Minister Josephine Teo's Speech for the Parliamentary Motion on Building an Inclusive and Safe Digital Society

1. Mr Speaker, Sir, I rise in support of the Motion in the name of Ms Tin Pei Ling and thank her, together with Mr Sharael Taha, Ms Hany Soh, Ms Jessica Tan and Mr Alex Yam, for drawing attention to this important topic.

2. When the Smart Nation Initiative was launched in 2014, we envisioned Singapore as "a nation where people live meaningful and fulfilled lives, enabled seamlessly by technology, offering exciting opportunities for all."

3. A decade on, this vision has certainly come alive. Technology has become a big part of our daily lives and 84% of Singaporeans say they have benefitted in one way or another. Of every $100 value-added in our economy, at least $17 can now be attributed to digital-related activities. It amounted to $106 billion in 2022, more than financial services and insurance, and comparable with wholesale trade.

4. There are, today, more than 200,000 tech jobs in Singapore, earning median wages that are higher than that of the resident workforce. Although they represent just over 5% of all jobs, there are thousands more across all other sectors that have been enhanced by digital technologies.

5. Our aim must be for all Singaporeans to gain from these developments. Senior Minister of State Tan Kiat How has spoken about digital inclusion and the Government's efforts to ensure that benefits are felt by all segments of society.

6. At the same time, our digital way of life has exposed us to new risks. Cyberattacks, scams and harmful content pose a growing threat to our safety and security. As many Members have noted, trust in society, so crucial for normal human interactions, could be undermined.

7. I will focus my speech on two topics specifically. The first is what we have we done so far to protect Singaporeans in the digital domain; and the second, what more we need to keep people safe.

8. Sir, in most domains, Singapore could learn from the examples of many other countries when designing our own governance approach. Unfortunately, in the digital domain, there are few ready playbooks with proven solutions. In fact, Singapore is considered an early mover in digital governance and has been recognised as such.

9. Mr Mark Lee spoke about the need for our businesses to protect and handle customer information ethically. We moved to address this issue more than a decade ago. In 2012, we introduced the Personal Data Protection Act or PDPA, before the EU's General Data Protection Regulation. By 2020, we had amended the Act to strengthen organisational accountability and consumer protection, while bolstering confidence for using personal data for innovation. In 2018, we enacted the Cybersecurity Act to address the threats in cyberspace, particularly those faced by our critical information infrastructure (CII).

10. Beyond protecting our CII, we have also introduced initiatives to help businesses enhance their cybersecurity posture. Mr Lee recommended developing sector-

specific resources. We agree. In the next phase of the SG Cyber Safe Programme for enterprises, CSA will introduce sector-specific cybersecurity initiatives, starting with healthcare and manufacturing.

11. Also, I had previously announced that we expect to update the Cybersecurity Act so that it remains fit-for-purpose. Public consultations on the proposed amendments are ongoing.

12. In 2019, recognising the harms of misinformation, we introduced the Prevention of Online Falsehoods and Manipulation Act (POFMA). As a small, multiracial, and multi-religious country, Singapore is particularly vulnerable to falsehoods that deepen fault lines and polarise society. POFMA is a calibrated tool to safeguard the infrastructure of fact. Its usefulness was especially evident during the COVID-19 pandemic, to defend against all kinds of falsehoods about vaccines and COVID-19 related deaths.

13. In 2021, to counter potential hostile information campaigns launched by other states against us, we introduced the Foreign Interference (Countermeasures) Act or FICA. This helps to ensure that Singapore politics remains only for Singaporeans.

14. Dr Wan Rizal, Ms Mariam Jaafar and Ms Nadia Samdin spoke about the risks of children being exposed to harmful content online. We have also introduced measures to tackle this. In July 2023, the Infocomm Media Development Authority (IMDA) launched the Code of Practice for Online Safety. It requires social media services with significant reach or impact in Singapore to put in place measures to

minimise users' exposure to harmful content on their platforms. These include additional measures to protect children below the age of 18.

