12 October 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,

(sent via email)

RE: Submission of comments regarding concerns about aspects of the Cyber Security Act.

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.

We thank the Thai Government for seeking comments on this latest draft of the Cyber Security Act and welcome further collaboration and public consultation. Cybersecurity is a serious global concern and we commend the Thai Government for its commitment to protecting security and privacy. Building cybersecurity 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 Act, submitted on 28 March 2018, we respectfully submit our concerns about aspects of the Cyber Security Act in its current form, as follows:

1. Consistency with the Personal Data Protection Bill

Thailand's 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. Thus, 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 still view the current level of data protection of data subjects under this Bill is insufficient and suggest there should be a clearer provision regarding personal data protection.

2. Definitions

Section 3. It is notable that neither critical infrastructure nor election security is mentioned in the section. This lends one to view the law as, less about cybersecurity in a traditional sense, and more about preserving the existing "martial security" and power structures. We request reconsideration of scope, especially if building cybersecurity capacity is a primary goal of this law.

Section 3. The terms "unusual operation" and "other similar systems" are not defined. Defining these terms would help to better define the scope of the law's applicability, otherwise any broad range of cyber-related activity could be made to constitute a "cyber-attack" and make the law difficult to apply and enforce.

Section 3. In regard to "Fundamental Information Infrastructure", this should explicitly not include "the private sector." Further, we recommend that the law should be restricted to companies incorporated in Thailand that operate or control critical infrastructure in Thailand. Additionally, this section should clarify to what "public interest" refers to.

3. Authorities

Section 9(3). It would be helpful to define "materially or severely" in the context of cyber-attack to focus the law's applicability.

Section 9(9)(1). Regarding the "specification of the risk that may expose to the Information Asset...", the risk is not defined and should be narrowly tailored.

Section 9(9)(3). The word "monitor" is of concern as it opens the door to surveillance, which could harm the public good. We suggest it be removed. Additionally, "examine" should be changed to "study" to indicate an after-the-fact action. This is also true for Section 16(4) where "monitor" is used.

Section 16(8). This is a problematic clause and we would respectfully request removal. The terms “collecting and analysing the data of the Cybersecurity of the country” and “publicise the information in relation to the risk and incidents of the Cybersecurity to the Government Agency and private sectors” must be defined – this clause could be used to surveil user data or security practices and publicise private information in the name of cybersecurity. This clause also has the potential, if exploited, to cause grave economic and reputational harm to platforms and their users, and that reputational harm could extend to Thailand in a worst-case scenario.

Section 18(4). Similar to Section 17(6) above, this is problematic, because if any of this money or assets are coming from private sector companies, it has the potential to create favouritism for companies not bound by anti-bribery laws.

Section 19, to strengthen human capital for cyber security, the committee supervising the Office of the National Cybersecurity Committee should also comprise civil society representatives and industry representatives to ensure industry best practices can be provided.

Section 26(5). We feel that the Official should be away from the government for more than 1 year to prevent the existence or appearance of bias or favouritism.

4. Policies and Plans

Section 36. It is unclear what "protect, deal with, and mitigate the risks" fully encompasses. Clarity would be helpful to prevent this language from being overly broad.

Section 36. "Which shall at least cover the following issues” - the term "at least" makes the list non-exhaustive and therefore leaves it ill-defined. The scope should be explicitly stated.

Section 38. It is unclear what "each organisation" means in this section. This should be clarified.

5. Management

Section 39. It is unclear what "protect, deal with, and mitigate the risks" fully encompasses. Clarity would be helpful to prevent this language from being overly broad.

6. Fundamental Information Infrastructure

Section 42. It is unclear what "protect, deal with, and mitigate the risks" fully encompasses. Clarity would be helpful to prevent this language from being overbroad.

7. Critical information infrastructure

Section 43(8). This catch-all point "others as prescribed by the NCSC" is overly broad and we would request its removal.

Section 43. We would request there be concrete criteria of what constitutes critical information infrastructure (CII), 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. The proposed definition of CII is too broad. Moreover, we suggest that bill should not capture private agencies working on CII.

The lists of regulated organisations should be scoped. For example, “information technology and telecommunications” is very broad. It could cover aspects from application level to internet infrastructure level. Thus, it should be clear who is subject to this Bill and their duties and liabilities under the Bill.

Section 44. It is of concern that the NCSC is envisioned to make its own rules and then decide if there are “inquiries or claims” regarding those rules – we suggest MDES consider having a different body to be the arbiter of “inquiries or claims” to prevent too much power being seated with the NCSC.

8. Access to information and facilities

Section 46 allows authorities to request the following information.

> (1*) Information on designing and configuring of the Critical Information Infrastructure and such information of the system connected to or communicating with such Critical Information Infrastructure;*
>
> *(2) Information on the operation of the Organisation of Critical Information Infrastructure, the system connected to or communicating with such Critical Information Infrastructure that is under control of the Organisation of Critical Information Infrastructure;*

(3) Other information deemed necessary to maintain the level of cybersecurity of the Organisation of Critical Information Infrastructure.

