกชนรายงานไปยังเลขาธิการกรณีเกิดหรือคาดว่าจะเกิดเหตุภัยคุกคามทางไซเบอร์ตามมาตรา 35 นั้นอาจจะกว้างเกินไป การกำหนดเงื่อนไขของการรายงานที่กว้างเกินไปนั้นอาจกลับทำให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์กระทำได้ยากขึ้น เนื่องจากจะทำให้บริษัทต่างๆ รายงานเหตุที่เกิดขึ้นกับระบบของตนบ่อยครั้งเกินไป อันทำให้ความใส่ใจต่อการรายงานลดหายไป อีกทั้งทำให้มีค่าใช้จ่ายสูงขึ้น การปฏิบัติงานถูกรบกวน และยากที่จะระบุว่าเหตุภัยคุกคามใดที่มีความสำคัญที่สุดและควรดำเนินการอย่างไร ดังนั้น บีเอสเอและสภาธุรกิจฯ จึงขอเรียนเสนอให้การรายงานต้องกระทำเฉพาะในกรณีของ "เหตุภัยคุกคามทางไซเบอร์ที่สำคัญ" ที่ส่งผลกระทบต่อ "โครงสร้างพื้นฐานที่สำคัญ" เท่านั้น ตามที่เรียนไว้ข้างต้น

ดี. อำนาจในการสอดส่องดูแล

บีเอสเอและสภาธุรกิจฯ ทราบว่า ร่าง พ.ร.บ. ปี 2561 นั้นได้มีการแก้ไขปรับเปลี่ยนตามที่บีเอสเอได้เรียนเสนอไว้ในครั้งก่อนเกี่ยวกับอำนาจหน้าที่ของเลขาธิการในการสอดส่องดูแลตามร่าง พ.ร.บ. ปี 2558 แล้ว กล่าวคือ มาตรา 47 แห่งร่าง พ.ร.บ. ปี 2561 กำหนดว่า เลขาธิการอาจเข้าถึงข้อมูลการติดต่อสื่อสารของหน่วยงานเอกชนได้ต่อเมื่อมีคำสั่งศาลอนุญาตให้ปฏิบัติการดังกล่าว เว้นแต่ "ในกรณีจำเป็นเร่งด่วนหากไม่ดำเนินการในทันทีจะเกิดความเสียหายอย่างร้ายแรง" ซึ่งกฎหมายได้อนุญาตให้เลขาธิการเข้าถึงข้อมูลการติดต่อสื่อสารไปก่อน แล้วจึงรายงานให้ศาลทราบโดยเร็ว บีเอสเอและสภาธุรกิจฯ ขอเรียนว่า ข้อยกเว้นที่บัญญัติไว้อย่างกว้างดังกล่าวนี้อาจก่อให้เกิดความไม่ชัดเจนในทางปฏิบัติ ซึ่งอาจทำให้ความเชื่อมั่นของผู้บริโภคที่ว่าโดยทั่วไปแล้วบริษัทต่างๆ จะสามารถรับรองได้ว่าข้อมูลส่วนบุคคลหรือข้อมูลลับของ

ผู้ใช้บริการจะได้รับการป้องกันไม่ให้มีการเข้าถึงโดยไม่ได้รับอนุญาตนั้นต้องถูกลดทอนลงไป ในเรื่องนี้ บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอแนวทางแก้ปัญหาดังนี้

