Ministry of Communications and Information
An Engaged and Connected Singapore

OPENING SPEECH FOR SECOND READING OF CYBERSECURITY (AMENDMENT) BILL BY DR JANIL PUTHUCHEARY, SENIOR MINISTER OF STATE, MINISTRY OF COMMUNICATIONS AND INFORMATION
7 MAY 2024

(A) Introduction

1. Mr Speaker, on behalf of the Minister for Communications and Information, I beg to move that the Bill be now read a second time.

2. Sir, the Cybersecurity Act was enacted in 2018. At that time, we explained that the Act had three key objectives:

a. First, to strengthen the protection of Singapore's Critical Information Infrastructure, or CII, against cyber attacks. Our CII are core computer systems, that if disrupted, could affect our national security and survival, and thus were important to secure first;

b. Second, to authorise the Cyber Security Agency of Singapore, or CSA, to lead in the prevention and response to cybersecurity threats and incidents; and

c. Third, to establish a licensing framework to regulate cybersecurity service providers.

(B) Lessons Learnt

3. In 2018, we saw that there was a need for stronger regulatory levers to safeguard our national cybersecurity. At that time, we were one of the first jurisdictions in the world to introduce cybersecurity legislation. The Cybersecurity Act has now been in force for six years. The core objectives continue to be relevant today. We have reviewed the Act, learning from our experiences, and taking into account changes in technology.

4. We have made progress, and in some certain areas we lead in cybersecurity. This has allowed us to play a useful role in international efforts to address cybersecurity challenges. For example, Singapore has been chairing the United Nations Open-Ended Working Group (or OEWG) on Security of and in the Use of Information and Communications Technologies since 2021. The five-year OEWG is the only UN forum for discussions on cybersecurity and

norms for responsible State behaviour in cyberspace. The OEWG is also part of the reason why Minister Josephine Teo cannot be here today – she is currently in the US to participate in and lend her support to the OEWG-related discussions amongst other engagements.

5. In order to continue to ensure Singapore's cybersecurity, a review and an update to the Act is needed as several aspects of our operating context have changed:

a. Technology has evolved, and as a result, business models have changed.

i. Cloud computing as-a-Service has become widely available and widely used. Approximately 60% of all businesses in Singapore now use some form of cloud computing technology in their operations. When the Act was first written, it was the norm for CII to be physical systems held on premise and entirely owned or controlled by the CII owner. But the advent of cloud services has challenged this model.

ii. Key benefits of digitalisation are scale and aggregation. Today, it is possible to aggregate and share common digital services and functions across borders, to deliver essential services in different countries. This has likewise challenged us to review how we can safeguard the cybersecurity of our essential services.

b. The cyber threat landscape has also evolved. Malicious actors are increasingly finding new ways to their target, such as through supply chain attacks or starting with adjacent systems. One example Members may be familiar with is the SolarWinds cybersecurity breach in 2020, where a network management software that was widely used by major companies worldwide was compromised. The attacker used the software's regular updates to implant a backdoor, gain a foothold in the networks of organisations that downloaded and installed the malicious update, and then this provided the attacker with privileged access to internal networks.

c. Our relationship with technology has also evolved. Digital technology is now an integral part of our lives. In Singapore, over 90% of residents now communicate online. Firms use digital technologies intensively – their technology adoption rate has grown from 74% in 2018 to 94% in 2022. More of us are now online

for longer and online for more varied purposes. This means that we are exposed to more cyber risks, as every digital technology we use, every transaction we make, and every connection made between computers, is a possible route for attack. The cybersecurity professionals refer to this as an increased "attack surface". To cause significant disruption to the way we work and live, those who mean us harm can take down the digital infrastructure we depend on, or the institutions and entities that hold our sensitive information or perform functions of national interest. Hence, when it comes to securing Singapore in cyberspace, regulating the cybersecurity of CIIs is no longer sufficient.

6. It is vital that we update our cybersecurity laws to continue to stay ahead of the curve.

7. We are not alone in doing so. Other jurisdictions like Australia, the European Union, Malaysia, UK, and the US, have also been grappling with these developments and the ensuing implications on how to do cybersecurity. These jurisdictions have also recently introduced or announced plans to have new cybersecurity legislation to address these same concerns.