15. Dr Rizal and Ms Nadia suggested that platforms implement age assurance measures. There is currently no foolproof measure to prevent false age declarations on social media platforms. But the technology has improved. Today, age assurance is achievable to a fairly high degree of accuracy without compromising privacy. MCI and IMDA are monitoring the developments and will study viable regulatory options to better protect children online through age assurance measures.

16. I am aware that Mr Darryl David will speak about addressing online dangers such as cyber stalking and body shaming, and providing support for victims. Currently, online harassment and doxxing are dealt with under the Protection from Harassment Act 2014. Victims can seek redress through the Protection from Harassment Court, which has served thousands since it was set up in 2021.

17. The Ministry of Law (MinLaw) is looking further into how victims can be better empowered to put a stop to such online harms, and to seek redress from those responsible. MinLaw's efforts will complement MCI's efforts to enhance the Government's regulatory tool kit, as well as the Ministry of Home Affairs (MHA)'s efforts to address online criminal harms, which I will say more about later.

18. Sir, from what I have cited, Members will see that we have actively and progressively introduced new laws and regulations for digital governance. We have consciously avoided a big-bang approach, choosing instead an accretive approach

to understand the issues deeply and to move quickly when we identify measures that are likely to be effective.

19. Where solutions are untested, we have not held back completely. Instead, we have introduced model frameworks or advisory guidelines for voluntary adoption.

20. We have also developed practical tools to help organisations meet their regulatory obligations, or raised governance standards. This will remain Singapore's approach to digital governance for the foreseeable future. It was, in fact, how we dealt with AI governance. I thank Dr Wan Rizal, Ms Sylvia Lim, Assoc Prof Jamus Lim and Ms Mariam Jaafar for emphasising the importance of responsible AI use and development.

21. Members may recall that even before we launched our first National AI Strategy (NAIS) in 2019, we had introduced a Model AI Governance Framework or MGF – the first of its kind in the region. In 2021, Singapore became one of the first in the world to develop a testing framework and software toolkit for safe and responsible AI, which we call AI Verify.

22. More recently, we committed to develop Advisory Guidelines on the use of personal data in AI systems, including safeguards to protect personal data of vulnerable groups like children.

23. Global conversations on AI governance are important. Singapore will continue to participate actively at international fora, such as the Global Partnership on AI and the United Nations' High Level Advisory Board on AI.

24. As mentioned by Ms Tan and Ms Mariam, we have refreshed our AI strategies through NAIS 2.0. We will soon update our recommendations on dealing with AI risks. For example, we are very concerned about the mis-use of generative AI to spread misinformation and carry out targeted scams.

25. Mitigating biasness and enhancing the explainability of AI models are also crucial to developing and deploying them responsibly. We aim to release MGF 2.0 for public consultation later this month.

26. Of all the risks in the digital domain, one category is particularly concerning – and they are scams. This was an issue raised by almost all MPs.

27. Recent concerns about scams may sound new, but are in fact very similar to past cases of fraud. Older Singaporeans may remember the sale of fake insurance policies in the 1970s. In 2006, Sunshine Empire, which disguised itself as a multi-level marketing company, operated a Ponzi Scheme that promised high returns on fake products and services. In the early 2010s, the SureWin4U Ponzi Scheme lured victims to invest in betting schemes against casinos.

28. These days, scammers use technology to sell fake jobs, fake love and fake discounted items like eggs or holiday packages. Through variety, speed and scale, they have claimed more victims than before. Whenever I speak with a scam victim and hear their harrowing experience, I am reminded of a very similar panic I experienced as a child.

29. Back in the 1970s, I lived with my grandmother in an old shophouse in Joo Chiat. On several occasions, we were awakened in the middle of the night to nearby shouts of "Fire! Fire!". We had very little clue as to how far and how fast the fire might reach us, only that we must be ready to run for our lives. And this kind of fear and helplessness – you will never forget it.

30. Today, fire hazards have largely been brought under control and most fire incidents have moderate impact. This is because we have well-trained and well-equipped firefighters to contain fires that do break out. There are regulations, including the Fire Safety Code, to prevent potential fire incidents. We also have the support of organisations and citizens alike, who do their part to create and maintain an environment that is safe from fires.