- **ควรกำหนดให้คำสั่งศาลมีผลเพียงช่วงระยะเวลาหนึ่ง** บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า คำสั่งศาลไม่ควรมีผลบังคับโดยไม่จำกัดระยะเวลา เนื่องจากอาจก่อให้เกิดความไม่ชัดเจนต่อหน่วยงานเอกชน
- **ข้อยกเว้นของการขอคำสั่งศาลควรใช้ถ้อยคำที่ชัดเจน** บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า กรณี “จำเป็นเร่งด่วน” ที่เป็นข้อยกเว้นดังกล่าวนั้นควรระบุให้ชัดเจนว่าต้องเป็นกรณีที่อาจก่อให้เกิดความเสียหายต่อความมั่นคงของชาติเท่านั้น
- **ควรกำหนดให้มีหน่วยงานอิสระควบคุมดูแลการใช้อำนาจของ กปช. ตามมาตรา 47** บีเอสเอและสภาธุรกิจฯ ขอเรียนย้ำว่า หน่วยงานอิสระ เช่น คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เสนอให้มีการแต่งตั้งตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ควรมีอำนาจในการตรวจสอบดูแลการใช้อำนาจของ กปช. ตามมาตรา 47 แห่งร่าง พ.ร.บ. ปี 2561 เพื่อให้แน่ใจว่ามีการถ่วงดุลระหว่างผลประโยชน์ของเอกชนกับความจำเป็นในการใช้อำนาจสอดส่องดูแล

อี. ความรับผิดทางอาญา

มาตรา 53 ถึงมาตรา 56 แห่งร่าง พ.ร.บ. ปี 2561 ได้กำหนดโทษทางอาญาสำหรับการกระทำที่ฝ่าฝืนร่าง พ.ร.บ. ปี 2561 ในเรื่องนี้ บีเอสเอและสภาธุรกิจฯ เห็นว่า การดำเนินคดีอาญาควรจำกัดเฉพาะในกรณีที่ผู้กระทำผิดก่อกวน ทำให้เสียหาย หรือก่อให้เกิดปัญหาต่อโลกไซเบอร์ด้วยเจตนาทุจริตเท่านั้น

บีเอสเอและสภาธุรกิจฯ เห็นว่า การกำหนดโทษทางอาญาต่อหน่วยงานเอกชนที่ไม่ปฏิบัติตามคำขอของ กปช. ตามมาตรา 47 นั้นเป็นบทลงโทษที่รุนแรงเกินควร อันอาจทำให้บริษัทต่างชาติระงับแผนที่จะเข้ามาประกอบธุรกิจในประเทศไทยหากมีความเสี่ยงว่าบุคลากรของตนจะต้องมีความรับผิดทางอาญาสำหรับการกระทำความผิดโดยไม่ได้จงใจหรือการกระทำความผิดเพียงเล็กน้อย

เอฟ. แง่มุมอื่น ๆ ของนโยบายด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ

นอกจากนี้ บีเอสเอและสภาธุรกิจฯ ขอเรียนเสนอว่า นโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยควรครอบคลุมประเด็นที่สำคัญอื่นๆ ด้วย เช่น การปฏิบัติตามแนวทางในการจัดซื้อเทคโนโลยีและซอฟต์แวร์ของภาครัฐ การให้การสนับสนุนจากรัฐบาลอย่างเต็มที่ในด้านการวิจัยและพัฒนาเทคโนโลยีสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ โครงการให้ความรู้เพื่อเพิ่มความตระหนักรู้ การฝึกอบรม และการจัดทำนโยบายต่างประเทศให้ครอบคลุมถึงเรื่องการประสานความร่วมมือในการรักษาความมั่นคงปลอดภัยไซเบอร์ บีเอสเอและสภาธุรกิจฯ ขอสนับสนุนให้รัฐบาลไทยพิจารณาเพิ่มเติมประเด็นที่สำคัญเหล่านี้ไว้ในร่าง พ.ร.บ. ปี 2561 และขอเรียนเสนอกรอบนโยบายสากลและแบ่งปันประสบการณ์ในการดำเนินการในระดับสากลของเราในด้านนี้เพื่อเป็นแนวทางในการจัดทำนโยบายที่เกี่ยวข้องต่อไป

