Public Consultation Paper on the Draft Cybersecurity Bill

Issued by the Ministry of Communications and Information (MCI) and the Cyber Security Agency of Singapore (CSA)

10 July 2017

Part 1: Introduction

Background

1. Cyber-attacks are increasingly frequent, sophisticated and impactful. Globally, we have seen a surge in the number of cybersecurity incidents, such as ransomware, cyber theft, banking fraud, cyber espionage and disruptions to Internet services. Attacks on critical information infrastructure ("CII") systems that manage utility plants, transportation networks, hospitals and other essential services have become more frequent. Successful attacks may result in disruptions to essential services which could cripple economies and lead to loss of life.

2. Cybersecurity is especially essential for Singapore, as we are a small and highly connected nation. As we become more dependent on info-communications technology in our daily lives, cybersecurity has taken on a much greater significance to our society.

3. Singapore has consistently taken cybersecurity threats seriously and developed timely responses. In April 2015, the Government set up the Cyber Security Agency of Singapore ("CSA"), as the central agency to oversee and coordinate all aspects of cybersecurity for the nation. CSA was established under the aegis of the Prime Minister's Office ("PMO"), and under the administration of the Ministry of Communications and Information ("MCI"). CSA's mandate is to (i) devise and coordinate national cybersecurity strategy and policy development, (ii) carry out both cybersecurity capability development and crisis management across all CII sectors, and (iii) adopt a holistic approach towards managing the cybersecurity of information infrastructure.

The need for cybersecurity legislation

4. Since then, and in light of major cyber incidents globally and locally, it has become clear that Singapore needs a more pro-active approach to cybersecurity, especially for CII. For Singapore to effectively address increasingly sophisticated cyber threats to national cyberspace a new cybersecurity law is needed.

5. This Cybersecurity Bill takes a holistic approach to making Singapore resilient against cyber-attacks, to ensure that we are prepared and can respond effectively and in a timely manner when such attacks happen.

6. The Bill will establish a framework for the oversight and maintenance of national cybersecurity in Singapore, and empower CSA officers to carry out their functions.

7. The Bill has four objectives:

a) To provide a framework for the regulation of CII. This formalises the duties of CII owners in ensuring the cybersecurity of their respective CIIs.

b) To provide CSA with powers to manage and respond to cybersecurity threats and incidents. Section 15A of the current Computer Misuse and Cybersecurity Act ("CMCA") provides some existing powers related to cybersecurity. These will be enhanced within the Cybersecurity Bill, and specific powers will be vested in CSA officers as sitting powers.

c) To establish a framework for the sharing of cybersecurity information with and by CSA, and the protection of such information.

d) To establish a light-touch licensing framework for cybersecurity service providers.

Cybersecurity and Cybercrime

8. In the cyber realm, a distinction can be drawn between cybercrime and cybersecurity.

9. Cybercrime typically refers to two categories of offences. The first category involves traditional, real-world crimes that are committed using a computer. Offences in this category, such as e-commerce scams, are covered by criminal laws such as the Penal Code. The second category involves criminal acts that target computer systems.

Such offences are commonly referred to as "hacking", and are covered by the CMCA – examples include criminal acts like the unauthorised access of computer material. Cybercrime is under the purview of MHA and SPF, with objectives such as identifying and prosecuting the perpetrators of cybercrime.

10. On the other hand, cybersecurity refers to the security of a computer or computer system against unauthorised access or malicious acts, to preserve the availability and integrity of the computer or computer system, or the confidentiality of information stored or processed in the computer or computer system. National cybersecurity matters are under the purview of the CSA. In particular, CSA's objectives are the protection of computers and computer systems, the detection and response to cybersecurity threats and incidents, as well as the recovery from such incidents.

International Developments / Perspectives

11. Various countries have strengthened or are strengthening their legislative frameworks for cybersecurity. Some countries chose to enact an omnibus cybersecurity law (e.g. Germany, Czech Republic). Other countries, particularly those without a central cybersecurity agency, amend multiple laws, which either cover specific sectors (e.g. South Korea) or specific aspects of cybersecurity or emergency preparedness (e.g. Estonia)

12. Generally, cybersecurity legislation in other countries accord authorities with powers in five areas: (i) setting standards, (ii) information sharing, (iii) incident management, (iv) crisis management, and (v) international conduct.

