REPORT ON PUBLIC CONSULTATION ON THE DRAFT CYBERSECURITY BILL

Issued by the Ministry of Communications and Information
and the Cyber Security Agency of Singapore

13 November 2017

1 The Ministry of Communications and Information (MCI) and the Cyber Security Agency of Singapore (CSA) held a public consultation exercise on the draft Cybersecurity Bill (the "Bill") from 10 July to 24 August 2017. The purpose of the Bill is to establish a framework for the oversight and maintenance of cybersecurity in Singapore.

2 The original submission deadline of 3 August 2017 was extended in response to public requests for more time to provide feedback. A wide range of stakeholders responded to the six-week public consultation exercise. Respondents included members of the public, local and international organisations, academia, as well as industry and professional associations. During this period, CSA participated in dialogues with industry organisations, and attended clarification sessions organised by professional associations to address queries regarding the Bill. Prior to this public consultation exercise, MCI and CSA also held several rounds of closed-door consultations with key stakeholders, including those from the 11 critical information infrastructure (CII) sectors[1], industry associations, and cybersecurity professionals.

Overview of Feedback Received

3 In total, we received 92 submissions. Of these, 17 submissions originated from organisations or individuals that provided input through their legal representative or affiliated associations. The list of respondents to the Bill is in **ANNEX A**.

4 Respondents were generally supportive of the Bill. They shared the Government's concerns on cyber threats and the impact of cyber-attacks on Singapore. They acknowledged the importance of the Bill in providing the necessary legislative framework to protect CIIs better, and give CSA the legislative powers to act on cybersecurity incidents that impact the nation. Several respondents also agreed with the importance of sharing cybersecurity information between CSA and other organisations, and of safeguarding the sources and information disclosed.

5 However, several respondents expressed reservations with the proposed licensing framework. They felt that the requirements to be imposed on businesses should not be too onerous. Several suggested simplifying the licensing framework, or making it voluntary, e.g. through an accreditation regime.

[1] The CII sectors are: air aviation, banking and finance, energy, government, healthcare, land transport, media, maritime, security and emergency, infocomm, and water.

Response to Feedback in Specific Areas

(i) Administration

6 Duties of Commissioner and Assistant Commissioners. Many respondents had concerns about how the Bill would be implemented vis-à-vis existing sectoral requirements, such as whether there would be duplicated reporting to the Commissioner and sector regulators, or whether the Commissioner might issue instructions that potentially conflict with those from sector regulators. The Commissioner of Cybersecurity will be given powers necessary for his duties and functions[2] under S5 of the Bill. To assist the Commissioner in discharging his functions, Assistant Commissioners may be appointed by the Minister-in-charge of Cybersecurity. The policy intent is to appoint Assistant Commissioners from the sector regulators to oversee CIIs and CII owners only within their respective sectors. The Bill will empower the Assistant Commissioners and the Commissioner will be working through them to improve the cybersecurity of CIIs in their respective sectors. The CII owners will interact with their sector regulators for requirements under the Bill as the CII owners will already be familiar with the sector regulators for any existing sectoral regulatory requirements, and this arrangement prevents the CII owners from having to report to yet another regulator. The Commissioner will have direct oversight of CIIs owned by the government.

(ii) Regulation of CIIs

7 Designation of CIIs. Several respondents sought clarifications regarding the designation of CIIs. For instance, several felt that the proposed definition of CIIs was too broad and asked for more clarity on the scope of "computers" and "computer systems" that might be designated as CIIs. We wish to clarify that this definition is intended to formalise our existing engagements with CII stakeholders, based on a working definition of CIIs which has been in place since 2013. We have already held initial consultations with the sector regulators and potential CII owners, and will engage any new potential CII owners before they are formally designated. We also wish to clarify that computer systems in the supply chain supporting the operation of a CII will not be designated as CIIs.

8 Several respondents also recognised that Singapore offices of multinational organisations may be supported by infrastructure located wholly outside Singapore. They suggested that such computers and computer systems located wholly outside Singapore should not be designated as CIIs due to potential conflicts with other countries' regulatory regimes. We wish to clarify that we do not currently intend to designate computers and computer systems located wholly overseas as CIIs.