3. บทสรุปและการดำเนินการขั้นต่อไป

บีเอสเอและสภาธุรกิจฯ ขอแสดงความชื่นชมรัฐบาลไทยอีกครั้งสำหรับความพยายามในการปกป้องโครงสร้างพื้นฐานจากภัยคุกคามทางไซเบอร์และการก่ออาชญากรรมทางไซเบอร์ อย่างไรก็ดี บีเอสเอและสภาธุรกิจฯ ใคร่ขอความอนุเคราะห์ให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมพิจารณาประเด็นที่ได้เรียนเสนอไว้ข้างต้น เพื่อที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมจะสามารถจัดทำนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ ซึ่งคำนึงถึงเรื่องความเสี่ยงเป็นหลักและสอดคล้องกับแนวปฏิบัติในระดับสากล อันจะช่วยเสริมสร้างความเชื่อมั่นระหว่างภาครัฐและเอกชน และยกระดับความมั่นคงปลอดภัยของข้อมูลและโครงสร้างพื้นฐาน

บีเอสเอและสภาธุรกิจฯ ยินดีจะหารือกับท่านในเรื่องนี้เพิ่มเติมได้ทุกเมื่อ หากท่านมีข้อสงสัยหรือความเห็นประการใด กรุณาติดต่อโดยตรงไปที่ afeldman@usasean.org หรือที่หมายเลข 202-375-4393 หรือที่ jaredr@bsa.org หรือที่หมายเลข +65 6292 9609 หรือติดต่อ**นางสาววารุณี รัชตพัฒนากุล ผู้จัดการประจำประเทศไทยแห่งบีเอสเอ ได้ที่** varuneer@bsa.org **หรือที่หมายเลข +668-1840-0591 หรือนางสาวเอลล่า ดวงแก้ว ผู้จัดการประจำประเทศไทยแห่งสภาธุรกิจสหรัฐอเมริกา-อาเซียน ที่** eduangkaew@usasean.org **หรือที่หมายเลข 202-440-3642** บีเอสเอและสภาธุรกิจฯ ขอขอบพระคุณที่ท่านสละเวลาพิจารณาในเรื่องนี้

ขอแสดงความนับถือ

(ลายมือชื่อ)

อเล็กซานเดอร์ ซี. เฟลด์แมน
ประธานและประธานเจ้าหน้าที่บริหาร
สภาธุรกิจสหรัฐอเมริกา-อาเซียน

(ลายมือชื่อ)

เจเร็ด แร้กแลนด์
ผู้อำนวยการอาวุโส ฝ่ายนโยบาย ภูมิภาคเอเชียแปซิฟิก
บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์

สำเนาถึง
1. ดร.พิเชฐ ดุรงคเวโรจน์ รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
2. นางสุรางคณา วายุภาพ ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

Annex D:
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.

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

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

(กระดาษหัวจดหมายของบีเอสเอ)

วันที่ 6 พฤษภาคม 2558

เป็นความลับและห้ามเผยแพร่

เลขาธิการคณะกรรมการกฤษฎีกา
สำนักงานคณะกรรมการกฤษฎีกา
ถนนพระอาทิตย์ เขตพระนคร
กรุงเทพมหานคร 10200

เรื่อง ความเห็นของบีเอสเอเกี่ยวกับร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

เรียนท่านเลขาธิการคณะกรรมการกฤษฎีกา

บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์ (บีเอสเอ)[1] ใคร่ขอขอบพระคุณที่ท่านได้เปิดโอกาสให้มีการเสนอความเห็นต่อคณะกรรมการกฤษฎีกาเกี่ยวกับร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (“**ร่าง พ.ร.บ.**”) และขอแสดงความชื่นชมในความพยายามครั้งสำคัญที่แสดงถึงความมีวิสัยทัศน์ของรัฐบาลไทยในครั้งนี้ที่ดำเนินการให้แน่ใจว่าประเทศจะมีความพร้อมในการระงับยับยั้งและจัดการกับภัยคุกคามทางไซเบอร์ อนึ่ง กลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพต้องจัดทำขึ้นบนพื้นฐานกฎหมายที่ชัดเจน เพื่อเอื้อให้มีการประสานความร่วมมือระหว่างหน่วยงานผู้บังคับใช้กฎหมาย ภาครัฐ และภาคเอกชน ซึ่งการประสานความร่วมมือดังกล่าวย่อมต้องอาศัยความไว้เนื้อเชื่อใจกัน ซึ่งจะเกิดขึ้นได้ก็ต่อเมื่อมีมาตรการป้องกันอย่างเพียงพอและภาคเอกชนจะได้รับประโยชน์อย่างเหมาะสม ตัวอย่างเช่น ข้อกำหนดเกี่ยวกับการรักษาความปลอดภัยต้องมีความสมดุลอย่างเหมาะสมระหว่างความจำเป็นในการคุ้มครองความเป็นส่วนตัวกับเสรีภาพของประชาชน เมื่อคำนึงถึงหลักการเหล่านี้เป็นสำคัญ บีเอสเอมีความกังวลว่า บทบัญญัติของร่าง พ.ร.บ. นี้ที่ให้อำนาจในการสอดส่องดูแล