8. Additionally, having had the experience of operationalising the Act and engaging with multiple stakeholders over the last six years, we have received feedback and we have learnt many lessons on how we can better implement and enforce the Act.

9. In developing the Bill before the House today, CSA has consulted extensively with stakeholders over two years. These included our CII owners, cybersecurity and legal professionals, academic experts, sector regulators, industry players, trade associations and chambers, and members of the public. Stakeholders have generally been supportive of our proposed Bill. They understand the need for stronger cybersecurity regulation and are supportive of the policy objectives of the Bill. Our stakeholders have also provided useful feedback that has helped CSA refine the Bill. I would like to thank all who participated for their feedback and for their suggestions.

(C) Key Provisions of the Cybersecurity (Amendment) Bill

10. The Cybersecurity (Amendment) Bill seeks to update the Act to address the shifts in the operating context in cybersecurity, and strengthen the administration of the Act to address operational challenges CSA has faced.

11. Mr Speaker, Sir, before I go through the key provisions proposed in the Bill, allow me explain that I will not disclose in this Opening Speech, nor in answers to Members' clarifications, any specific real-life examples of the critical systems and entities that we regulate, or seek to regulate, for cybersecurity. It is not in Singapore's national security interests to do so, as public disclosure of these systems and entities may expose them to more risks. The list of CIIs is not made public. Similarly, systems and entities regulated pursuant to the proposed amendments will also not be made public.

I. Adapting to the Shifts in Our Operating Context

12. Sir, the Bill seeks to create new regulatory frameworks to keep up with the changes in our operating context.

13. We will update CII-related provisions. The 2018 Act was developed to regulate CII that were physical systems, but new technology and business models have emerged since. Hence, we need to update the Act to allow us to better regulate CIIs so that they continue to be secure and resilient against cyber threats, whatever technology or business model they run on. The Bill will do this in the following ways:

a. Clause 3(j) extends the meaning of "computer" and "computer system" in specified portions of the Act to include "virtual computers" and "virtual computer systems", which in turn are defined in new definitions inserted by clause 3(i). Clause 3(j) also introduces provisions setting out what "ownership" means in relation to virtual computers or computer systems.

i. Currently, the Act's definitions of "computer" and "computer system" are predicated on them being physical computers that are built out of dedicated physical hardware, such as hard disk drives, memory and processor chips. This was suitable in 2018, as CII were physical systems. However, given recent technological advancements, it is now possible that a CII could be a virtual computer system.

ii. Our interest is in the computer or computer system that is necessary for the continuous delivery of the essential service, whether it is physical or virtual. However, in the case of a virtual CII, such as in a Cloud

environment, the underlying physical infrastructure could be shared or easily replaced, and therefore it would not be sensible or meaningful to regulate the underlying hardware.

iii. The new definitions we are introducing allow us to make it clear that the CII owner is responsible for the cybersecurity of its virtualised CII, and not other parties that supply the underlying physical infrastructure.

b. Clause 14 seeks to introduce a new Part 3A which will regulate providers of essential services who rely on CII owned by third parties, for the continuous delivery of essential services. This will deal with situations where a provider of an essential service could leverage a computer system owned by a third party, because it could be more effective or efficient to do so.

i. For example, hypothetically, a third-party vendor could own, operate and supply a critical Operations Management system that is used by multiple providers of a given essential service. The third-party vendor could have greater expertise operating such a system and is able to do so at a lower cost, due to demand aggregation.

ii. The principal Act did not provide for such business models because it was the norm then for providers of essential services to own and operate their critical systems. Business models may be changing, but the fundamental principle remains the same. Providers of essential services must remain responsible for the cybersecurity and cyber resilience of the computer systems relied upon to deliver essential services they provide. New Part 3A will ensure that they cannot outsource this responsibility, even if they rely on a third party's computer system for the continuous delivery of the essential service.

iii. Under the new Part 3A, the responsibility rests with the provider of essential service. To be clear, CSA does not seek to regulate the owners of these systems under Part 3A, who are the third-party vendors. However, the providers of essential services must ensure that the systems they rely on can meet comparable cybersecurity standards

and requirements of a CII through legally-binding commitments, such as contracts.

