Ministry of Communications and Information
An Engaged and Connected Singapore

CLOSING 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, I thank Members for their interest in and strong support for the Bill.

a. All Members who spoke have given strong support for the Bill. Several Members noted the rise in cyber threats both in Singapore and around the world and that this has become a growing concern amongst Singaporeans.

b. **Mr Gerald Giam**, **Mr Alex Yam**, and **Mr Darryl David** spoke about the potentially devastating impact that a successful attack on our CII could have on the lives of Singaporeans. **Ms Hany Soh** spoke about recent major cybersecurity incidents and their serious consequences, while **Mr Desmond Choo** said that it was crucial that we have robust and regularly-updated cybersecurity laws against the increase in cyber threats. I agree.

2. As the cyber threats we face intensify, it is clear that there is agreement in this House on the timeliness of this Bill, and the need to put CSA in a better position to safeguard Singapore's cybersecurity.

3. **Mr Melvin Yong** spoke about the urgent need to tackle scams. The Government agrees. In January 2024, Minister Josephine Teo spoke about Building an Inclusive and Safe Digital Society, and outlined what the Government is doing to combat scams, so I will not belabour those points. The Cybersecurity Act is not aimed at tackling scams. Even so, Clause 7 of the Bill will allow us to take a stronger stance against impersonation scams, by making it an offence for any person to use CSA's gazetted symbols or representations without the Commissioner's prior written permission.

4. Cybersecurity threats are ever evolving. **Mr Melvin Yong** also spoke about the need to secure operational technology (OT) systems. The cybersecurity of OT is a nascent field, but it is already one of CSA's key areas of work as part of its national cybersecurity mission. CSA has established thought leadership when it published the OT Cybersecurity Masterplan in 2019, which is a strategic blueprint to guide Singapore's efforts to foster a resilient and

secure cyber environment for our OT CII. CSA also organises the OT Cybersecurity Expert Panel Forum every year, which is a platform for cybersecurity practitioners, operators, researchers, and policy makers to discuss governance policies, best practices and trends related to OT cybersecurity.

5. The Members who have spoken today have raised several important considerations relating to the Bill, and I would summarise them into three groups:

a. First, are the compliance costs arising from the cybersecurity measures introduced by the Bill justified?

b. Secondly, will the new obligations be operationalised in a sensible and practical manner?

c. Finally, will there be safeguards in place to prevent abuse, as the Bill expands CSA's powers?

6. Let me address these considerations in turn.

(B) Are the compliance costs justified?

7. **Some Members** raised concerns about the additional costs of regulatory compliance. Some have suggested that such costs could even adversely impact the community of SMEs in Singapore, or industry development more generally.

8. To clarify, neither the Cybersecurity Act nor the amendments proposed in this Bill impose cybersecurity obligations on the business community at large. What the Act and amendments proposed in the Bill seek to do is regulate only the cybersecurity of systems, infrastructure and services that are important at a national level, because their disruption or compromise could affect our survival, security, safety, or other national interests. This is a known and finite set of systems and entities. Our approach is a targeted and calibrated one, precisely because we recognise that regulation will involve compliance costs.

9. With the amendments covered in the Bill, the Cybersecurity Act will only be imposing obligations on four groups of entities:

a. The first is providers of essential services, whether they are Critical Information Infrastructure (CII) owners or rely on third party vendors for the CII. Securing the computers and computer systems that are necessary for the continuous delivery of our essential services is a matter of national security and survival.

b. The second group comprises owners of Systems of Temporary Cybersecurity Concern (STCC). Where there is loss of a computer system, even a system established on a temporary basis, would have a serious detrimental effort on Singapore's national interests, CSA must be allowed to proactively oversee the cybersecurity of such systems.

c. The third group comprises Entities of Special Cybersecurity Interest (ESCI). The ESCIs. This is because we need them to be cybersecure if their computer systems contain sensitive information or they perform functions which if disrupted will have a significant detrimental effect on our national interests.

d. The last group comprises major providers of Foundational Digital Infrastructure (FDI) services, because disruption to these FDI services that FDI service providers provide could have knock-on disruptions to Singapore-based organisations and Singaporeans who rely on them for their business operations, work and lives.