[1] บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์ (www.bsa.org) เป็นหน่วยงานชั้นนำที่ทำหน้าที่เป็นผู้แทนในการรักษาสิทธิประโยชน์ของอุตสาหกรรมซอฟต์แวร์ในทั่วโลกต่อรัฐบาลและในตลาดระดับสากล สมาชิกของบีเอสเอเป็นบริษัทต่างๆ ที่สร้างสรรค์นวัตกรรมที่ทันสมัยที่สุดของโลก ซึ่งนำเสนอโซลูชั่นซอฟต์แวร์ที่ผลักดันให้เศรษฐกิจเติบโตและปรับปรุงคุณภาพชีวิตในยุคปัจจุบัน บีเอสเอมีสำนักงานใหญ่ตั้งอยู่ที่กรุงวอชิงตัน ดี.ซี. และมีการดำเนินการในกว่า 60 ประเทศทั่วโลก โดยเป็นผู้ริเริ่มโครงการส่งเสริมการปฏิบัติตามกฎหมายเพื่อรณรงค์การใช้ซอฟต์แวร์ที่ถูกกฎหมาย และสนับสนุนนโยบายสาธารณะที่ส่งเสริมให้มีการสร้างสรรค์นวัตกรรมเทคโนโลยีและขับเคลื่อนให้เศรษฐกิจดิจิทัลเติบโต สมาชิกของบีเอสเอรวมถึงบริษัท 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 และ Trend Micro

(ตามมาตรา 35) อาจก่อให้เกิดผลอันไม่พึงประสงค์ได้ ซึ่งรวมถึงการที่ความเชื่อมั่นของผู้บริโภคต่อระบบเทคโนโลยีสารสนเทศของประเทศไทยอาจลดทอนลง ด้วยเหตุนี้ บีเอสเอจึงขอเรียนเสนอความเห็นต่อไปนี้ด้วยเจตนาที่จะมีส่วนช่วยให้ร่างกฎหมายดังกล่าวบรรลุตามเจตนารมณ์อันดีในการกำหนดให้มี “การดำเนินการที่ทันท่วงทีและเป็นไปในทิศทางเดียวกัน” ต่อภัยคุกคามทางไซเบอร์

มาตรา 6 กรรมการในคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

กรรมการส่วนใหญ่ในคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (“กปช.”) มาจากหน่วยงานของรัฐที่เกี่ยวข้องกับการรักษาความปลอดภัยและความมั่นคง เช่น กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กระทรวงกลาโหม และกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ บีเอสเอขอเรียนเสนอว่า เพื่อให้ กปช. มีทัศนคติที่เป็นกลางและเพื่อให้แน่ใจว่าจะมีการพิจารณาในเรื่องความเป็นส่วนตัวของบุคคลและเสรีภาพของประชาชน กปช. ควรประกอบด้วยกรรมการที่แต่งตั้งจากคณะกรรมการสิทธิมนุษยชนและสำนักงานผู้ตรวจการแผ่นดินด้วย เนื่องจากการที่คณะกรรมการประกอบด้วยกรรมการที่มีความรู้และประสบการณ์ที่หลากหลายนั้นจะช่วยป้องกันไม่ให้สิทธิของบุคคลถูกกระทบเกินควรได้