Related laws and regulations

13. There are already some existing cybersecurity laws and regulations in Singapore. Other than the CMCA, the regulators of some CII sectors (such as MAS and IMDA) already have powers to enforce cybersecurity requirements on their licensees. The situation, however, varies greatly from sector to sector, depending on the history, context, operating environment and level of technology adoption in each sector. Some sector agencies regulate primarily on the basis of outcomes – for example, PUB has contractual relationships with water suppliers, but does not have regulatory powers to impose additional conditions on the supply of water, only that certain service conditions are met based on existing contracts.

14. Cybersecurity is also related to personal data protection. The Personal Data Protection Act ("PDPA") requires organisations to make reasonable security arrangements to protect personal data in its possession or under its control (also known as the "protection obligation"). However, cybersecurity is more than personal data, and covers all types of information, as well as the computers and computer systems that store or process such information.

15. MCI/CSA has considered the possibility of introducing cybersecurity requirements and powers in every sector, by amending each sector's legislation. However, this would be a long and tedious process, and it may not achieve the desired outcome of a consistent cybersecurity framework applied across sectors. This approach would also not allow for a common national (as opposed to sectoral) definition of cybersecurity threat and CII. Moreover, CSA would not be able to address cybersecurity threats that happen outside of the critical sectors, even if they affect a wide segment of the public. Hence, MCI/CSA decided to pursue the route of a broader omnibus cybersecurity law.

Past consultations

16. MCI/CSA commenced work on the Bill in late 2015. Since then, we have held several rounds of consultations with key stakeholders, including regulators of our critical sectors, potential CII owners, industry associations, and cybersecurity professionals. This public consultation is an opportunity for all stakeholders to provide formal feedback on the draft Bill, and also for members of the public to understand the Bill, and to surface their concerns.

Part 2: Key Concepts and Principles

Appointments

17. The powers of the Bill shall be vested in a Commissioner of Cybersecurity ("Commissioner"), to be appointed by the Minister-in-charge of Cybersecurity ("Minister"). The position will be held by the Chief Executive of CSA.

18. The Minister may appoint a Deputy Commissioner ("DC"), as well as a number of Assistant Commissioners ("AC"). These ACs will oversee and enforce the protection requirements for CIIs. The role of AC is most appropriately carried out by senior public officers with knowledge of both cybersecurity and sectoral domain issues. The ACs will ensure that reasonable, risk-based requirements are imposed on CII owners, and harmonise any existing sectoral regulations with the Cybersecurity Bill.

19. The Minister may also appoint cybersecurity officers and authorised officers for carrying the Act into effect. These will be public sector officers, primarily from CSA (for cybersecurity officers) and the sector regulators (for authorised officers).

20. The Commissioner may also appoint technical officers if necessary, to aid investigations of cybersecurity incidents when specialised technical knowledge is required.

Key Principles

21. In developing the bill, MCI/CSA has adopted certain key principles:

a) Oversight and maintenance of national cybersecurity. In cybersecurity, we are only as strong as our weakest link. The intention is to have a coordinated national approach and to level up the cybersecurity posture across the critical sectors, which disruptions would adversely impact our society. There should be a common framework across all sectors, so that CIIs can be protected consistently. The Bill adopts a whole-of-government approach by empowering not only CSA officers to investigate cybersecurity threats and incidents, but also officers from sector leads as well.

b) Consistent framework across CII sectors. The Bill recognises that every CII sector is different, in terms of the types of technology used, the nature of relationships between government and the private sector, as well as the current cybersecurity

maturity level of industry players. The framework will be consistently applied across sectors but it has to be flexible, taking into account the unique circumstances of each sector.

c) Proactive approach for CII protection. The Bill will require measures to be taken to enhance the cybersecurity of CIIs before cybersecurity threats and incidents happen, based on the risk profile of each CII and critical sector. This proactive approach will reduce the impact from cybersecurity incidents when they happen.

d) Equal application across publicly and privately owned CIIs. The provisions of the Bill will apply equally to both public and private sectors. Hence, the same duties shall apply to owners of CII in the private sector, in statutory boards and in the Government. The offences and penalties are imposed not to punish those who encounter cybersecurity threats and incidents – since such threats and incidents are inevitable, and different organisations face different types and levels of risk – but rather to ensure compliance with requirements in the bill.