In addition, the organisation receiving the letter in accordance with paragraph one may not claim duties under other laws or contracts as an excuse to not disclose the information. The compliance with this Section with good faith shall not be deemed violation of the laws or breach of the contracts.

This above provision should be removed because it could conflict with protections under other laws, e.g., patent, trade secret, personal data protection. In addition, the language where the organisation will be exempt from liabilities under other laws or contracts could not be enforceable in certain circumstances, especially in the case of conflict of laws, where the contract is governed by foreign law.

The language 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 does not align with the internationally recognized best practices in data protection, and would be nearly impossible to enforce, particularly if a private agency is subject to foreign law that would contradict their responsibility under Section 46.

Further, provision of information in accordance to item 1,2,3 will increase the risk of the security system of being attacked, for example if the information fell into the wrong hands.

Section 49, and again in Section 57. The word "monitor" is of concern as it opens the door to government surveillance, of social media and other platforms in the name of preserving cybersecurity which could harm the public good. As such, it should be removed. Additionally, we suggest "examine" should be changed to "study" to indicate an after-the-fact action.

Section 51 and Section 52(1) and Section 56, 56(3) and Section 57. It is unclear what "protect, deal with, and mitigate the risks" fully encompasses. Clarity would be helpful to prevent this language from being overly broad. 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 occurs or 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.

Section 53(2). This section could be difficult in application as it is currently written, as sometimes it is unclear whether a cyberattack has occurred, and the circumstances under which one is announced could cause reputational harm if there is not enough internal investigation first. "Necessary and appropriate" should please be better defined. Transparency is important, but in the right circumstances where the facts are appropriate for public disclosure and verifiable.

Sections 54, 55, 57 and 58 specifically authorise relevant authorities to access to information and facilities. The authorities have the power to command, request and order the Organisation 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 section 58 (4)).

It should be highlighted that this version of the Bill has removed court order requirements in access to information and equipment of other persons. We respectfully request that Items 1, 2, and 4 require a court order.

Further, regarding Section 54, these are all situations where legal counsel would need to be present. "Appropriate" and "prescribed" are undefined and give too much power to the enforcer. "Beneficial" is over-broad and we would request its removal.

Section 55. We would request clarification for what "use electronic devices" means in this context. This is problematic because it raises the spectre of surveillance or monitoring by the government.

Section 57. We would request that the term "person" be defined to exclude a corporate person. Also, this section should permit the potential private entity to remediate from a cyber-attack independently without government intrusion.

Section 57(2). We would respectfully request the word "study" instead of "investigate" be used.

Section 57(3). Section 58(4). This seems overly prescriptive conduct and we would recommend this be redrafted to be more business-friendly to ensure businesses do not move out of Thailand due to compliance difficulty.

Section 58. The scope of applicability of this provision is not clear.

Section 58(2). This section risks becoming dated as a technological matter very quickly and we would respectfully recommend this be redrafted in a technology-neutral manner.

Section 58(4). This seems overly prescriptive conduct and we would recommend this be redrafted to be more business-friendly to ensure businesses do not move out of Thailand due to compliance difficulty.

We request that Items 1, 2, 3 and 4 should require a court order.

9. The Cyber Attack which is at a critical level

The Secretary General has additional authorities in case the Cyber Attack is at a "critical" level. However, the criteria to identify the critical level is rather ambiguous and is difficult to differentiate from a normal attack.

10. Potential for criminal penalties and fines for non-compliance

There are penalties for non-compliance which appear in sections 47, 50, 54 (1) and (2), 57, and 58. *Failure to comply with the order of the Secretary-General and/or the Officer under sections 57 (3) and (4) and 58 could be subject to an imprisonment and/or fines. The authorised person, a manager or any person responsible for the operation of such juristic person could also be subject to an imprisonment.*

These sections of the Bill continue to impose criminal liability for several breaches under the Bill. We 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. 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.

Section 63. It is not clear what "disrupting" or "not complying" would mean.

Section 64. This might conflict with the intention of Thai Corporate Laws which states that only the authorised director of the company will be liable on behalf of the company. Therefore, this Bill should not broaden the liability to others, such as employees or managers in the company.

11. There is no confidentiality protection under this Bill.

We note that there are no general provisions regarding confidentiality protection when the Thai authorities exercise their powers under this Bill. We also note that the provisions prohibiting the Officers from disclosing information to other persons and the penalty for failure to do so have been removed. Both removals should be reinstated. 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.

12. The Committee, The Secretariat and Officer's authorities

We suggest that there must be a penalty clause for misconduct or any abuse of power by The Committee, The Secretariat and The Officer(s).

We hope that our comments above are useful to the Thai Government as insight into the industry perspective. We look forward to working constructively together and hope to be a resource to policy makers such as yourself, 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