มาตรา 7 ถึงมาตรา 34 ของร่าง พ.ร.บ. ให้อำนาจแก่ กปช. อย่างกว้างขวาง

บีเอสเอเห็นด้วยกับการที่ร่างกฎหมายนี้กำหนดให้ กปช. ทำหน้าที่เป็นศูนย์กลางที่อำนวยความสะดวกในการประสานความร่วมมือระหว่างหน่วยงานของรัฐทั้งหมดที่เกี่ยวข้องในกรณีที่เกิดเหตุภัยคุกคามทางไซเบอร์ ทั้งนี้ ตามมาตรา 7 กปช. มีอำนาจหน้าที่ต่างๆ ซึ่งรวมถึงการ “จัดทำแผนปฏิบัติการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” และมาตรา 27 และมาตรา 28 ได้กำหนดให้สำนักงาน กปช. จัดทำแนวทาง มาตรการ แผนปฏิบัติการ หรือโครงการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องและเป็นตามนโยบายและแผนดังกล่าว ดังนั้น ร่าง พ.ร.บ. นี้จึงควรต้องกำหนดไว้อย่างชัดเจนว่าเหตุการณ์ลักษณะใดที่ถือเป็นภัยคุกคามทางไซเบอร์ที่กฎหมายนี้กำหนดให้ต้องมีการดำเนินการอย่างหนึ่งอย่างใด เช่น เมื่อเกิดภัยคุกคามทางไซเบอร์ มาตรา 33 ได้ให้อำนาจแก่ กปช. ในการสั่งการให้หน่วยงานของรัฐทั้งหมดที่เกี่ยวข้องดำเนินการใดก็ตามอันจะมีผลเป็นการควบคุมหรือบรรเทาความเสียหายที่เกิดขึ้น และมาตรา 34 ได้ขยายอำนาจของ กปช. ให้สามารถสั่งการให้หน่วยงานภาคเอกชนกระทำการหรืองดเว้นกระทำการอย่างใดอย่างหนึ่ง และให้รายงานผลการปฏิบัติการต่อ กปช. หากเป็นกรณีที่ภัยคุกคามทางไซเบอร์อาจกระทบต่อความมั่นคงทางการเงินและการพาณิชย์ หรือความมั่นคงของประเทศ

จะเห็นได้ว่า บทบัญญัติในมาตราข้างต้นได้ให้อำนาจแก่ กปช. ไว้อย่างกว้างขวาง แต่กฎหมายฉบับนี้กลับไม่ได้กำหนดคำจำกัดความของ “ภัยคุกคามทางไซเบอร์” ไว้อย่างชัดเจน อีกทั้งไม่ได้กำหนดหลักเกณฑ์ในการพิจารณาว่าความเสี่ยงที่เกิดขึ้นนั้นถึงขนาดที่ กปช. พึงต้องดำเนินการอย่างหนึ่งอย่างใดหรือไม่ นอกจากนี้ ร่าง พ.ร.บ. ดังกล่าวไม่ได้กำหนดแนวทางในการพิจารณาว่าเหตุการณ์ใดที่อาจกระทบต่อ “ความมั่นคงทางการเงินและการพาณิชย์ หรือความมั่นคงของประเทศ” ซึ่งมีความรุนแรงถึงขนาดที่ กปช. มีอำนาจสั่งการต่อหน่วยงานภาคเอกชนได้ ร่าง พ.ร.บ. ดังกล่าวจึงควรกำหนดคำจำกัดความของคำที่มี

ความหมายกว้างเหล่านี้ให้ชัดเจน เพื่อที่บุคคลทุกคนที่ได้รับผลกระทบจะได้เข้าใจสถานะของตน และเพื่อที่จะได้ไม่มีความกำกวมต่อไป

