29 November 2018

Ms. Ajarin Pattanapanchai
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

To Ms. Ajarin Pattanapanchai,

RE: Additional Submission with comments on Thailand's Cyber Security Bill.

We thank the Thai Government for seeking comments on the Cyber Security Bill. Cyber security is a serious global concern and we commend the Thai Government for its commitment to protecting security and privacy. Building cyber security capacity while also enabling businesses and innovation to thrive in the digital economy is critical to ensure that Thailand is a strong player in the digital marketplace. Following our previous comments on the Cyber Security Bill, submitted on 12 October 2018, AIC would like to make this additional submission. We wish to incorporate this submission to the AIC comments dated 12 October on the provisions that remain unchanged from the previous draft of the Bill. We are also attaching the 12 October AIC submission for your reference.

The Asia Internet Coalition (AIC) is an industry association made up of leading internet and technology companies. The AIC seeks to promote the understanding and resolution of Internet policy issues in the Asia Pacific region. Our Members include Amazon, AirBnb, Google, Facebook, Apple, Twitter, LinkedIn, Expedia, Rakuten, LINE and Yahoo.

1. DEFINITIONS

SECTION 3

Recommendation: The definition of "**Code of Practice**" means "any regulations issued or approved by the National Cybersecurity Committee, including further additional or amended notifications, guidelines." The NCSC is authorized to prescribe the Code of Practice and standard framework in respect of the Cybersecurity as the minimum requirements for the Government Agency and the Organization of Critical Information Infrastructure (section 9 (5)). This definition should be updated to clarify what is meant by "notifications" and also to permit for advance public notice and comment to ensure that any implementing regulations do not expand the scope of the law.

Recommendation: The definition of **"Critical Information Infrastructure"** as presently drafted is too broad. We recommend that there are concrete criteria of what constitutes critical information infrastructure, including the location of the infrastructure, size of the owner, and number of affected persons. The procedure to identify the owner should also be clear (e.g., notify the regulated owners), and the owner should have to right to appeal. Moreover, we recommend that Bill should not capture private agencies working on Critical Information Infrastructure.

Recommendation: The definition of "**Cybersecurity Incident**" as presently drafted is overly broad and could apply outside the cybersecurity context. This term could be defined to be more in line with a more

globally-accepted definition, such as that currently proposed by the National Institute of Standards and Technology in the United States, which is under a notice and comment period at present, but currently defines a computer security incident as: "An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies."[1]

CHAPTER 1

i. SECTION 9 (6), (7)

Recommendation: These sections presently provide, "(6) coordinate and cooperate on establishing the Computer Emergency Readiness Team (CERT) in the country and foreign countries with respect to Cybersecurity Incident, and determine Cybersecurity Solution" and "(7) help coordinate with other agencies to determine the framework and cooperation in respect of Cybersecurity with local and foreign agencies." Section 9(6) is a bit confusing because it appears to indicate that CERT would be established in "foreign countries" and maybe what is intended is, "coordinate and cooperate with foreign countries." In any event, it would be beneficial to know which "foreign countries" and "foreign agencies" are being contemplated and what factors will be considered in deciding to coordinate and cooperate with a foreign country to ensure that cybersecurity best practices are implemented in Thailand.

ii. SECTION 10

Recommendation: This section provides, in relevant part, with regard to the National Cybersecurity Committee (NCSC) "and any other committee as a managing representative under NCSC's supervis[ion]. Details, elements, appointment, removal, qualifications, and authorities of the aforementioned committee including the appealing process of NCSC's and the committee's orders shall be determined by the NCSC". This section could be revised to provide better checks and balances so that not all NCSC committee power, including appeal adjudication, is centralized within NCSC.

In addition, this section permits the NCSC to appoint new committees for the internal management of NCSC - the Committee of the National Cybersecurity ("Committee Supervising the Office" or "CNC"), the National Cybersecurity Regulating Committee ("NCRC"), the Critical Information Infrastructure Supporting Committee ("CIISC"), and any other committee as a managing representative under NCSC's supervision. We recommend revising this section to make it clear which entity/committee will have the ultimate decision-making power in the event of a Cyber Threat. As currently drafted, there could be a conflict in authority. The use of "Committee of the National Cybersecurity" and "Committee Supervising the Office of the National Cybersecurity Committee" in section 3 (definition section) and section 10 are also not consistent (may be a typo). These terms should be made consistent.