10. Some compliance cost cannot be avoided when regulation is concerned. It is something we are mindful of, we do not seek to regulate without good reason. For these four groups, it was a considered decision that **we must have the necessary legislation in place to govern their cybersecurity because our national security and other national interests are at stake.**

a. Cyber attacks can have serious consequences. Where essential services are concerned, lives and livelihoods can be affected. Attacks like these can also indirectly hurt the reputation of the organisation or Singapore, and can have an external, impact on the customers and business partners of the victim organisation. These are in addition to potential direct financial costs - according to some reports, the average cost of a cyber attack on an organisation with more than one thousand employees is around S$71,000, and one in eight firms suffered costs of S$330,000 or more.

b. These security reasons are also why I had caveated in my Opening Speech that I will not disclose any specific real-life examples of the critical systems and entities we seek to regulate, which includes ESCIs. I seek **Ms Ng Ling Ling'**s understanding that I will not respond directly to her query on the entities that will be designated as ESCI. **Ms Hany Soh** asked whether there would be circumstances that go toward publication or disclosure of an ESCI's identity - this will be on a case-by-case basis, and we must keep the security of the ESCI in mind.

11. The issue for consideration is not whether a regulated entity is a large company, an MNC or a SME. The key consideration is whether a cyber attack on the entity could have serious implications on our national security or other national interests. We do not take these decisions to impose obligations lightly. For instance, we are proposing the expansion of the incident reporting requirements for CII owners under Part 3 because the evidence shows that malicious actors are using CII-adjacent systems and supply chains to attack the CII, and we need to stay situationally aware of what is happening around the CII in order to keep the CII itself safe.

12. **Mr Mark Lee** seemed to have the impression that the Bill only focuses on "personal information" and does not protect other types of confidential business information. This is not the case. The Cybersecurity Act does not differentiate between protecting personal information and business information, as the cybersecurity of all information in a CII must not be compromised. The Bill will do the same for the new categories of systems and entities we are proposing to regulate for cybersecurity.

13. **Mr Sharael Taha** asked about how we would address the cybersecurity threats posed by machine learning and generative AI. The Act and this Bill allow CSA to compel regulated entities to take the necessary measures to mitigate cyber risks, regardless of the technologies used by the regulated entities, or by malicious actors to perpetuate their attacks. The AI landscape is still developing and relatively nascent. CSA will continue to monitor our threat landscape carefully, work with regulated entities to take the necessary steps to protect themselves and address the challenges as the technology emerges and become clearer.

14. I would also like to clarify that not all the amendments add to the operating costs of regulated entities and systems. Some of the key amendments I covered in my Opening Speech will allow CII owners to make use of new technologies and new business models. This can result in efficiencies while maintaining the cybersecurity of the CII. These include the use

of commercial cloud solutions, and demand-aggregated system infrastructure owned by a third party. These could be business opportunities as **Mr Neil Parekh** observed in his speech.

(C) How will CSA ensure that the new obligations are operationalised in a sensible and practical manner?

15. How CSA will ensure that the new obligations are operationalised in a sensible and practical manner?

16. The technologies are constantly advancing, and changes our business and operating context. Malicious actors are inventive, and continually find new ways to compromise their targets. Several members have asked questions about how the amendments would be implemented. Underlying their questions is an important consideration – will CSA operationalise these new laws sensibly and give regulated entities support to meet their statutory obligations? The short answer to both is yes, but I am going to give a slightly longer answer.

17. CSA understands the need to take into account business realities and to be practical and sensible when implementing the Act. CII owners and other industry stakeholders representing potential ESCIs and major FDI service providers were consulted extensively. Many trade associations and chambers provided their views during the consultation process.