22. MCI and CSA have also continuously engaged key stakeholders in the development of the Bill. Several hundred people across various stakeholder groups have been consulted for their views and concerns. This public consultation continues this engagement.

Part 3: Critical Information Infrastructure

23. A critical information infrastructure ("CII") is a computer or computer system that is necessary for the continuous delivery of essential services which Singapore relies on, the loss or compromise of which will lead to a debilitating impact on national security, defence, foreign relations, economy, public health, public safety or public order of Singapore. The list of essential services shall be set out in a Schedule, and new essential services may be added from time to time by the Minister. Computers and computer systems that are necessary during times of National Emergency may also be designated as CIIs.

24. The government has identified essential services in 11 critical sectors, across utilities, transport and services. These critical sectors are: government, security and emergency, healthcare, telecommunications, banking and finance, energy, water, media, land transport, air transport, and maritime.

25. There is a large variety of CIIs across these 11 sectors. CIIs include both information technology (IT) systems, as well as operational technology (OT) systems such as industrial control systems, programmable logic controllers, supervisory control and data acquisition systems, and distributed control systems. Some sectors, such as banking and finance, have predominantly IT systems, while others such as energy and water have predominantly OT systems. The definition of CII in the Bill is also sufficiently flexible to cover new types of computers and computer systems that may emerge in the future.

Designation of CII

26. Section 7 of the Bill will allow the Commissioner to designate a computer or computer system as a CII. In doing so, the Commissioner will provide written notice to the owner of the computer or computer system ("CII owner"). This owner is deemed as the person who (a) has effective control over the operations of the CII and has the ability and right to carry out changes to the CII; or (b) is responsible for ensuring the continuous functioning of the CII.

27. Prior to designating a CII, it is important for the Commissioner to have sufficient information to determine whether the computer or computer system in question fulfils the criteria of a CII. Hence, the Commissioner may require the owner to provide certain information about the computer or computer system. The types of information that the Commissioner may ask for are set out in Section 8(2). The owner shall not be

obliged to disclose any information if doing so will constitute a breach of any written law.

28. The designation of a computer or computer system as a CII is an official secret under the Official Secrets Act, and shall not be divulged to the public.

29. CII owners may, within 30 days of official designation, appeal against the designation to the Minister-in-charge of cybersecurity, whose decision shall be final.

Duties of CII Owners

30. CII owners shall be responsible for ensuring the cybersecurity of the CIIs that they own. To this end, every CII owner shall be subject to certain statutory duties. These duties are set out in Section 10:

(a) Duty to provide information – i.e. to provide the Commissioner with information on the technical architecture of the critical information infrastructure;

(b) Duty to comply with codes and directions – i.e. to comply with such codes of practice or directions in relation to the CII as may be issued by Commissioner;

(c) Duty to report incidents – i.e. to notify the Commissioner of (i) any cybersecurity incident that occurs in respect of the CII; and (ii) any cybersecurity incident that occurs in respect of any computer or computer system under the owner's control that is interconnected with or communicates with the CII.

(d) Duty to conduct audits – i.e. to cause regular audits of the compliance of the CII with the Act, codes of practice and standards of performance to be carried out by an auditor approved or appointed by the Commissioner;

(e) Duty to conduct risk assessments – i.e. to carry out regular risk assessments of the CII as required by the Commissioner; and

(f) Duty to participate in exercises – i.e. to participate in cybersecurity exercises are required by the Commissioner.

31. The details of these duties are set out in Sections 11 to 17. Administratively and where required, CSA will provide more guidance on how CIIOs may comply with these duties.

32. The offences in this part are criminal offences, and apply to CIIOs in cases where they fail to perform their duties wilfully, or fail to comply with Commissioner's directions without reasonable excuse. CIIOs will not be directly penalised for cybersecurity breaches. These are criminal offences because of the national security implications of non-compliance.

