ASIA PACIFIC CARRIERS' COALITION
(Incorporated in the Republic of Singapore)

PUBLIC CONSULTATION ON DRAFT CYBERSECURITY BILL

SUBMISSION TO

SINGAPORE MINISTRY OF COMMUNICATIONS AND INFORMATION AND SINGAPORE CYBERSECURITY AGENCY

BY THE ASIA PACIFIC CARRIERS' COALITION

24 AUGUST 2017
[Public Version]

Asia Pacific Carriers' Coalition
c/o Rajah & Tann Singapore LLP
9 Battery Road #25-01
Singapore 049910
T: +65 6535 3600
F: +65 6225 0747
Email: secretary@asiapacificcarriers.org

TABLE OF CONTENTS

A. SUMMARY OF MAJOR POINTS

The Asia Pacific Carriers' Coalition (APCC) thanks the Singapore Ministry of Communications and Information (MCI) and the Singapore Cybersecurity Agency (CSA) for the opportunity to comment on the proposed Cybersecurity Bill (Bill). The APCC and its members are keen to work with the various stakeholders to develop a regime that best protects the interests of Singapore without imposing unnecessary compliance burdens.

The APCC's comments below can be divided in to three main themes.

1. Definition of Critical Information Infrastructure (CII).

   The APCC seeks clarity on the definition of CII as the language in the Bill leaves some ambiguity as to who can be designated an owner. This is a particular concern to the APCC as its members are the providers of telecommunications services to enterprise customers.

   The designation of CII as an official secret is problematic as maintaining the confidentiality of this designation may conflict with the reflection of duties of a CII owner in customer or vendor contracts.

   The APCC is also concerned with the possible extra-territorial aspect of CII, which in certain circumstances may conflict with the regimes in other countries.

2. The Powers of the Commissioner and Information Sharing.

   Under the Bill the Commissioner has sweeping powers to designate CII. Although the APCC has no objection in principle to such a power, it believes that it should be subject to established criteria and due process.

   The APCC agrees with the sentiment expressed in the Bill that there is a need for information sharing between Government and CII providers but is concerned that the Bill makes this rather one sided. The APCC strongly believes that it is important for information sharing to be collaborative amongst all concerned stakeholders.

3. Licensing Framework

   The APCC fully agrees with the principle that any necessary regulation should be light touch. The APCC believes however that the licensing approach adopted in the Bill is not consistent with this and could be counter-productive. The APCC therefore suggests an alternative approach of the Singapore Government accepting and recognizing internationally recognized standard and accreditation regimes.

B. STATEMENT OF INTEREST

1. On 10 July 2017, the Singapore Ministry of Communications and Information (MCI) and the Singapore Cybersecurity Agency (CSA) issued a Public Consultation on the Cybersecurity Bill (Bill) which the Asia Pacific Carriers' Coalition (APCC) is pleased to offer a written submission.

2. The APCC is an industry association of global and regional telecommunications carriers operating in the Asia Pacific region, formed to work with governments, National Regulatory Authorities and users in advocating open market policies and best practice regulatory frameworks in order to promote competition and efficient investment in telecommunications markets.

3. The APCC understands and agrees that cybersecurity is an issue of increasing and critical importance which requires government attention as can be seen by recent well publicized events where attacks have been made on the institutions of the state. Many countries as diverse as China and Australia have seen the need to introduce legislation to protect against such attacks on its national institutions and essential services as well as safeguard the personal information of its citizens.

4. The APCC commends the MCI and CSA for taking a consultative approach with the various stakeholders and is committed to working to establish legislation that balances the need to protect Singapore and its citizens without imposing unnecessary compliance and costs burdens on industry.

5. APCC members may be directly affected by the proposed Bill as designated Critical Information Infrastructure (CII) providers and also (and possibly more likely) their customers will be so designated.

6. In addition, many of the APCC's members may be classed as suppliers or potential suppliers of investigative and non-investigative cybersecurity services to customers in Singapore under the Bill. The proposed new licensing regime will impact those APCC members by requiring them to obtain licenses in Singapore, ensure that their employees and vendors are licensed under the new regime and add to an existing compliance burden in Singapore.

7. In the interests of accessibility, the APCC has endeavored to keep this submission brief but will be pleased to provide more detailed comments or engage in workshops moving forward.

8. The APCC does not assert confidentiality in respect of any part of this submission.

C. COMMENTS

9. In this section, the APCC sets out its specific comments in relation to the Consultation Paper and the Bill.

CRITICAL INFORMATION INFRASTRUCTURE (CII)

10. The basic mechanism for securing cybersecurity is to create a framework to regulate CII. It is therefore essential that there is a very clear understanding of the definition of CII and there are a number of points where the APCC seeks clarity.