9 Identification of CII owners. Several respondents suggested that the Bill be clearer on who would be identified as CII owners, given that there could be scenarios whereby more than

[2] These include the proactive protection of CIIs, monitoring of and response to cybersecurity threats and incidents that have impact at a national level, and development and promotion of the cybersecurity industry in Singapore.

one party could fulfil the definition of a CII owner for the same CII, e.g. in outsourced business operations. We intend to identify as CII owners only those entities which have effective control over the CII or are responsible for the CII, and this would be the legal owner of the CII asset in most cases. In some situations, there may be more than one such entity, and the Commissioner would need to be able to identify all such owners. We intend to review the definition of CII owners in the Bill to take such situations into account.

10 Several respondents suggested that third-party vendors should also be held responsible for the protection of CIIs. We wish to state that CII owners are ultimately responsible for the cybersecurity of their CIIs. If need be, CII owners can impose cybersecurity requirements contractually on their vendors. As explained in paragraph 7, computer systems in the supply chain supporting the operation of a CII will not be designated as CIIs, therefore third-party vendors will not be considered as owners of the CII.

11 There was feedback regarding the practicality of classifying the designation of a computer or computer system as a CII as an official secret, under the Official Secrets Act (OSA). There would be practical difficulties for CII owners to maintain the confidentiality of their designations as CIIs. For example, CII owners may need to reveal the designation to their customers or vendors, or when communicating to staff outside the Singapore office in the case of international organisations. Some also gave feedback that it was unclear whether all or only several employees of a CII owner would be bound by the OSA. We acknowledge the practical challenges raised and will no longer require that CII designations be deemed as official secrets under the OSA. Instead of maintaining the confidentiality of CII designations, it would be more important to ensure that the technical and operational details of each CII are kept confidential. This would minimise constraints that could impede CII owners from fulfilling their obligations.

(iii) Duties of CII Owners

12 Compliance with statutory requirements. Several respondents commented that CII owners should be given sufficient time to implement measures to ensure compliance with the Bill, and they should not be penalised if there were legitimate grounds for failure to comply with the obligations. We agree that it is prudent to give CII owners sufficient time to comply with the obligations after the Act comes into force. The grace period will be determined in consultation with the Assistant Commissioners to take into consideration the unique complexities in each CII sector. In addition, CSA will implement on-boarding programmes to help sector regulators assist CII owners in getting ready for the Bill. We will also revise the Bill such that penalties in Parts 3 and 4 will be imposed only for wilful non-compliance with the requirements under the Bill without reasonable excuse.

13 Existing codes and standards, and international practices. Respondents suggested that any codes of practices and standards of performance required under the Bill should take into consideration any existing codes and standards that CII owners were already required to comply with, e.g. sectoral regulations, in order to avoid inconsistencies and confusion. In addition, respondents gave feedback that any standards or codes of practice issued or

approved under the Bill ought to be aligned with globally compatible policies and benchmarks, to avoid additional cost and bureaucracy for CII owners. We fully agree that we should not subject CII owners to inconsistent or unnecessary requirements. We will work closely with sector regulators to streamline and harmonise the obligations of CII owners under the Bill with their respective sectoral regulations, code of practices and standards. The appointment of Assistant Commissioners to oversee CIIs in each sector will ensure that the Bill requirements are sensible and take into account existing sector-specific requirements, including international requirements. This is because the sector regulators understand the unique contexts and complexities in each sector, and are in a good position to balance the sectors' cybersecurity needs and business requirements. Where applicable, internationally-recognised policies and standards will be referenced when establishing cybersecurity codes of practice and standards of performance.

14 Audits and risk assessments. There was feedback that the requirement for audits and risk assessments to be conducted at least once every three years was inadequate given the pace of technological change and the dynamic nature of the cybersecurity threat landscape. Also, there was feedback to allow more flexibility to determine the audit and risk assessment requirements, given that the cybersecurity threat would differ across sectors. In view of the fast evolving cyber threat landscape, we will consider increasing the minimum required frequency for audits and risk assessments to ensure that the objectives of the Bill can be met. Sectors will also be allowed to conduct audits and risk assessments at a higher frequency as may be required in the sectoral regulations. Some also suggested that Government should consider implementing grants to help organisations offset compliance cost. We will work with the sector regulators to streamline requirements, to minimise additional compliance costs imposed on companies arising from the Bill. However, MCI/CSA will not provide grants to offset the costs of audits and risk assessments, which are a regulatory requirement.

