PUBLIC CONSULTATION PAPER ISSUED BY
THE CYBER SECURITY AGENCY OF SINGAPORE
(THE MINISTRY OF COMMUNICATIONS AND INFORMATION)

DRAFT CYBERSECURITY (AMENDMENT) BILL

15 DEC 2023

CHAPTER I. INTRODUCTION

Impetus for the review of the Cybersecurity Act 2018

1. Singapore's digitalisation efforts have progressed rapidly, and Singapore is now one of the most digitally connected countries in the world. In the past five years, our connectivity, computing, and data storage needs have grown significantly, which in turn, has increased our attack surfaces and made us more vulnerable to cyber attacks. This first review of the Cybersecurity Act 2018 ("the Act") seeks to update the Act so that it keeps pace with developments in our cyber threat landscape and business environment, so that we can continue to secure Singapore's cyberspace and safeguard our digital way of life.

Past Consultations

2. Since the commencement of this review of the Act in 2021, CSA has held several rounds of consultations with key stakeholders, including providers of essential services and their regulators, operators of CII, industry players, as well as cybersecurity experts and professionals. This public consultation is intended as an opportunity for all interested parties to provide formal feedback on the draft Bill, if any.

CHAPTER II. CRITICAL INFORMATION INFRASTRUCTURE (CII)

3. CII are computers or computer systems that are necessary for the continuous delivery of essential services in Singapore. The compromise or disruption of such computers or computer systems could pose severe threats to our national security and survival. Therefore, in the first iteration of the Act in 2018, we had established a framework to protect and safeguard the cybersecurity of Singapore's CII, and this culminated in Part 3 of the Act. The framework established under Part 3 of the Act has worked well over the past five years; CSA has established a close partnership with the providers of essential services and the regulators of the essential service sectors to secure our CII.

4. Since 2018, the technological and business contexts for the delivery of essential services have changed. Advances in virtual computing and the availability of a wider and more sophisticated range of computing services today have unlocked greater business efficiency and service quality. The review aims to facilitate these developments, while ensuring that cybersecurity outcomes are not compromised. The review also seeks to address feedback that CSA has received from those who own or operate CII, for improved operationalisation of the provisions governing the cybersecurity of our CII.

Facilitating virtualisation and new business models

5. As a matter of policy, CSA agrees that where the use of virtual computers or the use of vendors that can meet specific computing needs ("computing vendors") to improve a provider's ability to provide essential services ("providers of essential services") to Singaporeans, such use should be facilitated. However, such providers of essential services and CSA must work together to ensure that cybersecurity outcomes are not compromised. To achieve this, CSA will seek amendments to the Act to account for such circumstances, where necessary.

6. Under the current Part 3 of the Act, the duties in relation to the CII are imposed on the owners of the CII at the first instance. At the time the Act was enacted, providers of essential services tended to own and control the CII used for the continuous delivery of the essential services they were responsible for.

7. To facilitate the new business models involving the use of computing, CSA is proposing a new Part 3A to the Act to facilitate the use of computing vendors. However, the responsibility for the cybersecurity of the essential service must still, ultimately, rest with the provider of essential service. The proposed new Part 3A will allow the Commissioner to subject such providers of essential services to duties that are designed to ensure that the same cybersecurity outcomes that Part 3 was designed to bring about will continue to hold even if they chose to make use of such non-provider-owned CII from a computing vendor. These include duties to:

(a) Provide the Commissioner with information on the non-provider[1]-owned CII;

[1] "Provider" in this instance refers to the provider of the essential service.