มาตรา 35 (1) และ (2) รัฐบาลเรียกขอข้อมูลหรือให้ดำเนินการอย่างใดอย่างหนึ่ง

มาตรา 35 (1) แห่งร่าง พ.ร.บ. นี้ให้อำนาจแก่พนักงานเจ้าหน้าที่ที่ได้รับมอบหมายเป็นหนังสือจากเลขาธิการสำนักงาน กปช. ในการมีหนังสือสอบถามหรือเรียกให้หน่วยงานของรัฐ หรือบุคคลใดๆ มาให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งบัญชี เอกสาร หรือหลักฐานใดๆ มาเพื่อตรวจสอบหรือให้ข้อมูลเพื่อประโยชน์ในการปฏิบัติตามพระราชบัญญัตินี้

มาตรา 35 (2) ให้อำนาจแก่พนักงานเจ้าหน้าที่ในการมีหนังสือขอให้หน่วยงานราชการ หรือหน่วยงานเอกชนดำเนินการเพื่อประโยชน์แห่งการปฏิบัติหน้าที่ของ กปช.

บีเอสเอขอเรียนเสนอว่า เพื่อให้แน่ใจว่าจะไม่มีการใช้อำนาจที่กว้างขวางเหล่านี้ในทางมิชอบ กฎหมายฉบับนี้ควรต้องมีหลักเกณฑ์ที่ชัดเจนที่กำหนดประเภทและขอบเขตของข้อมูลที่พนักงานเจ้าหน้าที่สามารถเรียกได้ และระบุกรณีที่สำนักงาน กปช. สามารถเรียกให้หน่วยงานเอกชนดำเนินการอย่างใดอย่างหนึ่งได้ อีกทั้งควรกำหนดว่าบุคคลใดในสำนักงาน กปช. ที่อาจเรียกขอข้อมูลได้ และกำหนดหลักเกณฑ์ในการจัดการข้อมูลดังกล่าวเพื่อให้แน่ใจว่าข้อมูลที่ กปช. ได้รับไปนั้นจะได้รับความคุ้มครองอย่างเหมาะสม นอกจากนี้ การใช้อำนาจเหล่านี้ควรจำกัดอยู่เฉพาะในกรณีที่เชื่อได้ว่าจะมีภัยคุกคามทางไซเบอร์อย่างใดอย่างหนึ่งเกิดขึ้นเท่านั้น

มาตรา 35 (3) อำนาจในการสอดส่องดูแล

มาตรา 35 (3) ให้อำนาจแก่ กปช. ในการเข้าถึงข้อมูลการติดต่อสื่อสารทั้งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสารสื่ออิเล็กทรอนิกส์หรือสื่อทางเทคโนโลยีสารสนเทศใด เพื่อประโยชน์ในการปฏิบัติการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ เนื่องจากอำนาจหน้าที่อย่างกว้างขวางของ กปช. ในการสอดส่องดูแลดังกล่าวนี้ทำให้ กปช. สามารถเข้าถึงเครือข่ายสื่อสารได้อย่างไม่จำกัด บีเอสเอจึงมีความกังวลเป็นอย่างยิ่งในเรื่องความเป็นส่วนตัว บีเอสเอเห็นว่ามาตรา 35 (3) ดังกล่าวไม่มีการถ่วงดุลที่จำเป็นต้องมีระหว่างความมั่นคงของประเทศกับความเป็นส่วนตัวของข้อมูล เนื่องจากกฎหมายดังกล่าวกำหนดให้รัฐบาลมีดุลพินิจในการใช้อำนาจได้โดยที่ไม่ต้องมีการตรวจสอบความชอบด้วยกฎหมายโดยศาล เช่น ไม่มีบทบัญญัติใดที่กำหนดให้ต้องขอหมายศาลก่อนเข้าถึงการติดต่อสื่อสารส่วนบุคคล กฎหมายนี้เพียงแค่กำหนดว่า พนักงานเจ้าหน้าที่อาจมีอำนาจเข้าถึงข้อมูลได้หากได้รับมอบหมายเป็นหนังสือจากเลขาธิการสำนักงาน กปช.