Essential Services – Info-communications

11. The First Schedule to the Bill sets out the list of essential services that are relevant for the purposes of the definition of CII. The APCC notes that the four essential services covered in the Info-communications category include:

    (a) Fixed Telephony;

    (b) Mobile Telephony;

    (c) Broadband Internet Access[1]; and

    (d) National Domain Name Services.

12. The list of Info-communications essential services appears to target domestic residential basic telecoms services in Singapore rather than international enterprise services which are generally targeted by members of the APCC. The APCC seeks clarity on this point as well as whether the term "Broadband Internet Access Service" includes Singapore internet service provider (ISP) services.

Ancillary Services supplied to owners of CII.

13. The APCC notes that its members provide ancillary services such as connectivity and colocation services to enterprise customers in Singapore who will be designated as owners of CII under the proposed Bill.

14. The APCC believes further clarity is required on clause 2 of the Bill in the definition of *"owner of a critical information infrastructure"*. which is defined as "a person" who:

    (a) has effective control over the operations of the critical information infrastructure and has the ability and right to carry out changes to the critical information infrastructure; or

    (b) is responsible for ensuring the continuous functioning of the critical information infrastructure

    and as to the ownership of critical information infrastructure and the primary responsibility under the bill.

[1] We note that "Broadband Internet Access Services" is duplicated in paragraphs 5 and 6 of the First Schedule.

Designation of CII as an Official Secret.

15. Paragraph 28 of the Consultation Paper states that the designation of a computer or computer system as CII is an official secret. This may cause a practical problem in circumstances where an owner of CII is required to reflect its duties under the Bill in contracts with service providers and vendors but would be prevented from disclosing that the relevant computer or computer system was designated as CII. The APCC would like to understand the rationale for an official secret designation as this is something that maybe easily inferred but in any case there should be a mechanism for CII owners to pass these obligations on without breaching the Official Secrets Act.

The powers of the Commissioner to designate CII

16. Section 7(1) of the Bill states that the Commissioner may by a written notice, designate a computer or computer system as CII for the purposes of the Act. Although it is stated that the Commissioner has to be satisfied that the computer or computer system should fulfill the criteria of CII, it is a somewhat ambiguous as to what those criteria are. The APCC suggests therefore that there should be some guideline as to the process and criteria under which the Commissioner can make such a designation.

Designation of CII as Computer System as outside of Singapore

17. Section 7(1)(b) of the Bill indicates that a computer or computer system "located wholly or partly in Singapore" can be designated as CII. As APCC members provide customers with regional and global networks this is likely to apply to them, either directly or indirectly. The APCC seeks confirmation that computer systems that are wholly outside of Singapore will not be designated as CII.

18. There is also an extra jurisdictional issue here that the APCC respectfully submits should be further considered. In some circumstances, there is a possibility that an obligation placed under Singapore law may conflict with regulations in another country. It may also be very difficult for the CSA to enforce obligations against owners of CII which are located outside Singapore which may also potentially undermine the credibility of the CSA and the objectives of the Bill.

Obligation to establish mechanisms and processes.

19. Section 15(2) of the Bill states that the duties of CII owners include an obligation to *establish mechanisms and processes as may be necessary in order to detect any cybersecurity threat in respect of its critical information infrastructure*. This creates an ambiguous and onerous obligation that would require owners of CII to ensure threat detection capability for CII (even though a breach of section 15(2) does not constitute an offence for the purposes of clause 15(3)). Given the absolute nature of this obligation, the APCC submits that this obligation be removed, or at least tempered by a reasonableness or a materiality threshold.

OBLIGATIONS ON OWNERS OF CII

Further guidance on duties of owners of CII

20. The APCC notes that owners of CII are subject to certain statutory duties including:

    (a) Providing information to the Commissioner;

    (b) Complying with Codes and directions;

    (c) Reporting incidents;

    (d) Conducting audits;

    (e) Conducting risk assessments; and

    (f) Participating in exercises.

21. The APCC also notes that paragraph 31 of the Consultation Paper states that the CSA will provide more guidance on how owners of CII may comply with these duties. The APCC welcomes the CSA's proposal to provide more guidelines on the scope of these duties and requests an opportunity to contribute to a further public consultation process in relation to any guidelines or Codes of Practice implemented by the CSA in relation to these duties. In any event, the APCC notes at this time that these duties will impose an additional compliance burden on owners of CII and submits that the duties should be proportionate to the objectives of the Bill and clearly defined.