iv. Third-party vendors that seek to work with providers of essential services will need to have the necessary expertise and capability to own and operate a CII in a manner that meets the cybersecurity standards we hold a CII to. It is a specialised area and a considered business decision to operate in this space. Members will appreciate that not many businesses will be or can be in this space.

c. Clause 8 allows CSA to deal with situations where a CII is supporting an essential service from overseas. The Act currently only allows CSA to designate computers or computer systems as CII if the entire or part of the computer or computer system is in Singapore. However, this has also meant that CSA is currently unable to regulate a CII that is wholly located overseas. Clause 8 inserts a new section 7(1A) which will allow CSA to designate and regulate such CIIs that are wholly located outside Singapore, so long as its owner is in Singapore and the computer system would have been designated as a CII under section 7(1) had it been located wholly or partly in Singapore.

14. We will also be updating CII-related provisions to address the inventiveness of malicious cyber actors.

a. Under the principal Act, a CII owner is generally only obliged to report cybersecurity incidents relating to the CII, or computers or computer systems that are interconnected with or communicate with the CII. CSA needs such incident reporting so that it can intervene early if necessary, and gain a better situational awareness so that it can proactively alert other sectors and prevent the spread of similar attacks. Such reports serve to sound the alarm.

b. As the tactics and techniques of malicious actors evolve to target systems at the periphery or along supply chains, we must also start placing our alarms at those places. Clause 12 will therefore amend section 14 to require CII owners under Part 3 to additionally report incidents that affect: (i) other computers

under the owner's control, and (ii) computers under the control of a supplier that are interconnected with or communicates with the CII.

i. The former requirement will help us be better prepared should any of our essential services be targeted in the same manner as in the SolarWinds case.

ii. The latter requirement will enable us to take proactive steps to protect our CIIs if CII owners' immediate suppliers are compromised, to pre-empt potential disruptions to essential services. The requirement to report on incidents affecting immediate suppliers will apply only if the CII is owned by the provider of essential service. This is a practical approach. In situations where a third party owns the CII, the provider of essential service is unlikely to have visibility of the third party's suppliers to be able to report any incident to CSA.

15. We will also expand the Act to regulate a new type of system called Systems of Temporary Cybersecurity Concern, or STCC, so as to address the evolution of our threat landscape.

a. Clause 15 inserts a new Part 3B to regulate the cybersecurity of STCCs, which are systems that for a time-limited period, are at high risk of cyber-attacks, and if compromised would have a serious detrimental effect on Singapore's national interests.

i. The COVID-19 pandemic drove home the importance of being able to secure such systems. During the pandemic, many governments around the world developed temporary systems to support the tracking and distribution of vaccinations, and many of these systems were targeted by malicious actors seeking to exploit the urgency of the situation. Should we be faced with another pandemic, we need to be in the position to secure the systems critical to our crisis response.

ii. Another potential group of STCCs could include systems supporting high-key international events in Singapore, such as the Trump-Kim Summit in 2018, or the Youth Olympic Games in 2010. Such

international events could be attractive targets for cyber-malicious actors seeking a global stage. The Tokyo Olympics of 2021, for example, was reported to have encountered 450 million cyber attacks. We need to take the cybersecurity of such systems and such events seriously to maintain Singapore's reputation as a safe and reliable place to host such events.

iii. Before the Commissioner of Cybersecurity can designate a system an STCC, the Commissioner must be satisfied that, for a limited period, the system is at a high risk of a cybersecurity threat or incident; and the loss or compromise of the system will have a serious detrimental effect on the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore. In other words, this is intended to apply to systems that are critical to Singapore.

iv. Given that STCCs are critical systems when they are set up, Part 3B will impose on STCC owners cybersecurity obligations similar to those for CII owners, where practicable. Part 3B will allow CSA to be proactive in raising the cybersecurity posture of the STCC, depending on the operating context and the time period for which the STCC is needed.