(b) Comply with such codes of practice, standards of performance or written directions in relation to providers responsible for the non-provider-owned CII as may be issued by the Commissioner;

(c) Notify the Commissioner of any change in the beneficial or legal ownership of the non-provider-owned CII;

(d) Notify the Commissioner of any prescribed cybersecurity incident involving the non-provider-owned CII (specific details set out in the Incident Reporting section below);

(e) Cause regular audits of the compliance of the non-provider-owned CII with the Act, codes of practice and standards of performance, to be carried out by an auditor approved by the Commissioner;

(f) Cause regular risk assessments of the non-provider-owned CII to be carried out; and

(g) Participate in cybersecurity exercises relating to the providers responsible for non-provider-owned CII as required by the Commissioner.

8. Under the proposed Part 3A, the provider of essential services will be required to obtain legally binding commitments from their computing vendor to ensure that the provider of the essential service is able to discharge its duties under the Act. In the event that the provider of the essential service fails to obtain the required commitments from the computing vendor, the Commissioner may order the provider of the essential service to cease the use of the non-provider-owned CII.

9. Part 3A will not apply to any computer or computer system for which a designation under Section 7 of the Act is in effect. If the Bill is passed, CSA will work closely with stakeholders to implement Part 3A.

Incident reporting

10. Every digital connection presents a possible surface for attack. In recent years, CSA has observed that sophisticated threat actors will take advantage of innocuous connections to peripheral systems and supply chains to gain access to targeted networks. CSA's situational awareness of the threats to our essential services is paramount, as it allows CSA to take expedient and proactive action to secure Singapore, and pre-empt or minimize risks of potential disruptions to our essential services.

11. The Act currently requires persons with duties under Part 3 to report only (a) prescribed cybersecurity incidents in respect of the provider-owned CII; (b) prescribed cybersecurity incidents in respect of any computer or computer systems under the provider-owner's control that is interconnected with or that communicates with the provider-owned CII; and (c) any other type of cybersecurity incident in respect of the provider-owned CII that the Commissioner has specified by written direction to the owner. To enhance CSA's

situational awareness, CSA proposes to expand the types of incidents to be reported to the Commissioner and include:

(a) Prescribed cybersecurity incidents in respect of any other computer or computer system under the owner's control that does not fall within Section 14(1)(b) of the Cybersecurity Act; and

(b) Prescribed cybersecurity incidents in respect of any computers or computer systems under the control of a supplier to the owner that is interconnected or communicates with the provider-owned CII.

12. CSA also proposes that persons with duties under Part 3A be required to report the following:

(a) Prescribed cybersecurity incident in respect of the non-provider-owned CII;

(b) Prescribed cybersecurity incident in respect of any computer or computer system under the owner's control, or the provider's control that is interconnected with or that communicates with the non-provider-owned CII.

(c) Prescribed cybersecurity incident in respect of any other computer or computer system under the provider of essential services' control that does not fall within paragraph (b); and

(d) Any other type of cybersecurity incident in respect of the non-provider-owned CII that the Commissioner has specified by written direction to the provider responsible for non-provider-owned CII.

13. If the Bill is passed, subsidiary legislation and further administrative guidance will be published to set out the operational details.

Updates to provisions governing CII

14. CSA proposes to make other updates to the provisions governing provider-owned CII to account for feedback provided by persons with duties under Part 3, and to close operational gaps. These include:

(a) Allowing computers or computer systems to be designated provider-owned CII if the criterion set out under Section 7(1)(a) is met, even if the computer system is located wholly overseas. This is to ensure that providers of essential services located in Singapore cannot avoid their duties under Part 3 by seeking to offshore their CII.

(b) Allowing the Commissioner to grant a time extension to a designation made under Section 7(1) before the expiry of the designation. Where a service continues to be essential, and the computing infrastructure supporting it does not change, this will facilitate continuity in the Commissioner's oversight of the provider-owned CII. The Commissioner will also be granted similar powers to

extend the designation of a provider of essential services responsible for the non-provider-owned CII under the new Part 3A.