22. The APCC also request further clarification on:

    (a) what would be considered "significant cybersecurity incident" for the purposes of section 15 of the Bill; and

    (b) whether the duties of owners of CII will require any public disclosure.

Obligations on owners of CII should only apply to designated CII

23. The APCC notes that the there is a potential issue arising from the definition of *critical information infrastructure* in Section 2 of the Bill and the language in Section 10 which sets out the duties of owners of CII. Specifically, Section 10 does not expressly state whether the obligations apply only to *designated* CII which creates ambiguity in the section as to whether an owner of *critical information infrastructure* (which is defined without mentioning *designation* in Section 2) is required to comply with the duties regardless of whether the CII is designated or not. The APCC assumes that this is not the intention of the Bill. However, in the event, that the APCC has misunderstood the MCI and CSA's intent, the APCC submits that the owner obligations in Section 10 should only apply to *designated* CII, and for clarity, the definition of *'critical information infrastructure'* in section 2 be amended to refer to the required designation under Section 7.

RESPONDING TO AND PREVENTION OF CYBERSECURITY INCIDENTS

24. The Commissioner seems to have wide and sweeping powers in investigating and responding to cybersecurity incidents. The APCC entirely understands that it is important for the Singapore

authorities to investigate and deal with cybersecurity threats and incidents and supports the rights to do so. The APCC urges that the powers of the Commissioner be subject to due process (including appropriate appeal mechanisms) rather than at the sole discretion of the Commissioner. In the USA for instance the CII owners are required to comply with similar measures, but only under a court order. Other countries are adopting a more collaborative approach between industry and Government agencies to tackle cybersecurity threats. For example:

(a) **USA** Between 2014 and 2016, the US passed legislation including the Cybersecurity Act of 2015 as well as implemented initiatives such as the Cybersecurity National Action Plan which involve a collaborative approach between state agencies and industry.

(b) **UK** In December 2016, the UK launched its National Cybersecurity Strategy 2016-2021 which focuses on a collaborative approach to managing cyber risks to critical national infrastructure and sharing of information. In particular, the UK government has committed to sharing threat information with industry that only the government can obtain so that the industry knows what they must protect themselves against.

(c) **Canada** A Canadian government initiated industry consultation on Canada's future Cybersecurity concluded in October 2016 emphasised the need for a collaborative approach between all stakeholders including providers of communications infrastructure. The resultant Canadian Plan for Critical Infrastructure, rather than take a prescriptive regulatory approach instead sets out a number of collaborative actions and educational measures across Government, industry and infrastructure owners to combat cyber threats.

(d) **Australia** In June 2017 the Parliamentary Joint Commission on Intelligence and Security provided an advisory report at the request of the Attorney General. In this report the Committee recommended that the Attorney-General's Department works collaboratively with industry to ensure effective and regular information sharing, in particular sharing threat information with industry.

25. The APCC also notes that paragraph 7(c) of the Consultation Paper and the preamble to the Bill states that a key objective of the Bill is "to establish a framework for the sharing of cybersecurity information with and by CSA and the protection of such information". The APCC fully supports this, but feels that the way the Bill is drafted imposes duties on the CII providers to report to the CSA and so the flow of cyber threat information is rather one way. There will be instances where the Singapore Government would receive intelligence of impending threats which would help industry take the necessary steps to protect their networks. Information sharing between industry and government enables a flexible, coordinated and rapid response to emerging cyber threats. The APCC recognizes the rapidly evolving technology sector and correspondingly varied and quickly evolving cyber-threat landscape and therefore fully supports the principle of information sharing but submits that it be a two-way process. Such two-way information sharing will provide a much stronger capability to protect Singapore's infrastructure and its citizens.

CYBERSECURITY SERVICE PROVIDERS

26. The APCC commends the MCI and the CSA for adopting a holistic approach to the regulation and licensing of cybersecurity practitioners and service providers in Singapore. The APCC considers that this approach is preferable to a sector specific approach to cybersecurity which may lead to inconsistency of approach and confusion in relation to overlapping regimes across different sectors

– particularly for members of the APCC who supply services to customers across different sectors in Singapore.

27. The APCC also welcomes the MCI and CSA's stated intention implement a "light touch licensing framework for cybersecurity providers"[2] and to keep "licensing requirements and registration procedures as light as possible"[3].