18. CSA's practice is, has been, and will be, to provide ample support to our regulated entities, by 'walking with them towards compliance'.

a. This begins even before a system or an entity is designated. Where CSA has reason to believe that a system or entity should be designated, CSA's general practice has been to first engage the system owner or the entity to better understand their operating context such as the cybersecurity measures already implemented and their level of cybersecurity capabilities to ensure that any designation is appropriate. Subsequently, CSA will then work with the system owner or entity to assess what needs to be done for the entity or system to be in compliance with the Act, as well as the support and lead time that the organisation will need. I hope this addresses **Mr Mark Lee's, Mr Neil Parekh's** and **Ms Hany Soh's** clarifications on the designation process, **Ms Tin Pei Ling's** question on how we can calibrate our implementation approach and **Ms Joan Pereira's** query on whether all ancillary or supporting infrastructure will be designated as STCCs

for high-profile, high-security or high-level events in Singapore. We will only make such decisions after fully understanding the context and how the relevant systems are designed.

b. CSA will also consider waivers of the application of a code of practice or standard of performance on a designated entity where possible on a case-by-case basis, to account for specific operating contexts, or the developmental journey of the organisation in question.

19. As **Mr Sharael Taha** noted, our CII supply chains are getting more complex. If a breach occurs to a supplier's system that is not directly interconnected with or communicates with a CII, the Bill will not require the owner of the compromised system to report such breaches to CSA. **Mr Darryl David** asked how we would manage, if vendors and suppliers to our CIIs are not directly obliged by statute to disclose cybersecurity incidents. The principle we apply is that CII owners are responsible for the security and resilience of their essential services. That means that it is in their interest and it is also their responsibility to be situationally aware of supply chain attacks that could affect their CII and report such incidents to CSA when they become aware of them. It was a deliberate decision on the Government's part not to compel reporting of cybersecurity incidents from all the suppliers of a CII owner to CSA directly. Doing so would add the reporting burden to more parties and may not be directly useful for enhancing the security of the CII itself, which ultimately is what all this work is focused on.

20. Where the CII is owned by a third party, Clause 14 requires the provider of essential service from the third-party vendor to obtain legally-binding commitments from the vendor that would put the provider in a position to discharge its statutory obligations, so that the cybersecurity of the CII is not compromised.

a. **Mr Louis Ng** asked several questions relating to how the Government would ensure that we would have sufficient levers against such a third party. The intent behind these provisions is to allow the provider of essential service to consider market solutions from third parties, so that they can be more efficient in the provision of their essential services, without compromising cybersecurity. It is not to indirectly regulate these third parties.

b. Where the third party is unwilling or unable, as **Mr Darryl David** noted could happen, CSA could direct the provider of essential services to stop using the

system owned by that third party under the provisions in new Sections 16E(2), 16H(2), 16I(2) and 16J(2).

c. **Ms Joan Pereira** asked if it would be feasible for CSA to require a provider of essential services to cease using a third party vendor on the market. Ultimately, what Part 3A seeks to do is to ensure that providers of essential services who use a third party's system do so without compromising cybersecurity. Where a provider of essential services faces certain constraints, CSA is prepared to work with them on possible arrangements that could be made. However, if there are no solutions on the market that are adequately secure, the provider of essential services should take responsibility for building the CII it needs. The security of our essential services cannot and should not be compromised.

d. In response to **Mr Desmond Choo's** question on data security when CII owners move to the Cloud, CSA will work with CII owners to conduct cybersecurity risk assessments of any migration of a CII to the Cloud. The principle remains – they must be able to meet their statutory obligations with respect to the cybersecurity of the CII regardless of the operating model.

21. The same principle applies to **Ms Tin Pei Ling's** and **Mr Gerald Giam's** questions about overseas CII. Under the new Part 3 provisions proposed by the Bill, the owner of the CII will be held responsible for the cybersecurity of their CII. It does not matter whether the CII is located in Singapore, or located wholly overseas and designated under the new Section 7(1A). Section 7(1A) only applies when the owner is in Singapore. Similarly, the new Part 3A applies to a provider of essential service located in Singapore, who will be held responsible for the cybersecurity of the CII that they rely on. It does not matter whether the CII owned by the third-party is located in Singapore, or located wholly overseas. The obligations are placed on the CII owner or the provider of essential service in Singapore, so there is no extra-territoriality enforcement of the provisions in new Part 3 and Part 3A.