(c) Granting the Commissioner the power to authorise the conduct of on-site inspections of provider-owned CII located in Singapore. This seeks to facilitate the Commissioner's supervisory duties over provider-owned CII where it appears to the Commissioner that a person with duties under Part 3 has not complied with a provision of the Act, an applicable code of practice or standard of performance, or has provided information (under Section 10 of the Act) that is false, misleading, inaccurate or incomplete.

(d) Allow the Commissioner to grant time extensions to persons with duties under Part 3 and Part 3A. During the COVID-19 pandemic, some owners of provider-owned CII with duties under Part 3 were unable to meet the timelines for conducting audits due to the strict safety measures imposed. CSA has heard this feedback and proposes to allow the Commissioner to grant time extensions for the performance of statutory duties a person responsible for the cybersecurity of a CII (regardless of whether it is provider-owned or non-provider-owned) is required to do under Part 3 and Part 3A, if the Commissioner is satisfied that there are good reasons to do so.

CHAPTER III: FOUNDATIONAL DIGITAL INFRASTRUCTURE (FDI)

15. In a country as digitally connected as Singapore, a significant proportion of our work and lives takes place in the digital domain, and our ability to function has become increasingly dependent on the good functioning of the digital infrastructure that underpins this connectivity. Even if they are not considered CII today, digital infrastructure[2] is growing in importance due to the foundational role they play in our technological stacks.

16. The digital infrastructure we rely on is an attractive target for malicious actors because vulnerabilities within can be exploited to reach many other systems, or to gain unauthorised access to systems for operations. Disruptions to the functioning of digital infrastructure can also have a significant impact, given the potentially pervasive knock-on impact on the services that rely on them. There is therefore a need to ensure that the digital infrastructure that Singaporeans rely on, beyond those that are already designated as CII, is secure.

17. In light of the above, CSA's position is that major providers of digital infrastructure that provide infrastructural services of a foundational nature ("foundational digital infrastructure" or "FDI") should bear the responsibility for ensuring the cybersecurity and resilience of the FDI service they provide. As the Government's national cybersecurity authority, CSA seeks to ensure that appropriate cybersecurity safeguards are in place.

18. In this review, CSA seeks to achieve the following two policy objectives in relation to foundational digital infrastructure:

(a) To enhance CSA's situational awareness of prescribed cybersecurity threats and incidents targeting FDI; and

(b) To ensure that an adequate level of cybersecurity is met in relation to FDI.

Identification of FDI and Major FDI Service Providers

19. CSA proposes to introduce a new Part 3B to empower:

(a) The Minister to specify the types of services that would be regulated as FDI services in a new Third Schedule to the Act, provided that the service is one that promotes the availability, latency, throughput or security of digital services;

(b) The Commissioner to designate a provider of FDI services as a major FDI service provider, if the Commissioner is satisfied that the FDI service provider provides an FDI service to or from Singapore, and the impairment or loss of the provision of the FDI service could lead to or cause disruption to a large number of businesses or organisations that rely on or are enabled by the FDI service. This

[2] Digital infrastructure comprises the physical components that house or carry data (e.g. data centres, internet exchanges), as well as virtualised infrastructure that provide important services that support the digital domain (e.g. Domain Name System, cloud services, content delivery networks).

reflects CSA's risk-based approach, i.e., focusing on providers of FDI that, if targeted by a cyber-attack, could have widespread and significant impact on users of the FDI service. Providers that do not agree with the Commissioner's decision would be able to appeal against the designation to the Minister within 30 days of the designation.

(c) The Commissioner to grant a time extension to the designation of a major FDI service provider before the expiry of the designation if the Commissioner is of the opinion that the designation criteria continue to be fulfilled.

(d) The Commissioner to withdraw the designation of a major FDI service provider if the Commissioner is of the opinion that the designation criteria is no longer fulfilled.

20. Once designated, a major FDI service provider would be subject to several duties, including duties to:

(a) Provide the Commissioner with information related to the cybersecurity of the major FDI.