28. However, the APCC is concerned that the licensing regime as articulated in the draft Bill will cause unnecessary complexity, ambiguity, compliance burdens and costs in a way that is above and beyond the need to regulate cybersecurity providers and practitioners as well as at the expense of the Bill's stated intention to develop the cybersecurity industry in Singapore.

29. The APCC sets out some of these complexities, ambiguities, costs compliance burdens in the draft Bill at paragraphs 30 to 37 below. Further, at paragraphs 38 to 41 the APCC proposes an alternate light approach to regulation of the cybersecurity industry in Singapore.

THE PROPOSED LICENSING FRAMEWORK

Global cybersecurity service providers and practitioners

30. The APCC notes that the proposed licensing regime is intended to apply to both domestic and overseas providers and practitioners of cybersecurity services in order to ensure that *there is as much as possible a level playing field between local and overseas service providers'*[4].

31. The APCC is concerned that the proposed requirement that both domestic and overseas cybersecurity providers and practitioners be licensed in Singapore carries a number of practical challenges and difficulties and does not appear to recognize the fact that there is a global market for cybersecurity skills and services. In particular, many operators including APCC members are likely to supply services to customers in Singapore using infrastructure and employees located in multiple countries depending on cost and availability of specialist skills. By way of a hypothetical example, a cybersecurity service provider is likely to supply a cybersecurity solution to a customer in Singapore comprising:

    (a) employees who would be classified as providing investigative cybersecurity services working as a team in geographically diverse locations in Singapore and other countries;

    (b) vendors based inside and outside Singapore;

    (c) managed security operations centre (SOC) monitoring service infrastructure that could be located inside or outside Singapore; and

    (d) a virtual private network connecting sites in Singapore with sites outside Singapore (including any managed SOC outside Singapore).

[2] Para7(d) of the Consultation Paper
[3] Para 55 of the Consultation Paper
[4] Paragraph 56 of the Consultation Paper

32. The APCC submits that the requirement for global cybersecurity practitioners or service providers to acquire a Singapore based licence in respect of their global operations would:-

(a) impose an onerous compliance burden that is not proportionate or reasonably required to meet the objectives of the Bill;

(b) be very difficult for the CSA to enforce in respect of overseas cybersecurity service providers and practitioners which may also potentially undermine the credibility of the CSA and the objectives of the Bill; and

(c) increase the cost and complexity of supplying cybersecurity services to customers in Singapore – particularly if cybersecurity service providers were forced to establish full service capabilities in Singapore or create artificial and impractical partitions between Singapore based and overseas personnel.

Record Keeping Obligations

33. The APCC notes the duty under Section 34 of the Bill for licensees to record on each occasion that a licensee provides services information including:

(a) the name and address of the person engaging those services;

(b) the date on which the services are provided;

(c) details of the services provided; and

(d) any other details as may be prescribed.

The APCC recognizes and acknowledges the need for cybersecurity service providers and practitioners to maintain proper records to allow the CSA and the Commissioner to work with providers and practitioners to prevent and respond to cybersecurity threats to Singapore's essential services. However, the APCC respectfully submits that the scope of the record keeping requirements are not proportionate for what might be considered necessary to fulfil the aims and objectives of the Bill.

34. In particular, the APCC submits that the document retention period of 5 years for investigative cybersecurity services is too long and would impose an unreasonable burden on individual practitioners and service provider licensees to store data that would likely have limited utility up five years. The proposed 5 year period[5] also goes further than other cybersecurity regimes; e.g Australia the period is 2 years. The APCC respectfully submits that the MCI and the CSA should be guided by other existing cybersecurity regimes as mentioned above.

35. The APCC also notes that the requirement for global cybersecurity providers and practitioners to maintain record introduces additional unnecessary complexity which would need to be addressed in the Bill and any implementing regulation and guidelines including whether:

[5] The APCC notes that paragraph 53 of the Consultation Paper states that record keeping requirements for investigative and non-investigative cybersecurity service providers will apply for 5 years. However, section 34(1)(b) of the Bill provides that the document retention period for investigative cybersecurity service and non-investigative cybersecurity service licensees will be 5 years and 3 years (respectively). We request that the MCI and the CSA clarify the document retention periods in light of this apparent inconsistency

(a) the licensee's obligation to maintain records of details of services covers just a description of the services or a full scope of work or operational, performance and service logs;

(b) records may be stored or hosted in a virtual environment outside Singapore and if so, how the CSA would propose to obtain access to those documents under due process of law; and

(c) licensees are required under section 34 to obtain and retain details of services supplied by vendors.