15 Detection of cyber threats and incidents. There were concerns that the requirement for CII owners to "*establish mechanisms and processes as may be necessary in order to detect any cybersecurity threats …*" in S15(2) appeared overly onerous given the wide range of cyber threats and difficulty in detecting them all. Also, respondents sought further clarity on the definition of a "*significant cybersecurity incident*" as stipulated under S15 of the Bill, especially since it would be a criminal offence to contravene S15(1). We acknowledge the concerns raised and will revise the language of S15 such that CII owners will be required to establish reasonable mechanisms and processes to detect cybersecurity threats and incidents. CSA will also introduce additional guidelines on the reporting of cybersecurity incidents for CII owners, including specific thresholds.

16 Reporting on change in ownership. Several respondents highlighted that it would be impractical to require CII owners to inform the Commissioner of any intended change in ownership of the CII, not later than 90 days before the date of the intended change in ownership. For instance, the CII owner (within the meaning of the Bill) might not have knowledge of the legal owner(s) of the CII, nor would the former typically have visibility of divestments before they occur. Also, such divestment transactions are typically kept strictly

confidential due to market sensitivities and the intended change in ownership date could be difficult to foresee. Furthermore, since the requirement was to inform the Commissioner rather than to seek approval for the change, respondents suggested that CII owners inform the Commissioner of any change in CII ownership only after the completion of the change. We have reviewed this feedback, and will require CII owners to inform the Commissioner of any change in ownership, not later than 7 days after the change. This ensures that the notification requirement is practical for CII owners while allowing CSA to receive timely information on the ownership and accountability of identified CIIs.

17 Protection from potential liability. On the requirement for CII owners to comply with directions issued by the Commissioner, there was feedback that CII owners should be indemnified against potential liabilities e.g. failure to meet service level agreements as a result of compliance with the Commissioner's directions. We would like to assure that such directions would be both necessary and reasonable since the Commissioner would typically consult closely with sector regulators before issuing directions to CII owners. In cases of emergency, where stronger measures may be required at shorter notice, S24 ("Emergency cybersecurity measures and requirements") already provides indemnity to CII owners should they be directed by Minister to take certain measures or comply with certain requirements.

(iv) Powers to Manage and Respond to Cybersecurity Threats and Incidents

18 The proposed legislative framework would allow the Commissioner of Cybersecurity to investigate cybersecurity threats and incidents, with the intent to: (i) determine their impact or potential impact, (ii) prevent further harm arising from the same incident, and (iii) prevent future cybersecurity incidents arising from the threat or incident. These powers may be exercised with respect to any computer or computer system in Singapore, not only to CIIs. We would like to clarify that the key intent is to provide the Commissioner with calibrated powers to respond to major cybersecurity threats or incidents in Singapore, including large-scale attacks on non-CIIs.

19 Powers of the Commissioner. Several respondents gave feedback that the broad powers of the Commissioner to investigate cybersecurity threats and incidents should be subjected to safeguards. This has consistently been our policy intent as reflected in the Bill. The Bill provides for calibrated powers of investigation, for the prevention and countering of cybersecurity threats, depending on the severity of the threat or incident. The Commissioner's powers over CII owners as well as powers that the Commissioner may invoke and authorise in cases of serious cybersecurity incidents have been specified in the Bill. For instance, as provided in S13(4) of the Bill, the Commissioner must consider the practicality and desirability of written directions issued to CII owners, as well as any representations or objections that are duly made.

20 Additionally, the Commissioner may only authorise the seizure of a computer without consent in the event of a serious cybersecurity threat or incident. Even then, the Bill specifies that any such seizures may only be done after the Commissioner is satisfied that there is no

less disruptive method of achieving the purpose of the investigation. Also, such seizure can only be done after consultation with the owner, and having considered the importance of the computer to the business and operational needs of the owner, that the benefit of seizure outweighs the detriment caused to the owner. Furthermore, the Commissioner has powers to request for information only under specified circumstances, such as to investigate cybersecurity threats and incidents, which in most situations will involve technical information. CSA officers may also be held criminally liable should they misuse such information.