(b) Comply with such codes of practice, standards of performance or written directions in relation to the major FDI as may be issued or approved by the Commissioner.

(c) Notify the Commissioner of any prescribed cybersecurity incident.

Incident Reporting

21. To facilitate CSA's situational awareness, CSA proposes to require major FDI service providers to report prescribed cybersecurity incidents in respect of computer systems under the major FDI provider's control, where:

(a) The incident results in a disruption or degradation to the continuous delivery of the FDI service it provides in Singapore; or

(b) The incident has a significant impact on the major FDI provider's business operations in Singapore.

22. Operational details of the incident reporting requirements will be developed in consultation with stakeholders and with reference to international practices. These include, but are not limited to, the list of cybersecurity incidents to be prescribed, the threshold (e.g., significance of an incident) for when a report becomes obligatory, the reporting timelines, and the information to be reported. These details, when finalised, will be set out separately, either in subsidiary legislation or administrative guidelines.

Cybersecurity Standards

23. The proposed amendments will empower the Commissioner to issue or approve codes of practice or standards of performance to ensure that major FDI providers maintain at least a baseline level of cybersecurity. CSA intends to work with industry stakeholders to co-create the standards applicable to each FDI service sector and to lean on the industry's experience and best practices. CSA will also take reference from international standards and practices, and work with other regulators in Singapore to ensure harmonisation, where possible, of cybersecurity standards imposed by the Government on FDI providers seeking to operate from Singapore or serve the Singapore market.

24. Major FDI service providers should take compliance with the code of practice or standard of performance seriously. Where a major FDI service provider fails to comply, the Commissioner may issue a written direction to compel compliance.

Penalty for Non-Compliance

25. If an FDI service were to be disrupted or degraded by a cybersecurity incident, the risks include widespread impact on parties that rely on the FDI service. Therefore, compliance with the cybersecurity duties that CSA intends to set out must be taken seriously. CSA's policy intent is to prescribe financial penalties that are (a) be commensurate with the risks resulting from non-compliance; and (b) be an effective deterrent effect against non-compliance. CSA is studying comparable laws in other jurisdictions that purport to regulate companies that would likely qualify as major FDI providers, as well as comparable statutes under Singapore law, and will set out the proposed penalty provisions in a future version of the Bill.

CHAPTER IV: ENTITIES OF SPECIAL CYBERSECURITY INTEREST (ESCI)

26. There are certain types of entities that are particularly attractive targets of malicious threat actors seeking to compromise a state because of the sensitive data that they possess or the function that they perform. Cyber-attacks on Singapore entities of such a nature could have a significant detrimental effect on the defence, foreign relations, economy public health, public safety, or public order of Singapore.

27. In light of the cybersecurity risks, CSA seeks to achieve the following policy objectives in relation to these entities ("entities of special cybersecurity interest" or "ESCIs"):

(a) To enhance situational awareness of prescribed cybersecurity threats and incidents targeting ESCIs; and

(b) To ensure that ESCIs meet an adequate level of cybersecurity.

Identification of ESCIs

28. CSA therefore proposes to introduce a new Part 3C to empower the Commissioner to:

(a) Designate an entity as an ESCI, if the entity stores sensitive information; or, if the entity uses computers to perform a function which, if disrupted, is likely to have a significant detrimental effect on the defence, foreign relations, economy, public health, public safety, or public order of Singapore. This is in line with taking a risk-based approach to focus on entities that, if targeted by a cyber-attack, could have significant negative impact on Singapore's interests. While designated entities will be notified, the list of designated ESCIs will not be published. Entities that do not agree with the Commissioner's decision would be able to appeal against the designation to the Minister within 30 days of the designation.

(b) Grant a time extension to the designation of an ESCI before the expiry of the designation if the Commissioner is of the opinion that the designation criteria continue to be fulfilled.

(c) Withdraw the designation of an ESCI if the Commissioner is of the opinion that the designation criteria is no longer fulfilled.