CHAPTER 3

i. Part 3. Section 44(4)

Recommendation: This section provides, "The NCSC shall have the power to prescribe the type of organizations that has the tasks or provide the services in the following aspects as a[n] Organization of Critical Information Infrastructure", and at (4) states that NCSC can prescribe "information technology and telecommunications [organizations]." This is very broad and could include service providers from the infrastructure level down to app services – this section should be clearly defined with parameters around what organizations constitute "information technology and telecommunications".

[1] https://csrc.nist.gov/glossary/term/incident

ASIA INTERNET COALITION

ii. Part 3. Section 44 (8)

Recommendation: This section provides, "The NCSC shall have the power to prescribe the type of organizations that has the tasks or provide the services in the following aspects as a[n] Organization of Critical Information Infrastructure" and enumerates a list of "critical information infrastructure," and at (8) states that NCSC can prescribe "others." It would be helpful to explain what process NCSC will use to prescribe a critical information infrastructure designation and that a notice and comment period will be provided.

iii. Part 4. Section 54

Recommendation: This section, or the definitions section, should be updated to define what constitutes a cyber threat at a "general," "critical," and "crisis" level, and the corresponding implications. This is especially the case given the comment at CHAPTER 3 Part 4. Section 59 (see below).

iv. Part 4. Section 54 (2), (3) and Part 4. Section 58(1)-(5)

Recommendation: This section provides that when it "appears" to NCSC that a cyber threat "is" or "may be" occurring, that NCSC can, under Section 54(2), "support, aid, and participate in the protection, dealing with, and mitigation of risks from Cyber Threats." This provision should be omitted or changed to be, "advised about the support, aid, and . . ." As written, the provision could expose sensitive cybersecurity information, which could further worsen a cyber threat. It would be better to permit for remediation without outside NCSC support, aid, or participation to ensure that a cyber threat is identified and resolved as quickly and effectively as possible and that sensitive cybersecurity information is protected. Similarly, under Section 54(3), this provides that NCSC can "suggest or order to use the solution system to maintain the Cybersecurity including finding a countermeasure or solution regarding Cybersecurity." Similarly, Section 58(1) - (5), permits NCSC, in response to a cyber threat, to engage in (1) monitoring, (2) investigation, (3) removal, (4) termination, or (5) access, subject to a court order. These provisions at Section 54 and 58, while well-intentioned, are overly intrusive and prescriptive and could result in an order or proposed countermeasure or solution that is not suitable for the cyber threat at issue and could do more harm than good. Instead, these provisions should be omitted or changed to be, "advised that a solution has been found to maintain the Cybersecurity." It is reasonable for NCSC to be advised on how the cyber threat is being handled and mitigated, but broader or deeper access risks surveillance of proprietary and otherwise sensitive information and information systems.

v. Part 4. Section 55

Recommendation: This section provides that, "any person giving information in accordance with paragraph one, which acts in good faith, shall be protected and shall not be deemed a wrongful act or a breach of contract". If a party complies with a section 55 order (which requires such party to deliver information/documents), and such compliance causes the entity to be in breach of contract with a third party, this provision grants an exemption to the party, whereby a third party cannot bring a claim for breach of contract or tort against the complying party, provided that such party was acting in good faith. This exemption could conflict with protections under other laws, e.g. patent, trade secret, personal data protection and we recommend that this is clarified.

vi. Part 4. Section 58

Recommendation: This section provides, "In case of necessity to access information under Section 58 (5), the NCSC or the NCRC, by the Secretary-General of the NCSC to submit the motion to the Court to order the owner, the possessor or the user of the computer or computer system or a person monitoring the computer system in accordance with paragraph one to comply with the motion". This provision is problematic because it does not define what would constitute "necessity". This section should be amended to codify the factors that the NCSC or NCRC must take into account when deciding whether the

issuance of an order is "necessary". Such factors should include that that the NCSC/NCRC weigh whether the issuance of an order is necessary to accomplish the aims or the objectives of the law, and take into account the order's effect on the private sector (which should be minimal).

vii. Part 4. Section 59

Recommendation: This section provides, "In case it is urgent and necessary and the Cyber Threat is at a crisis level, the NCSC may operate immediately, only to the extent it is necessary to prevent and remedy the damages in advance, and the motion to the Court is not required to be submitted. However, after such operations are complete, the NCSC or the NCRC shall notify the details of the operations to the Court without delay." This emergency access provision is problematic because it does not define what would constitute "urgency" or "necessity," and it only provides for judicial notice "after" an operation is concluded. This section should be amended so that judicial notice is submitted while NCSC is conducting its operation, to ensure proper legal oversight and prevent an abuse of the law. In addition, this section should codify the factors that the NCSC must take into account when deciding whether the issuance of an order is "necessary". Such factors should include that that the NCSC weigh whether the issuance of an order is necessary to accomplish the aims or the objectives of the law and take into account the order's effect on the private sector (which should be minimal).