36. In summary, the APCC is concerned that the proposed licensing framework is not in fact "*light touch*" and would create a disincentive for cybersecurity service providers to invest in Singapore or to supply services to customers in Singapore. Any increases in compliance and delivery costs would also likely be passed on to consumers and customers of cybersecurity services. This outcome would be contrary to the stated objectives of the Bill to develop and promote the cybersecurity industry in Singapore[6].

37. On that basis, the APCC proposes an alternate approach to the regulation of cybersecurity service providers and practitioners.

ALTERNATE APPROACH– INTERNATIONAL ACCREDITATION AND CERTIFICATION

38. The APCC notes that there are a number of internationally recognized accreditation bodies and certification standards for cybersecurity providers and practitioners (including penetration testing) including:

(a) ISO/IEC 27001;

(b) The EC Council[7];

(c) ICS2[8];

(d) Information Systems Audit And Control Association (ISACA)[9]; and

(e) CREST.

39. Each of the above accreditation bodies imposes rigorous certification requirements including (a) criminal checks; (b) ethical standards and (c) exams and tests. For example, in order to earn the prestigious EC-Council LPT (Master) Credential, an applicant has to go through a rigorous background check including a verification of no criminal conviction.

40. Given the global nature of the cybersecurity market, obtaining an internationally recognized accreditation from one of the aforementioned accreditation bodies would be the most cost effective and efficient means of regulation. To further mandate compliance with an additional local licensing framework would impose an unnecessary additional regulatory burden and an increased cost of compliance on cybersecurity service providers which already comply with leading industry

[6] Section 5(h) of the Cybersecurity Bill.
[7] https://www.eccouncil.org
[8] https://www.isc2.org/
[9] https://www.isc2.org/

standards as required by their international certification. The further unintended consequence of the proposed licensing framework would be to create a barrier to entry for security services which would benefit consumers in Singapore.

41. In the circumstances, the APCC is of the view that the alternate approach to the proposed licensing regime would be to require cybersecurity service providers to obtain an international certification or accreditation which is recognized by the CSA. In this regard, the APCC proposes that accreditation bodies be recognized and approved by the CSA subject to the fulfilment of certain criteria, which the APCC would be pleased to work with the CSA to develop.

NEXT STEPS

Time frame for Implementation

42. The Bill, once it is enacted will impose significant extra compliance actions and costs on CII owners and cybersecurity providers and practitioners. For this reason, the APCC suggests that the industry be given sufficient time to ensure compliance with the new Act. The APCC submits that a period of 18 months from the enactment of the new Cybersecurity Act and the publication guidelines or Codes of Ethics relating to the implementation of the licensing regime under the Bill would be a sufficient period of time.

Further consultation on operational framework for licensing of cybersecurity services

43. The APCC also welcomes the statements in the Consultation Paper that the CSA will seek further consultation with the industry on detailed requirements before the licensing framework is operationalized[10].

44. As set out above in the Statement of Interest, many of the APCC's members are engaged in the business of supplying investigative and non-investigative cybersecurity services to customers in Singapore. Accordingly, the APCC looks forward to participating in, and requests an opportunity to contribute to a further public consultation process in relation to: -

    (a) the operational framework for the new licensing regime under the Bill including licence fees, licence terms and licence conditions;

    (b) the prescription of any additional licensable cybersecurity activities under the Second Schedule of the Act; and

    (c) any subordinate regulation, guidelines or Codes of Ethics relating to the implementation of the licensing regime under the Bill.

[10] Para 58 of Consultation Paper

D. CONCLUSION

45. In conclusion, the APCC is supportive of the increased focus on cybersecurity with a view to protecting the networks, security and privacy of citizens. The APCC's members share these concerns and are eager to work with the CSA to develop a regime that meets those aims whilst at the same time being proportionate to the aims of regulation and minimizing the compliance burden.

46. In this regard, the APCC views can be summed up in three broad areas:

(a) The definition of Critical Information Infrastructure should be clear so there is no ambiguity as to who bears the ultimate responsibility of complying with the obligations in the Bill. It is also important that there should be no conflicts with regimes in other countries.

(b) Although the APCC fully understands and supports the need to investigate cybersecurity incidents, it feels that there needs to be more structure and due process around the powers of the Commissioner. The APCC further proposes the implementation of a more collaborative multilateral information sharing information approach rather than a unilateral approach.

(c) The APCC commends the objective of light touch regulation, but is of the view that the proposals for a licensing regime are inconsistent with that approach. The APCC believes that concerns in relation to the regulation of cybersecurity service providers can be better met by the CSA's recognition and acceptance of internationally accepted standards and accreditation regimes.