29. Once designated, an ESCI would be subject to several duties, including duties to:

(a) Provide the Commissioner with information on the system of special cybersecurity interest.

(b) Comply with such codes of practice, standards of performance or written directions in relation to the system of special cybersecurity interest as may be issued by the Commissioner.

(c) Notify the Commissioner of any prescribed cybersecurity incident.

Incident Reporting

30. To facilitate CSA's situational awareness, CSA proposes to require ESCIs to report prescribed cybersecurity incidents in respect of computer systems under the ESCI's control, where:

(a) The incident results in a breach of the availability, confidentiality or integrity of the ESCI's data; or

(b) The incident has a significant impact on the business operations of the ESCI.

31. Operational details of the incident reporting requirements will be developed in consultation to stakeholders. These include, but are not limited to, the list of cybersecurity incidents to be prescribed, the threshold (e.g., significance of an incident) for when a report becomes obligatory, the reporting timelines, and the information to be reported. These details, when finalised, will be set out separately, either in subsidiary legislation or administrative guidelines.

Cybersecurity Standards

32. The proposed amendments will empower the Commissioner to issue or approve codes of practice or standards of performance to ensure that ESCIs maintain at least a baseline level of cybersecurity with respect to computer systems of special cybersecurity interest. CSA intends to lean on existing cybersecurity standards in setting out any such code of practice or standard of performance, such as the Cyber Trust Mark.

33. ESCIs should take compliance with the code of practice or standard of performance seriously. Where an ESCI fails to comply, the Commissioner may issue a written direction to compel compliance.

Penalty for Non-Compliance

34. If an ESCI were to suffer a cyber-attack, this could result in adverse implications for Singapore. Therefore, compliance with the cybersecurity duties that CSA intends to set out must be taken seriously. CSA's policy intent is to prescribe financial penalties that are (a) commensurate with the risks resulting from non-compliance; and (b) an effective deterrent effect against non-compliance. CSA is studying comparable laws in other jurisdictions that purport to regulate companies that would likely qualify as ESCI, as well as comparable statutes under Singapore law, and will set out the proposed penalty provisions in a future version of the Bill.

CHAPTER V: SYSTEMS OF TEMPORARY CYBERSECURITY CONCERN (STCC)

35. There have been and will be times when a computer or computer system is critical to Singapore for a time-limited period, and for that period, are at high risk of cyber-attacks. Examples include systems that are set up specifically to support high-key international events in Singapore (e.g., the World Economic Forum), or systems set up to support the distribution of vaccines during the COVID-19 pandemic.

36. It is important to ensure the cybersecurity of these systems during these critical periods. However, given that they are critical to Singapore for a time-limited period and the contexts in which they are used, regulating these systems in the same way we do with CII would be unduly burdensome and could frustrate the time-sensitive objectives that these systems serve. To achieve this, CSA proposes to introduce a new Part 3D within the Act to allow the Commissioner to designate these systems and impose duties on the persons responsible for such STCC in order to:

(a) Enhance CSA's situational awareness of the cybersecurity threats and incidents targeting the STCC;

(b) Ensure that appropriate cybersecurity measures are taken to secure these STCC.

Identification of STCCs

37. In line with the risk-based approach CSA takes towards cybersecurity regulation, CSA intends to focus only on the most critical of such systems. CSA proposes to introduce a new Part 3D to empower the Commissioner to:

(a) Designate a computer or computer system (located wholly or partly in Singapore) as an STCC for a period of no more than one year, if the Commissioner is satisfied that that the risk of a cyber-attack on the computer or computer system is high and the loss or compromise of the computer or computer system will have a serious detrimental effect on the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore. Owners of designated STCC that do not agree with the Commissioner's decision may appeal against the designation to the Minister within 30 days of the designation.