16. Finally, provisions will be introduced to expand the ambit of the Act to other new entities beyond the current CII regulatory regime.

a. Clause 16 introduces a new Part 3C, that will allow CSA to regulate entities that could be particularly attractive targets for malicious threat actors, because the disruption of the function they perform, or the disclosure of sensitive information their computer systems contain, will have a significant detrimental effect on Singapore's defence, foreign relations, economy, public health, public safety, or public order. These entities will be referred to as "Entities of Special Cybersecurity Interest", or ESCIs.

i. One example of potential ESCIs could be universities. Universities are popular targets of malicious actors, given their standing in society, the sensitive research they may do, and the data they may possess. For instance, in 2019, the Australian National University detected a

database breach, reportedly by a state actor, which resulted in unauthorised access to extensive personal information, including bank records, tax details and passport information of students and staff dating back almost two decades. Senior Australian officials feared that such data could be used to exploit or recruit students and alumni as informants.

ii. Our own universities have also been targets of cyber attacks in the past. MOE and the universities have since taken steps to strengthen their cybersecurity defences. The proposed amendments in this Bill could further strengthen our universities' defences, and enable CSA to take stronger action to secure them, as well as other entities of special cybersecurity interest, if they are designated.

iii. However, the specific list of entities designated as ESCIs should not be disclosed publicly. This is to avoid inadvertently advertising these entities as worthy targets to malicious actors.

iv. CSA will be able to issue or approve cybersecurity standards of performance and codes of practice to stipulate the cybersecurity measures ESCIs should have in place. ESCIs will be required to report prescribed cybersecurity incidents that result in a breach of the availability, confidentiality, or integrity of the entities' data, or have a significant impact on the business operations of the entities. CSA will also be empowered to issue written directions to ESCIs, if necessary or expedient, for ensuring the cybersecurity of the ESCIs or the effective administration of the Act.

v. The obligations we impose on ESCIs will be moderated when compared to those imposed on CIIs or STCCs, in recognition that the impact on our national interest resulting from cyber attacks on ESCIs may not be as severe compared to the impact from cyber attacks on CIIs or STCCs. This ensures that regulatory obligations are commensurate with the cybersecurity risks posed.

b. Clause 17 introduces a new Part 3D, to cover the last new category of entities that CSA proposes to regulate for cybersecurity – providers of "Foundational Digital Infrastructure service", or FDI service. Our ability to operate normally, and to enable citizens to meet their day-to-day needs has become increasingly dependent on the good functioning of the digital infrastructure that powers our digital economy. The more foundational the digital infrastructure is to systems central to our work and lives, the more attractive it is to malicious actors. Infrastructural vulnerabilities can be exploited to compromise many systems, and can cause widespread disruption.

i. The new Part 3D will allow CSA to regulate major providers of FDI service for cybersecurity. This refers to entities that serve a large number of businesses or organisations. This reflects our interest in securing ourselves against the risk of widespread disruption or deterioration of activities that rely on or are enabled by the FDI service. This also means that smaller players, who are more sensitive to regulatory costs, will not be regulated.

ii. These major providers must be providers of FDI services specified in the new Third Schedule, which will be introduced by Clause 30. The digital world moves quickly, so our approach must allow for quick adaptation and agility. For a start, the Third Schedule will cover cloud computing services and data centre facility services, as they are crucial to the functioning of a wide array of digital services that enterprises and consumers use daily. As new types of digital infrastructure grow in importance to our needs, they can be added to the new Third Schedule.

iii. CSA will be able to issue or approve standards of performance and codes of practice to stipulate to the major FDI service providers that have been designated, the expected cybersecurity practices that should be in place. These providers will also be required to report prescribed cybersecurity incidents that: (i) result in a disruption or degradation of the designated provider's FDI service in Singapore, or (ii) have a significant impact on the major FDI service provider's business operations in Singapore. Recognising that major FDI service providers

provide services to clients across sectors, and often across borders, CSA has been consulting closely with industry and sector leads to develop inter-operable standards, codes, and operating parameters. We are mindful about compliance costs for these major providers and are committed to keeping them reasonable.

iv. The same appeal avenues available to those designated as CII owners under the Act today will be extended to providers of essential services under Part 3A, STCC owners, ESCI and major FDI service providers that CSA designates. For example, any entity that receives a designation notice may appeal against the designation, and regulated entities can appeal CSA's decisions, orders, and directions as well. This is encapsulated in the new section 35B introduced by Clause 19.