The last paragraph of Section 59 provides, "In case of emergency for the benefit of protecting, assessing, dealing with, suppressing, suspending, or mitigating the risks from Cyber Threats, the Secretary-General, upon the approval of the NCSC or the NCRC, shall have the power to request real-time information from a person related to the Cyber Threat. Such person shall cooperate and facilitate without delay". This emergency access provision is problematic because it does not provide proper legal oversight and there are no checks and balances to prevent an abuse of the law. We respectfully request that such provision be subject to a valid court order.

viii. Part 4. Section 60.

Recommendation: This section provides, "A person receiving the order under the authorities in Part 4 related to the dealing with Cyber Threats may appeal the order for the Cyber Threats at a general level only." This section severely limits the appeal rights for persons accused of perpetrating a "critical" or "crisis" level threat and could create perverse disincentives to label a cyber threat "critical" or "crisis" to prevent appeals. To ensure an equitable process and prevent this perverse incentive, appeal rights should be permitted for all threat levels, especially as the designation of a threat level could be called into question. This is especially true because "general," "critical," and "crisis" levels are undefined in the bill.

ix. Sections 49, 54, 55, 57, 58 and 59

Recommendations: These sections specifically authorize relevant authorities to access information and facilities. The authorities have the power to command, request and order the Organization of Critical Information Infrastructure and other relevant persons to provide information, personnel assistance, electronic equipment, and/or access to communication data and/or to summon person and any documents/evidence, and/or request compliance without court order under certain circumstances (except sections 58(5), 59(3) and 59(4)). We respectfully request that all sections that authorize relevant authorities to access to information and facilities in the private sector require a valid court order.

CHAPTER 4

i. Penalty Provisions. Part 4. Section 61 and Section 62

Recommendation: Section 61 provides "the officers and the inquiry officials under this [Bill] may not disclose or send computer data, computer traffic data, or data of the users or data related to Information Asset obtained from this Act to any person." Section 62 provides "any officer or inquiry official under this

[Bill] negligently act causing other persons to know computer data, computer traffic data, or data of the users or data related to Information Asset obtained from this [Bill]..." We recommend that section 61 and section 62 are expanded to protect all data that may be disclosed by the private sector to the competent authority in this Bill, as there may be additional data disclosed that does not fall within "computer data, computer traffic data, or data of the users or data related to Information Assets" that should be protected.

ii. Penalty Provisions. Part 4. Sections 64, 65, 66, 67, 68

Recommendation: This chapter on penalties helps place a check on misuse of information access contemplated elsewhere in the proposed legislation, but does not change that the NCSC powers provided for are too prescriptive and intrusive. To the extent the penalties provisions remain, "reasonable cause" should be defined to prevent an easy out from the penalty provision.

iii. Transitory Provisions. Part 4. Section 71

Recommendation: This section provides, "the NCSC may prescribe special considerations for the officials, personnel, or employee during the operation in the Office." It is unclear what "special considerations" means and whether a potential expansion of power could be conceived under this. Greater clarity here would be helpful to limit the scope of what "special considerations" could mean.

iv. Consistency with the Personal Data Protection Bill

Recommendation: The Personal Data Protection Bill issued by the Ministry of Digital Economy and Society (MDES) was recently revised in order to align with principles from the General Data Protection Regulation (GDPR) and ensure that Thailand meets the GDPR standard for cross-border transfers. However, 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 definition of cybersecurity under this Bill covers cyber-attacks that affect national security, economic security, military security, and public order. Economic security and military security could be beyond the scope of the GDPR. We recommend that the government should seek confirmation from the EU first if this Bill would be deemed in compliance with the GDPR and meet the objectives of the recent version of the Personal Data Protection Bill.

We hope that our comments above are useful to the Thai Government as insight into the industry perspective and look forward to working constructively together to be resources as Thailand builds its cybersecurity capacity while also maintaining a business-friendly environment that welcomes digital trade and investment. As always, we are happy to provide further comments or answer any query the Government may have, via e-mail or in person. Thank you for your consideration.

Yours sincerely,

Jeff Paine
Managing Director,
Asia Internet Coalition
www.aicasia.org | jeff@aicasia.org | Secretariat@aicasia.org