31. In many ways, we are fighting scams like how we successfully fought fires. We have invested resources to strengthen our capabilities to contain the impact of emerging scam campaigns. Two years ago, the Singapore Police Force (SPF) established the Anti-Scam Command (ASCom). This helps to facilitate the swift tracing of funds and freezing of scam-tainted bank accounts. In the first half of 2023, the ASCom froze over 9,000 bank accounts and recovered about $50.8 million of the victims' losses.

32. We have also put in place tools to limit losses for victims, much like the use of retardants to slow the spread of fires.

33. Banks have implemented an emergency "kill-switch", so customers can quickly suspend their accounts if they suspect compromise. In November last year, several

banks implemented a "Money Lock" feature, allowing customers to set aside an amount in their bank accounts that cannot be transferred digitally.

34. Another recent example is the lower default daily limit for online CPF withdrawals, which cannot be increased without strong user authentication. Members can also disable online CPF withdrawals easily by activating the CPF “Withdrawal Lock”, which instantly reduces this limit to $0.

35. Sir, these containment efforts are helpful but we really prefer to prevent the scams from happening in the first place. Preventive safeguards are easier said than done, as they require close coordination with industry. Several sets of measures have been or are being implemented.

36. First, we will keep closing off known avenues for scammers to reach prospective victims. Members will recall that not too long ago, scammers were spoofing the SMS IDs of key organisations to trick victims into giving their banking credentials. To counter this, IMDA introduced a novel solution. From January last year, all organisations that want to send SMSes using alphanumeric sender IDs had to register with the Singapore SMS Sender ID Registry (SSIR). SMSes from unregistered senders are labelled "Likely-SCAM" to alert phone users.

37. The SSIR has been effective. Cases of scam SMSes fell by 70% in the first three months that it was mandated and remain a minority – less than 5% – among new cases reported. Additionally, telcos have implemented firewalls within their networks to proactively block suspicious calls and calls that attempt to spoof local numbers. These efforts have also been helpful. The volume of suspicious

international calls blocked in 2023 has nearly doubled compared to a year ago. To further protect the public, telcos have now introduced an option for subscribers to block their mobile phones from receiving international calls, which is a common source of scam calls.

38. Sir, whilst we can introduce blocking measures, we must expect the scammers to keep starting fires in new ways. As mentioned by Mr Ong, scammers are increasingly abusing online platforms to deceive their potential victims. To deal with this more effectively, we introduced the Online Criminal Harms Act or OCHA, which will be progressively implemented from this year. Many Members supported the Bill and I thank them again.

39. This Act will allow authorities to order the swift blocking of online accounts or content suspected to be used for crimes, including scams. For the protection of consumer on high-risk platforms, we will also impose ex-ante requirements such as stricter requirements for identity verification.

40. The second set of preventive safeguards aim to disrupt fraudulent transactions, even after a victim has been tricked. This includes preventing Singpass accounts from being taken over. It is why last year, we introduced more friction into the authentication process for Singpass.

41. When conducting high-risk transactions, users are required to perform facial verification. To protect against impersonation attempts, which Ms Hazel Poa asked about, facial verification includes liveness checks, which guards against attacks such as using a still photo.

42. Facial verification was also introduced as an additional safeguard for high-risk CPF e-services. Since then, there have been no further losses to scams due to unauthorised CPF withdrawals.

43. Also last year, we observed the emergence of scammers exploiting malware to bypass existing safeguards and make unauthorised fraudulent transactions on victims' accounts. Having identified this new scam variant, we worked with the banks to enhance their fraud and malware detection capabilities. Compromised devices were prevented from transacting with the banks. We cannot quantify it but millions more dollars could otherwise have been lost.

44. Ultimately, our devices themselves must be better able to defend against malware attacks launched by scammers – Ms Tin spoke about this. We are therefore working with key industry players to enhance the security of mobile devices sold in Singapore. For instance, we are working with Google to design new features that can better detect and deter users from downloading malicious files onto Android devices.