33. While CSA shall strive to consult CIIOs before implementing codes of practice and directions, this may not always be possible. CIIOs may appeal to the Minister, who may be advised by an appeals advisory panel if the appeal is of a technical nature.

34. CIIs may be owned by either the public or private sector. The duties, offences and penalties pertaining to CII owners shall apply equally regardless whether the CII is owned by a private entity, or a statutory board, or the government. This will ensure that all CIIs in Singapore are protected consistently.

Assistant Commissioner

35. Today, CSA works with government lead agencies in charge of each sector – these are known as "Sector Leads". Such Sector Leads play an important role – they balance between the sector's cybersecurity needs and the sector's business requirements. Sector Leads understand the unique contexts and circumstances in each sector.

36. Under the Bill, the Minister may appoint Assistant Commissioners to assist the Commissioner in oversee the cybersecurity of CIIs, for example, by enforcing the duties of CIIOs. These Assistant Commissioners will, in most cases, come from the Sector Leads. Because the CIIOs would already be familiar with the Assistant Commissioners for existing regulatory requirements. This arrangement prevents the CIIOs from having to report to yet another regulator. CSA will work with Sector Leads to harmonise regulations in each sector.

Part 4: Response to cybersecurity threats and incidents

37. Singapore is a highly connected country, and cybersecurity threats and incidents occur on a daily basis. While most of these threats and incidents are not major and do not have serious consequences, there are some which will be quite serious, and have a real risk of affecting CIIs, Singapore's national security, or a large number of computers and people across Singapore.

38. CSA's mandate is to prevent and respond to cybersecurity threats and incidents at the national level. While the owner of each computer should be responsible for ensuring that the computer is well-protected, CSA's interest is in ensuring that cybersecurity threats and incidents are contained, and do not develop into more serious consequences.

39. Hence, should the Commissioner learn of a cybersecurity threat or cyber incident, he may choose to investigate the threat or incident. The objectives of the investigations would be to: (i) to determine the impact or potential impact of the threat or incident, (ii) to prevent further harm from arising from the same incident, and (iii) to prevent further cybersecurity incidents from arising from the threat or incident.

40. Given that cybersecurity threats and cyber incidents have the potential to develop quickly, it is essential that CSA officers have the necessary powers to conduct investigations effectively on the ground. Hence, the proposal is for the Commissioner to have certain sitting powers, and these powers may be delegated to Assistant Commissioners, cybersecurity officers and authorised officers. These powers may be exercised in respect of any computer or computer system in Singapore, not only CIIs.

Powers to investigate cybersecurity threats and incidents

41. The level of intrusiveness of powers that may be exercised will depend on the severity of the situation. There are three proposed scenarios for the exercise of power:

a) **All cybersecurity threats and incidents** – Under Section 20, if the Commissioner has information regarding a cybersecurity threat or incident, the Commissioner may examine anyone relevant to the investigation and take statements, and require the provision of relevant information. Such information will typically be in the form of technical logs. This will also allow the Commissioner to decide whether the threat or incident is serious and therefore take further action. To facilitate the provision of information, a person examined under this section who, in good faith, discloses any information to an

investigating officer shall not be treated as being in breach of any restriction upon the disclosure of information imposed by law, contract or rules of professional conduct.

b) **Serious cybersecurity threats and incidents** – Under Section 21, the Commissioner may exercise more intrusive measures, in addition to the information requisition measures under s20. These include directing persons to carry out remedial measures and assist in the investigation, enter premises where relevant computers and computer systems are located, access such computers, and scan computers for cybersecurity vulnerabilities. The Commissioner may also seize any computer or equipment for the purpose of carrying out further examination and analysis, if certain conditions are met: that doing so is necessary for the investigation, there is no less disruptive way of achieving the investigation's purposes, and the Commissioner is of the view that the benefit from doing so outweighs the detriment caused to the owner of the computer system (after consultation with the owner).

c) **Emergency measures and requirements** – In addition, under Section 24, the Minister may (by issuing a certificate) authorise any person or organisation to take such measures or comply with such requirements as may be necessary to prevent, detect, counter any threat to a computer or computer service, or any class of computers or computer services. These powers are adapted from Section 15A of the CMCA.