22. **Mr Yip Hon Weng** asked how we will deal with the cross-border nature of FDI services such as cloud services and data centre operations. We have designed the new provisions to account for this.

a. For example, where cloud computing is concerned, it is entirely possible that the cloud services provided to the Singapore market are provided using infrastructure that can be located in any part of the world. In fact, the ability to

tap on infrastructure from any part of the world is a key value proposition of cloud computing because it bolsters the resilience of a given cloud service. Thus, the focus of our proposed laws is not to insist that designated major FDI service providers report cybersecurity incidents affecting all their digital infrastructure around the world. Rather, new Section 18M will require them to report only prescribed incidents that result in the disruption or degradation of the designated provider's FDI service in Singapore, or has a significant impact on the designated provider's business operations in Singapore.

b. **Mr Yip Hon Weng** also asked if the designated providers of major FDI service will be held responsible for breaches occurring in overseas data centres if they disrupt their services in Singapore. Sir, I would like to make it quite clear that the Act, even if amended by the Bill, does not penalise victims of cyber attacks for being attacked. The statutory duties under the Act only require the designated provider to work with CSA to prevent and mitigate the cybersecurity risks by, for instance, reporting cybersecurity incidents, and complying with the necessary cybersecurity standards and written directions.

c. Penalties would apply when there is wilful non-compliance. **Mr Neil Parekh** asked about the types of penalties that could be imposed. If the proposed amendments are passed, such penalties could be criminal or civil in nature. **Ms Hany Soh** asked what factors would be taken into consideration on the penalties to impose for non-compliance – 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, the facts of the case.

d. **Ms Razwana Begum** asked how we would enforce the provisions relating to major FDI service providers if many of the providers are based overseas. Indeed, this could be the case for the cloud service sector. To facilitate enforcement, new Section 18G(6) requires a designated major FDI service provider who is located outside of Singapore to appoint a person in Singapore to accept service of notices or directions under the Act.

23. **Several Members** pointed out that some of the operational details are not contained within the Bill. Matters relating to the technical or other standards that regulated entities must meet, and how CII owners should work with the providers of cloud services they use, will be designed to reflect current business realities and prevailing industry norms. What the Bill does

is to allow CSA to address these in codes of practice or standards of performance and subsidiary legislation, so that we can be more agile in reflecting the operating context. CSA will be consulting industry on these matters, if the Bill is passed.

24. **Many Members like Ms Ng Ling Ling, Ms Jean See, and Mr Melvin Yong** also gave suggestions on how the Government can provide more support to regulated entities to help them comply with their statutory obligations and provide some assurance that their cybersecurity measures are adequate. We will consider these suggestions very carefully. As CSA operationalises the new amendments, CSA will continue to take onboard stakeholder feedback. Where appropriate and feasible, CSA will harmonise the cybersecurity standards and incident reporting parameters to be imposed under the Act with international practices.

25. **Mr Gerald Giam** asked about step-in rights and CSA's incident response frameworks. I understand the concern to be whether CSA is adequately empowered to respond effectively to cybersecurity incidents and do what it takes to secure our CII. Part 4 of the 2018 Act already provides CSA with the necessary powers to respond to cybersecurity threats and incidents and to take appropriate measures to secure the threatened or attacked system. Operationally, CSA and the DIS of the SAF have an excellent working relationship, and will work together to secure Singapore's cyberspace.

(D) Safeguards

26. Sir, let me now move on to the third consideration, that is, what safeguards are in place to prevent abuse? The Bill seeks to strengthen CSA's regulatory powers, but as **some Members** have pointed out, it is also important that CSA exercises its powers responsibly.