หากพิจารณาในแง่พาณิชย์ มาตรา 35 (3) ของร่าง พ.ร.บ. นี้อาจขัดขวางการลงทุนด้านเทคโนโลยีสารสนเทศในประเทศไทยได้ เนื่องจากธุรกิจใดก็ตามที่มีระบบเทคโนโลยีสารสนเทศ ตั้งแต่ธนาคารและสถาบันการเงินไปจนถึงธุรกิจค้าปลีก อาจต้องอยู่ภายใต้บังคับของมาตรา 35 (3) ดังกล่าว โดยที่ผู้ให้บริการไม่อาจรับรองแก่ลูกค้าของตนได้ว่าข้อมูลส่วนบุคคล ความลับทางการค้า หรือประวัติการซื้อหุ้นของลูกค้าจะถูกเก็บไว้เป็นความลับ ซึ่งอาจทำให้ธุรกิจด้านเทคโนโลยีสารสนเทศระงับการใช้หรือการ

ลงทุนด้านระบบเทคโนโลยีสารสนเทศในประเทศไทย อันเป็นทิศทางที่ตรงกันข้ามกับความพยายามในการผลักดันให้ประเทศไทยเป็นศูนย์กลางด้านเทคโนโลยีสารสนเทศของกลุ่มประเทศอาเซียน

การที่มาตรา 35 (3) ไม่มีมาตรการตรวจสอบและถ่วงดุลอำนาจดังกล่าวนั้นขัดกับมาตรการรักษาความเป็นส่วนตัวของข้อมูลตามกฎหมายที่ใช้บังคับอยู่ในประเทศไทยและตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เช่น ตามมาตรา 25 แห่งพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 (“**พ.ร.บ. การสอบสวนคดีพิเศษ**”) มีการให้อำนาจในการเข้าถึงข้อมูลส่วนบุคคลในทำนองเดียวกันหากมีเหตุอันควรเชื่อได้ว่ามีสื่อใดที่ถูกใช้เพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษ ประการสำคัญ มาตรา 25 แห่ง พ.ร.บ. การสอบสวนคดีพิเศษดังกล่าวกำหนดให้พนักงานสอบสวนคดีพิเศษต้องยื่นคำขอฝ่ายเดียวต่อศาลอาญาเพื่อมีคำสั่งอนุญาตให้พนักงานสอบสวนคดีพิเศษได้มาซึ่งข้อมูลข่าวสารดังกล่าวได้ นอกจากนี้ ศาลอาจสั่งอนุญาตดังกล่าวได้คราวละไม่เกิน 90 วันเท่านั้น ในทำนองเดียวกัน ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ก็ได้กำหนดให้พนักงานเจ้าหน้าที่ผู้บังคับใช้กฎหมายต้องได้รับคำสั่งศาลก่อนจึงจะเรียกให้ผู้ให้บริการเปิดเผยเนื้อหาของการติดต่อสื่อสารของผู้ใช้บริการได้

จากบทบัญญัติข้างต้น มาตรา 35 (3) ของร่าง พ.ร.บ. นี้จึงควรกำหนดให้พนักงานเจ้าหน้าที่ต้องได้รับคำสั่งศาลก่อนจึงจะสามารถเข้าถึงข้อมูลส่วนบุคคลได้เช่นกัน อีกทั้งควรกำหนดให้คำสั่งอนุญาตดังกล่าวมีผลบังคับเพียงช่วงระยะเวลาหนึ่งๆ เท่านั้น นอกจากนี้ ควรกำหนดให้พนักงานเจ้าหน้าที่สามารถใช้อำนาจตามมาตรา 35 (3) ได้เฉพาะในกรณีที่อาจเกิดความเสียหายต่อความมั่นคงของชาติเท่านั้น สุดท้ายนี้ บีเอสเอขอเรียนเสนอให้มีหน่วยงานอิสระ เช่น คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลที่เสนอให้มีการแต่งตั้งตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล มีอำนาจตรวจสอบการใช้อำนาจของ กปช. ตามมาตรา 35 (3) เพื่อให้แน่ใจว่ามีการถ่วงดุลอย่างเพียงพอระหว่างความเป็นส่วนตัวกับความจำเป็นของการใช้อำนาจในการสอดส่องดูแล