42. Based on Section 21(2), a cybersecurity threat or incident is deemed serious if it meets any of the criteria below:

a) It creates a real risk of significant harm being caused to a CII.

b) It creates a real risk of disruption being caused to the delivery of an essential service.

c) It creates a real threat to the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore.

d) The cybersecurity threat is of a severe nature, in terms of the severity of harm that may be caused or the number of computers or value of information put at risk, whether or not the computers or computer systems put at risk are of the nature of a critical information infrastructure.

43. There will be an internal governance process within CSA to ensure that the powers are exercised responsibly and in accordance with the Bill, and only by qualified persons. There will be a pre-authorised list of officers who may exercise these powers, and these officers will have to complete necessary training. Public officers from Sector Lead agencies may also be empowered as authorised officers, as they may have domain expertise and knowledge of specific systems in each sector. Such officers will also be subject to CSA's control.

Penalties

44. The maximum penalty for Section 20 ("all cybersecurity threats and incidents") is lower than that for Section 21 ("serious cybersecurity threats and incidents"). For the former, this is proposed to be $5,000 or imprisonment for a term not exceeding 6 months; for the latter, this is proposed to be $25,000 or imprisonment for a term not exceeding 2 years.

45. In many cases, the people that CSA will be dealing with during cybersecurity threats and incidents will likely be the "victims" – these are the owners of computer systems that have been compromised. The penalties are not intended to penalize these owners for cybersecurity breaches. Rather, the penalties will be levied only in cases of wilful non-compliance of instructions or wilful refusal to provide information.

Technical Experts

46. The Bill will also provide for the Commissioner to appoint technical experts to assist in investigations. Such technical experts may be from either public or private sectors, as long as they have suitable qualifications or experience. This is necessary in situations where CSA is unfamiliar with the computer system in question – for example, in cases of niche Industrial Control Systems in particular sectors. In such cases, the technical experts would assist the investigating officer in the investigation.

Part 5: Regulation of cybersecurity service providers

47. As cybersecurity risks become more widespread, the need for credible cybersecurity services is growing. Even as CSA continues to raise awareness and encourage adoption of cybersecurity services through other means, CSA has identified three considerations for cybersecurity services that will need to be addressed over time:

a) Improve assurance on security and safety: Some cybersecurity services can be sensitive because the service providers performing them can have significant access into clients' computer systems and networks. They may gain a deep understanding of the cybersecurity posture and vulnerabilities of the client and its operations. Such services, if abused, can compromise and disrupt the client's operations even after the service provider's job has been completed. Hence, it is important that the providers of some cybersecurity services be held to requirements or ethics that improves the assurance to customers on the security and safety of cybersecurity services being provided.

b) Raise quality and appreciation for it: If services are carried out by incompetent or substandard service providers, systems will be vulnerable or damaged or suffer loss of information. This can also endanger other computer systems. Given this negative externality caused by incompetent or substandard service providers, there may be a need, over time, to ensure that cybersecurity service providers and professionals meet baseline quality requirements or certifications. Buyers will also need to appreciate the need for competent services. This would be in line with the broader objective of developing a vibrant cybersecurity ecosystem in Singapore. It will ensure a sustainable source of expertise and solutions to support our plans for a resilient national infrastructure and a safer cyberspace, as part of Singapore's Cybersecurity Strategy. This will also go a long way in attracting and anchoring advanced cybersecurity capabilities in Singapore.

c) Address information asymmetry: The complexities of a technical and evolving but important area like cybersecurity can give rise to the problem of information asymmetry in the market. Buyers may not have expert knowledge, and may not know which cybersecurity service providers are ethical or of good quality. This is especially true for smaller buyers who do not have in-house cybersecurity expertise. This information asymmetry can create a situation where buyers do not end up with appropriate cybersecurity services from credible service buyers for their risks and budget. Hence, one objective is to help organisations identify credible service buyers, and increase demand for such services.

48. Therefore, as part of the Bill, MCI/CSA is proposing to introduce a light-touch licensing regime for cybersecurity service providers that service the Singapore market, and to also improve the standing of cybersecurity professionals. As this is a technical and evolving area, the list of licensable cybersecurity service providers will be set out in a Schedule to the Act that Minister may amend, instead of directly specifying them within primary legislation.