21 Regarding the steps that the Commissioner may require owners of a computer or computer system to take to assist with the investigations, there was feedback that allowing installation of software may pose system reliability issues and could cause unforeseen adverse impact to business. These include endpoint detection and response (EDR) tools, which are necessary and routinely used when responding to cybersecurity incidents. We note respondents' concerns, and intend to notify the system owners and follow appropriate protocols when deploying such investigation tools.

22 Threshold for exercising powers. Some respondents suggested that the Bill include specific severity thresholds for the exercise of investigative powers to provide clarity on the scenarios in which they could be used. We recognise the need to balance operational expediency with proportionate and judicious exercise of power, which are subject to safeguards as explained above. For severe cybersecurity threats or incidents occurring on CII systems, the Commissioner will determine the appropriate measures to take during investigations in consultation with the sector regulator and CII owner.

(v) Framework for the Sharing of Cybersecurity Information

23 The Bill provides the legislative framework for sharing of information with and by CSA specifically for the purpose of CII protection and for investigation of cybersecurity threats and incidents. The Bill also provides protection for such information shared with CSA and the source of such information.

24 Voluntary disclosure of information. Some respondents expressed support for having provisions in the Bill to protect the voluntary disclosure of information to CSA in good faith. We agree that facilitating information sharing will help to improve cybersecurity as timely cyber-threat information can help organisations to identify vulnerabilities and prevent cyber incidents more effectively. The Bill already provides for the protection of informers, such that CSA is not compelled to disclose their identities during criminal proceedings. Beyond the Bill, CSA will also explore implementing administrative arrangements to facilitate and encourage information sharing.

25 Information confidentiality. There was feedback that the Bill should ensure the confidentiality of information shared with CSA either during cybersecurity investigations or as part of CII owners' obligations, so as to reduce the risk of disclosure of sensitive business information, for example intellectual property. We recognise that information obtained

through statutory functions under the Bill could be sensitive in some cases, and S48 (preservation of secrecy) of the Bill provides a mechanism for such information to be marked as confidential and treated with care.

26 Indemnity for complying with information disclosure obligations. Some respondents requested to harmonise the indemnity accorded to parties for complying with information disclosure obligations under S11 (technical information on CII), S16 (audit and risk assessment), S20 (investigate and prevent cybersecurity incidents), S21 (investigate and prevent serious cybersecurity incidents) and S24 (emergency cybersecurity measures) of the Bill. Respondents noted that while the information requested under these provisions could be confidential, e.g. commercially-sensitive data, indemnity had not been consistently accorded in these provisions. We intend to indemnify persons who disclose information, in good faith, as required under the Bill. While the situations in S11, S16, S20, S21 and S24 are all slightly different, we will review the Bill to calibrate the indemnity accorded to parties for complying with information disclosure requirements in good faith.

(vi) Licensing Framework for Cybersecurity Service Providers

27 The earlier proposed licensing framework for cybersecurity service providers involved licensing penetration testing service providers and individuals under an investigative cybersecurity service license, and managed security operations centre (SOC) monitoring services providers under a non-investigative cybersecurity service license. The framework would apply to these providers and individuals serving the Singapore market. In-house provision of cybersecurity services is exempted.

28 Licensing of cybersecurity service providers. Some respondents expressed reservations about the proposed licensing framework and some were against licensing of cybersecurity service providers in any form as they felt that licensing could impact the development of a vibrant cybersecurity ecosystem in Singapore. In addition, there was feedback that it was not clear how the proposed licensing framework would treat the many other forms of cybersecurity service provision in the market, for instance resellers, white hats, cybersecurity risk assessment and audit services, as well as provision of services by companies affiliated to the service buyers.

29 We understand that the cybersecurity industry is evolving rapidly and there is a wide range of cybersecurity services that are of varying levels of intrusiveness and maturity. New and innovative services, products and business models are developing, and we do not wish to curb their development, especially since Singapore's cybersecurity also depends on the presence of a vibrant and innovative supporting ecosystem. Taking into consideration the feedback that has been received, and the need to strike a good balance between industry development and security needs, we are looking at introducing a licensing framework that is more narrowly scoped.