<u>บทสรุป</u>

บีเอสเอเห็นถึงความพยายามของรัฐบาลไทยในการปกป้องโครงสร้างพื้นฐานจากภัยคุกคามทางไซเบอร์และการก่ออาชญากรรมทางไซเบอร์ อย่างไรก็ดี พนักงานเจ้าหน้าที่ตามกฎหมายนี้ควรกระทำการอย่างโปร่งใสและไม่ล่วงละเมิดความเป็นส่วนตัวของผู้ใช้ ไม่เช่นนั้นอาจก่อให้เกิดผลเสียต่อแผนด้านดิจิทัลเพื่อเศรษฐกิจได้ นอกจากนี้ ควรเน้นย้ำในเรื่องการให้ความร่วมมือของเอกชนในการรายงานรัฐบาลเมื่อมีการกระทำที่เป็นภัยต่อความปลอดภัยของระบบเพื่อป้องกันภัยคุกคามทางไซเบอร์เพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของชาติ การที่กฎหมายนี้ให้อำนาจแก่ กปช. และ/หรือพนักงานเจ้าหน้าที่ตามกฎหมายนี้อย่างกว้างขวางอาจนำไปสู่การกระทำที่เป็นการหลอกลวง ความไม่ไว้เนื้อเชื่อใจ และทำให้เอกชนให้ความร่วมมือน้อยลงในการรายงานเมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ ในขณะที่มาตรา 5(4) มาตรา 7(8) มาตรา 17(2) มาตรา 17(3) และ มาตรา 18(3) พยายามส่งเสริมให้มีการประสานความร่วมมือระหว่างภาครัฐและเอกชนในการป้องกันภัยคุกคามทางไซเบอร์ แต่ในความเป็นจริงแล้วภาคเอกชนอาจเกิดความลังเลที่จะให้ข้อมูลกับรัฐบาลด้วยเกรงว่ารัฐบาลจะเรียกขอข้อมูลที่ไม่เกี่ยวข้องหรือเข้ายุ่งเกี่ยวกับการ

ติดต่อสื่อสารส่วนบุคคลทางสื่อเทคโนโลยีสารสนเทศ ด้วยเหตุนี้ บีเอสเอจึงใคร่ขอความกรุณาให้คณะกรรมการกฤษฎีกาพิจารณาความเห็นข้างต้นอย่างถี่ถ้วนเพื่อให้เกิดความโปร่งใสและเพื่อสร้างความไว้เนื้อเชื่อใจระหว่างภาครัฐและเอกชน โดยที่ยังสามารถรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้ในขณะเดียวกัน

บีเอสเอมีความยินดีที่จะหารือในเรื่องนี้กับท่านได้ทุกเมื่อ หากท่านมีข้อสงสัยหรือความเห็นใดๆ กรุณาติดต่อ**นางสาววารุณี รัชตพัฒนากุล ผู้แทนในประเทศไทยของบีเอสเอ ที่ varuneer@bas.org หรือที่หมายเลข +668-1840-0591**

ขอขอบพระคุณที่ท่านสละเวลาพิจารณาในเรื่องนี้

ขอแสดงความนับถือ

(ลายมือชื่อ)

บุน โพ มก
ผู้อำนวยการฝ่ายนโยบาย ภูมิภาคเอเชีย-แปซิฟิก
บีเอสเอ | กลุ่มพันธมิตรซอฟต์แวร์

สำเนาถึง

1. ฯพณฯ รองนายกรัฐมนตรี ดร. วิษณุ เครืองาม
2. นางสุรางคณา วายุภาพ ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)