27. Safeguards have been built into the Act from the outset, and will be extended to cover the proposed amendments.

a. First, any entity that receives a designation notice can appeal against it. A regulated entity may also appeal against CSA's decisions, orders and directions as well as codes of practice and standards of performance. This appeal mechanism was created in the 2018 Act to protect regulated CII owners, and will be extended to cover providers of essential services under Part 3A, STCC owners, ESCI and major FDI providers as well.

b. Second, the powers that the Bill seeks to confer on CSA are not unfettered. For example, the power of inspection provided for in the amended Section 15(4)(d) inserted by Clause 13, can only be used for the specified purpose and under the specified circumstances set out in the provision.

Third, Section 43 of the 2018 Act, which we are retaining, requires specified persons to preserve the secrecy of stipulated matters that come to these persons' knowledge in the discharge of their statutory duties. This includes information relating to business, commercial or official affairs of any person and identities of informants. Section 43 will continue to govern any such information that CSA obtains through the exercise of existing and new powers provided for by the amendments.

28. **Ms Tin Pei Ling**, **Mr Gerald Giam** and **Mr Sharael Taha** and noted that the Bill will significantly expand the scope of the Act, and asked if CSA will be sufficiently equipped to manage this expanded ambit. If the Bill is passed, the Government will ensure that CSA is resourced accordingly. CSA will also continue to develop the personnel and their expertise so that it can continue to deliver its mission at a high level.

(E) Conclusion

29. I hope that I have sufficiently addressed the queries raised in this House.

30. Mr Speaker, cybersecurity is ultimately about risk management. The only way we can absolutely guarantee cybersecurity is to not use digital technology at all. So the task at hand is to find the appropriate balance between security, usability, and cost. The Bill is the sum of the Government's proposal to address this trilemma for the most important systems that affect the national interest. It does involve trade-offs.

a. Where national interests are stake, the Government needs to proactively ensure that security considerations are optimised. Those responsible for our CII, STCCs, and FDI services, as well as our ESCIs will have to bear some compliance costs, but this is what it takes to keep Singapore and Singaporeans safe and secure in the digital domain.

31. Let me emphasise that these proposed new laws do not extend to the wider business community. That is not to say that their cybersecurity is not important. As **Mr Mark Lee** had

noted in his speech, confidential business information that our companies and organisations hold are also important and potentially sensitive in their own context. Our companies and organisations must recognise this and take the commensurate steps to address their own data security risks. The Government offers our support to them through other non-regulatory means.

a. For example, the SG Cyber Safe Programme. These are schemes to help the Singapore business community be more cyber secure. This includes the Cyber Essentials and Cyber Trust marks, which are certification schemes that recognise enterprises that have implemented good cybersecurity practices. CSA has also developed cybersecurity informational toolkits for companies of various profiles to guide enterprise leaders and their employees on cybersecurity best practices. Additionally, enterprises getting started on cybersecurity can use the Cybersecurity Health Plans programme, where consultants help them improve their cyber resilience, and help to develop a plan tailored to their needs. I urge all enterprises to apply for the various schemes and marks and take advantage of the resources available to uplift their cybersecurity posture.

b. I also thank **Ms Jean See, Mr Neil Parekh, Ms Razwana Begum** and **Mr Mark Lee** for their suggestions of other non-regulatory initiatives that the Government could consider, particularly on shifting the mindset of stakeholders from one of compliance to one of partnership. CSA will study these suggestions.

32. CSA has had a good track record in administering the Cybersecurity Act over the past six years. CSA works closely with the regulated entities to address their needs and concerns, and to date, no appeals have been made against CSA's decisions, orders or directions. This is in large part due to the good work of our CSA officers. We have been able to attract and retain officers with a high degree of expertise, professionalism and integrity, who are able to balance between the considerations of security, useability and cost, and who understand and believe in the mission of securing Singapore's cyberspace.

33. Cybersecurity is a team effort. We must continually improve our defences against cyber threats that are growing in scale and sophistication. Today, the Government proposes to strengthen our legislation so that we can ensure the cybersecurity of systems and entities

that are important to Singapore's national interests. I thank Members for their support of this Bill. Mr Speaker, I beg to move.

+++