17. The proposed scope of the Bill is targeted and affects only providers of essential services, owners of STCCs, ESCI and major FDI providers. These are a known and finite set, and CSA will be working closely with them. The Bill does not impose cybersecurity obligations on the larger business community.

II. Strengthening the Administration of the Act

18. We will also enhance the Act to strengthen the administration of the Act:

a. To improve CSA's ability to enforce the Act against recalcitrant CII owners regulated under Part 3 of the Act, Clause 13(b) will amend section 15(4) to empower CSA to inspect the CII if it appears to the Commissioner that the CII owner has not complied with its obligations or has provided information requested under section 10 of the Act that is false, misleading, inaccurate or incomplete. This is because wilful non-compliance by CII owners could jeopardise our national security and survival.

b. Currently, Part 5 of the Act regulates persons who provide licensable cybersecurity services. Clause 18 will provide monitoring powers for licensing officers, for the purposes of executing Part 5. In the absence of such powers, CSA could face difficulties in seeking information from uncooperative licensed cybersecurity service providers to verify their compliance with the conditions of their licences. The new provisions will give CSA powers of entry and

inspection, and to require the production of records, accounts and documents from licensed cybersecurity service providers. Non-compliance with such requirements without reasonable excuse will be a criminal offence.

c. While we seek to strengthen CSA's ability to act and enforce the law as the national cybersecurity authority, we recognise that there are criminals looking to exploit this authority through impersonation scams. Clause 7 will make it an offence for any person to use CSA's gazetted symbols or representations without the Commissioner's prior written permission.

d. Clause 22 allows the Commissioner to grant an extension of time to any person required to do any action under relevant parts of the Act, as long as there are good reasons to do so. This was borne out of our experience where there were valid reasons, at times, for regulated entities to not be able to comply with the obligations of the Act under business-as-usual timelines. With this amendment, we will be able to grant time extensions if regulated entities experience extenuating circumstances.

III. Revised Penalty Regime

19. If these proposed amendments are passed, they will expand the range of cybersecurity obligations placed on CII owners under the existing Part 3 and regulate four new classes of systems and entities for cybersecurity, while accounting for the varying degrees of risk posed to Singapore and Singaporeans. Thus, the Bill also recommends a key revision to the penalties that can be imposed for non-compliance.

a. In the current Act, non-compliance with statutory obligations in relation to CII is to be enforced through criminal penalties. This was appropriate as the measures imposed on CII in the 2018 Act are needed to ensure their cybersecurity, and in turn the undisrupted delivery of our essential services. We needed to underscore the gravity if there was any non-compliance.

b. This Bill will introduce more obligations on CII owners under the existing Part 3, such as the new reporting requirements relating to peripheral systems, as well as the proposed provisions covering new classes of systems and entities.

c. With a wider set of proposed obligations, Clause 20 gives the Commissioner the flexibility to bring an action in court for civil penalties with the Public Prosecutor's consent. In making a recommendation to the Public Prosecutor, CSA will consider a range of factors, including the risks created by the non-compliance, the egregiousness, and the facts of the case.

(D) Conclusion

20. Mr Speaker Sir, the Bill is a major update to the Cybersecurity Act given the significant shifts in the digital domain. The amendments will allow CSA to:

a. Keep pace with developments in technology and business practices;
b. Respond to evolving cybersecurity challenges in our cyber threat landscape;
c. Extend its regulatory oversight to other important systems and entities and use a risk-based approach to regulating entities for cybersecurity; and
d. Administer the Act more effectively.

21. This Bill will strengthen our national cybersecurity, and increase trust in using online services in Singapore and in our highly-digitalised nation. It is calibrated to address the risks to the nation, our economy and our way of life, while balancing compliance costs. In implementing the proposed new laws, our experience with the 2018 Act will serve us well, and we will continue to refine our approach, in consultation with stakeholders and consider new international best practices as they emerge.

22. With that, Mr Speaker, I beg to move.

+++