(b) Grant a time extension to a designation of an STCC before the expiry of the designation if the Commissioner is of the opinion that the designation criteria continue to be fulfilled. Each extension must be for a period that does not exceed 1 year, starting from the expiry of the earlier designation.

(c) Withdraw the designation of an STCC if the Commissioner is of the opinion that the designation criteria is no longer fulfilled.

Duties of STCC Owners

38. Once designated, the duties of the owner of the STCC would be subject to several duties, including duties to include:

(a) Provide the Commissioner with information on the STCC;

(b) Comply with such codes of practice, standards of performance or written directions in relation to STCC as may be issued by the Commissioner; and

(c) Notify the Commissioner of prescribed cybersecurity incidents.

Incident reporting

39. In order to secure and safeguard the STCCs, CSA needs strong situational awareness of the incidents and threats to the STCC. CSA proposes that persons with duties under Part 3D be required to report the following:

(a) Prescribed cybersecurity incidents in respect of the STCC;

(b) Prescribed cybersecurity incidents in respect of any computer or computer system under the owner's control, that is interconnected with or that communicates with the STCC;

(c) Prescribed cybersecurity incidents in respect of any computer or computer system under the control of a supplier to the owner that is interconnected with or communicates with the STCC.

40. If the Bill is passed, subsidiary legislation and further administrative guidance will be published to set out the operational details.

Penalties for non-compliance

41. Given the role and function that STCCs serve, the risks arising from a cyber-attack on or disruption to STCCs could lead to significant, adverse implications for Singapore. Thus, CSA proposes to make non-compliance with the duties set out in Part 3D criminal offences.

CHAPTER VI: OTHER AMENDMENTS

Monitoring Powers for Licensing Officers

42. Under Part 5 of the Act, persons engaging in the business of providing licensable cybersecurity services must have a cybersecurity service provider's licence granted or renewed in accordance with Section 26, in order to engage in such business or hold out that they are able or willing to provide the service. The grant or renewal of a licence may be subject to such conditions as the Licensing Officer thinks fit to impose. Non-compliance with licence conditions may lead to the rejection of a licence renewal application or the revocation of a licence.

43. To facilitate the operationalising of Part 5, CSA proposes to amend the Act to include monitoring powers for Licensing Officers. These include powers of entry and inspection.

Protection of CSA-related symbols

44. In recent times, CSA has received reports of unauthorised persons claiming to represent CSA in order to carry out scams against members of the public. As part of the Government's stepped-up efforts to combat scams, CSA proposes to amend the Act to make clear that only the Commissioner has the exclusive right to CSA's symbols or representations. Under this new provision, it will be an offence for any person to use a symbol or representation that is identical to CSA's symbols or representations without the Commissioner's written permission, or to use symbols or representations that are confusingly similar to CSA's symbols or representations.

CHAPTER VII. INVITATION FOR COMMENTS

45. CSA seeks views and comments from all interested parties on the draft Cybersecurity (Amendment) Bill, and on the above issues. The draft Bill released is to be used only for the purpose of this consultation and should not be used for individual or business decisions as it does not represent the final legislation.

46. All submissions should be clearly and concisely written, and should provide a reasoned explanation for any proposed revisions. Submissions are to be submitted through the **Public Consultation on Cybersecurity (Amendment) Bill** online form.

47. All submissions should reach CSA no later than **5pm on 15 January 2024**. We regret that late submissions will not be considered.

48. CSA reserves the right to make public all or parts of any 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 identified. Respondents are also required to substantiate with reasons any request for confidential treatment. If CSA grants confidential treatment, it will consider, but will not publicly disclose, the information. If CSA rejects the request for confidential treatment, it 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.

49. For the avoidance of doubt, all the information provided and views expressed in this consultation paper are for purposes of discussion and consultation only. Nothing in this consultation paper represents or constitutes any decision made by CSA. The consultation contemplated by this consultation paper is without prejudice to the exercise of powers by CSA under the Act or any subsidiary legislation thereunder.