30 At this point, we only intend to license penetration testing and managed SOC monitoring service providers, including resellers of such services. This is because penetration testing and managed SOCs are already mainstream and widely adopted. To allow innovative cybersecurity services to grow, we will not require other types of cybersecurity services to be licensed at this point. We will continue to monitor their development. Similar to the exemption given to in-house penetration testing and managed SOC monitoring services, we do not intend to require organisations to be licensed for providing these services to their affiliated organisations.

31 Licensing of cybersecurity professionals. Some were concerned that licensing of individual penetration testers serving the Singapore market would pose practical difficulties for global cybersecurity service providers who deploy employees from their global centres around the world to deliver time-critical services at short notice. There were also suggestions on how the policy objectives for licensing could be achieved through alternative means such as voluntary accreditation of cybersecurity professionals using internationally-recognised standards.

32 In consideration of the feedback, we intend to do away with the licensing of individual cybersecurity professionals. Consequently, cybersecurity service providers will not be required to hire licensed cybersecurity professionals. To raise the quality of cybersecurity service and further improve the standing of cybersecurity professionals, CSA will continue to work with the industry and professional association partners to establish voluntary accreditation regimes for cybersecurity professionals. The voluntary accreditation regimes will complement the simplified licensing framework for cybersecurity service providers, which will not impose quality requirements as part of the licensing conditions at the onset.

33 Types of licensable services. Some respondents suggested to reconsider the definitions of the two types of licensable cybersecurity services as they were too broad and the proposed differentiation between the types of services might become outdated in the future as cybersecurity services evolve. With the simplified licensing framework, we intend to remove the distinction between "investigative" and "non-investigative" types of licensable services. This will allow the Bill to be more future-proof, and enable it to stay relevant even as cybersecurity services continue to evolve.

34 Operational costs on businesses. Some also commented that the framework would impose an administrative burden on licensable cybersecurity service providers as the duration for which records of services provided must be kept was too long. Some cautioned that the licensing framework should not impose onerous requirements on businesses to avoid raising operational costs. We wish to clarify that we intend to keep licensing fees minimal and requirements simple to minimise the operational costs on businesses. The licensing framework will be light-touch when introduced and will be akin to a registration regime. We do not foresee significant operational costs on businesses. To lighten the administrative requirements on licensable cybersecurity service providers, the duration of service record keeping will be reduced from 5 years to 3 years.

(vii) Framework for Offences and Penalties

35 On the proposed criminal penalties for non-compliance with certain requirements under the Bill, there was feedback that the prospect of imprisonment should be avoided as non-compliance could be unintended, and due to technical reasons such as a lack of time or technical complications. In this regard, we wish to highlight that the offences are for wilful non-compliance with the requirements under the Bill, and not for the occurrence of cybersecurity breaches.

(viii) Implementation Timeline

36 We intend for Parts 3 and 4 of the Bill on CII protection and on responding to and prevention of cybersecurity incidents, and the supporting provisions in Part 1 (Preliminary), Part 2 (Administration) and Part 6 (General) to come into force a few months after, should the Bill be passed in Parliament. This is to allow time for the subsidiary legislations to be finalised and gazetted. However, the simplified licensing framework will not take immediate effect after the Bill is enacted. This is to allow CSA to further consult with stakeholders on the detailed requirements before operationalising the framework to further enhance its practicability for service providers.

Conclusion

37 There was also feedback pertaining to the implementation of the Bill. This includes, for instance, suggestions on the use of maturity models to assess the quality of cybersecurity implementation by CII owners and questions on operational details such as the types of cybersecurity exercises that CII owners would be required to participate in. Respondents also provided suggestions to refine the drafting of specific provisions in the Bill for better clarity. These will be taken into consideration as we refine the Bill and work on subsidiary legislation and supporting administrative processes.

38 We would like to thank our stakeholders and members of the public who provided feedback on the Bill. The feedback has allowed us to identify aspects of the Bill that could be refined or explained more clearly. It has also provided insights that will be useful during implementation.

39 We will continue to work closely with stakeholders in finalising the Bill, which we intend to introduce in Parliament in early 2018.