49. There are two types of licenses:

a) Investigative Cybersecurity Service: cybersecurity service that is investigative in nature and (i) involves circumventing the controls implemented in another person's computer or computer system; or (ii) requires the person performing the service to obtain a deep level of access to the computer or computer system in respect of which the service is being performed, or to test the cybersecurity defences of the computer or computer system, thereby giving rise to a potential for significant harm to be caused to the computer or computer system. For example, searching for or exploiting cybersecurity vulnerabilities in the computer or computer system of another person for the purpose of improving the cybersecurity of the computer or computer system.

b) Non-Investigative Cybersecurity Service: cybersecurity service that is not of investigative nature. For example monitoring of the cybersecurity of a computer or computer system of another person or assessing or monitoring of the compliance of an organisation's cybersecurity policy.

50. To start, CSA is proposing to license 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.

51. In-house provision of cybersecurity services will be exempted from having to obtain a license.

Requirements

52. The Bill will assist to address concerns about improving assurance on security and safety and improve information asymmetry.

53. Licensed service providers (both investigative and non-investigative) will need to meet certain basic requirements:

a) Requirement for key executive officers to be fit and proper persons.

b) The criteria for considering whether a person is fit and proper includes, but isn't limited to, honesty, integrity and financial soundness

c) Retention of service records for five years (e.g. client information, service provided, name of employee who provided the service).

d) Compliance with a Code of Ethics (e.g. maintaining confidentiality about client information).

e) Requirement for a process in place to ensure that employees performing the licensable services are fit and proper.

54. In addition, licensed individuals (under investigative cybersecurity service license) will need to be fit and proper persons, and comply with a Code of Ethics.

Other considerations

55. The intent is to keep licensing requirements and registration procedures as simple as possible. Hence, license applications will be submitted and processed online, and service providers with established track records will be granted longer license terms. CSA will conduct audits from time to time, to ensure that licensing requirements are met. CSA will also want to keep license fees low.

56. CSA recognises that there are overseas cybersecurity service providers in the Singapore market. The same licensing requirements will apply to such overseas providers. The intent is to ensure that there is as much as possible a level playing field between local and overseas service providers.

57. CSA may impose future requirements as necessary, with consultations. This could include, for example, a requirement for service providers to have professional insurance, or for individuals to have minimum competency requirements or certifications. This will assist to raise quality of service, and further improve the standing of cybersecurity professionals, when the industry and market are more ready. As far as possible, international standards and guidelines will be introduced.

58. The licensing framework will not take immediate effect, and CSA will have further consultation with the industry on detailed requirements before the framework is operationalised.

Part 7: Procedures and timeframe for submitting comments

59. MCI/CSA would like to seek views and comments from the industry and members of the public on the draft Cybersecurity Bill, and on the above issues and questions. Please note that the draft bill is still in the midst of development and some provisions will be further scoped or refined, based on feedback received during this consultation.

60. All submissions should be clearly and concisely written, and should provide a reasoned explanation for any proposed revisions. Where feasible, please identify the specific provision of the draft bill on which you are commenting, and explain the basis for your proposals.

61. All submissions should reach MCI/CSA no later than **5pm on 3 August 2017**. Late submissions will not be considered.

62. Submissions are to be in softcopy only (in Microsoft Word or PDF format). Please send your submissions to **csa_cs_bill_feedback@csa.gov.sg**, with the subject "**Public Consultation for the Cybersecurity Bill**".

63. MCI/CSA reserves the right to make public all or parts of any written submission and to disclose the identity of the source. Respondents may request confidential treatment for any part of the submission that the respondent believes to be proprietary, confidential or commercially sensitive. Any such information should be clearly marked and placed in a separate annex. Respondents are also required to substantiate with reasons any request for confidential treatment. If MCI/CSA grants confidential treatment, it will consider, but will not publicly disclose, the information. If MCI/CSA rejects the request for confidential treatment, it will return the information to the respondent that it submitted, and will not consider this information as part of its review. As far as possible, respondents should limit any request for confidential treatment of information submitted. MCI/CSA will not accept any submission that requests confidential treatment of all, or a substantial part, of the submission.