ANNEX A

LIST OF RESPONDENTS FOR THE PUBLIC CONSULTATION ON THE DRAFT CYBERSECURITY BILL

MCI and CSA received a total of 92 submissions to the public consultation on the proposed draft Cybersecurity Bill that ended on 24 August 2017. Of the submissions, 61 were from companies, 13 were from associations and 18 were from individuals.

Companies	
1. Accenture Pte Ltd	33. PSA Corporation Ltd
2. AdaptiveMobile Security Ltd	34. Pacific Light Power Pte Ltd
3. AIG Asia Pacific Insurance Pte Ltd	35. PricewaterhouseCoopers Risk Services Pte Ltd
4. American Express	36. Quann Asia Pacific Pte Ltd
5. Allen & Gledhill LLP (on behalf of 9 financial institutions)	37. Resolvo Systems Pte Ltd
6. Amazon Web Services	38. RHTLaw Taylor Wessing LLP
7. Baker & McKenzie. Wong & Leow	39. Rabobank Singapore
8. BAE Systems Applied Intelligence	40. RSM Risk Advisory Pte Ltd
9. Banking Computer Services Pte Ltd	41. Shell Eastern Petroleum (Pte) Ltd
10. BW Group Ltd	42. Singapore Airline Group
11. Changi Airport Group	43. Singapore Press Holdings Ltd
12. Clifford Chance Asia	44. Singtel Ltd
13. DLA Piper Hong Kong	45. Siemens Pte Ltd
14. EngieLab Singapore	46. SMRT Corporation Ltd
15. ExxonMobil Asia Pacific Pte Ltd	47. Starhub Ltd
16. FireEye Inc	48. Standard Chartered Bank
17. GlaxoSmithKline plc (GSK)	49. SP Group
18. Hong Leong Finance Ltd	50. Senoko Energy Pte Ltd
19. HP PSS Singapore (Sales) Pte Ltd	51. Swire Pacific Offshore Operations (Pte) Ltd
20. Hunton and Williams LLP	52. Symantec Corporation
21. KPMG LLP	53. TuasSpring Pte Ltd
22. Kaspersky Lab	54. Tuas Power Ltd
23. Maximus International LLC	55. Taylors Vinter Via LLC
24. Microsoft Corporation	56. United Overseas Bank Ltd
25. M1 Ltd	57. WASP Risk Solutions Pte Ltd
26. MediaCorp Pte Ltd	58. WongPartnership LLP
27. Nanyang Business School (Cyber Risk Management project), Nanyang Technological University	59. Wolfe Cyber Security Pte Ltd
28. NCC Group	60. YTL PowerSeraya Ltd
29. NTT Security (Singapore) Pte Ltd	61. Zurich Insurance Company Ltd (Singapore Branch)
30. Norvatis Global Service Center Malaysia	
31. Parkway Pantai Ltd, Singapore Operations	
32. Palo Alto Networks	

Associations	
1. Association of Information Security Professionals 2. The Association of Banks in Singapore 3. Asia Cloud Computing Association 4. Asia Pacific Carriers' Coalition 5. ISACA Singapore Chapter 6. Institute of Singapore Chartered Accountants 7. High Technology Crime Investigation Association (Singapore Chapter) 8. Allen & Gledhill LLP (on behalf of Singapore Corporate Counsel's Association) 9. Singapore International Chamber of Commerce 10. Singapore Infocomm Technology Federation	11. Singapore Computer Society 12. The Law Society of Singapore 13. Joint Submission by the American Chamber of Commerce in Singapore, BSA | The Software Alliance, Coalition of Services Industries, Information Technology Industry Council, US-ASEAN Business Council, U.S. Chamber of Commerce
Individuals	
1. Harris Zane 2. Collin Goh 3. Faith S Leong 4. Henry 5. Kenneth Chia 6. Li 7. Mohamed Noordin Yusuff 8. Sankara Bagham 9. Si WY 10. Yee Yik Wei 11. Harish Pillay 12. Jiahui Wan 13. Anthony Lim	14. R Vittal Raj 15. Yvonne Wong 16. Kevin Koh 17. Tripurari Rai 18. Joint submission by Mahdev Mohan, Alexis Ang, Gillian Seetoh and Shriram Jayakumar (Singapore Management University Scholars and Students of Public International Law and Commercial Dispute Resolution)