45. The third set of measures involve harsher consequences to deter money mules from misusing our key digital services, such as Singpass, to perpetrate scams. We have recently tightened our legislation to criminalise individuals who intentionally disclose their Singpass credentials in aid of scams. We are also reviewing how to extend these principles to those who sell SIM cards to scammers.

46. Sir, fighting scams is a team effort and the Government cannot do it alone. Ms Tan spoke about the need for platform players, telcos and device manufacturers to do more to improve online safety for their users. We agree. As mentioned by Mr Ong and Mr Tan, we need companies to ensure that their customers can enjoy a safe and secure environment as they interact online.

47. Last August, OCBC was among the first banks in Singapore to disallow account access, if the bank app detected the presence of potentially risky mobile apps on the customers' devices. Some customers felt inconvenienced, but in fact, they may have been among those that were saved from at least $2 million in losses in the first month of roll-out. The Monetary Authority of Singapore (MAS) has since worked with other major banks to implement similar safeguards.

48. Several MPs also spoke about the need for larger companies to take more responsibility to mitigate scams by unauthorised transactions. This year, the upcoming Shared Responsibility Framework (SRF) will further enhance the accountability of the banks and telcos in protecting their customers from the threat of phishing scams. During the public consultation on the SRF, many suggestions were received, which are similar to those raised today. They relate to the expansion of coverage to more scam types and more entities, besides banks and telcos.

49. Sir, the SRF covers phishing scams because such scams were the main contributor to fraudulent transactions taking place without the customer’s knowledge and consent when SRF was first designed. Compared to the payout frameworks in other jurisdictions, which only impose obligations on banks, the SRF already holds a wider scope of entities accountable by including telcos.

50. Duties are also specified to clearly hold banks and telcos accountable to the victims. Even if there is no breach of duty and, hence, no payout under the SRF, there are other avenues of recourse for victims. These include banks' goodwill frameworks, which can provide some comfort to victims of new scam tactics. As was shared in Parliament last year, MAS has leaned on the banks to be more accommodative in applying their goodwill frameworks.

51. These complementary measures notwithstanding, the Government will consider how to enhance the accountability of key entities and strengthen protection for individuals within SRF or through other means that are available to us.

52. We hear the specific calls to include social media platforms and closed-messaging services, in particular, for scam variants involving malware and phishing that result in unauthorised transactions. I appreciate Mr Vikram Nair and Ms Hazel Poa's acknowledgment that there are trade-offs and moral hazards to consider and that the Government cannot take a one-size-fits-all approach.

53. With regard to physical tokens, these are available upon customer request. I should caution, however, that existing physical tokens may be resistant to malware, but they are still vulnerable to phishing tactics. Agencies are, therefore, studying longer-term solutions, such as the Fast Identity Online (FIDO) passkeys that were mentioned by Ms Tin.

54. Sir, I thank Members who have recognised the many steps we are taking and also the challenges our agencies face, such as those identified by Mr Vikram Nair. To

Mr Yip Hon Weng's suggestion to learn from best practices abroad, we have been proactive. Our efforts include exchanging information on the latest scam variants and strategies to combat scams.

55. However, all of these efforts notwithstanding, this may still beg the question, "Has Singapore been slack in fighting scams?"

56. On the contrary, Singapore is widely regarded as a leader in thought and action when it comes to battling scams. When interacting with our international counterparts, I can only share with you how much they marvel at some of the initiatives that we have put in place, which they consider quite unthinkable in their own context and still quite cutting edge. And these include: widespread call blocking, the SSIR and the kill switches that the banks and also CPF Board now use.

57. The fact that we have an Anti-Scam Command, which involves the co-location of banks and, soon, other entities that we are speaking with; the fact that we have ScamShield; and something that people in the trade are very interested about: the backend processes that none of us will get to talk about in this room – among the agencies and all the stakeholders to smoothen the process of following up on leads – that is something that they find very difficult to even bring about.

58. Many measures have also reduced the losses – stemmed the losses – to a very significant extent. So, then that begs the question, "What about these rankings that you come across that named Singapore as one of the top places in terms of how much victims have lost?"

59. Well, I can only say this. In many places, scam victims are not going to take the trouble to report the fact that they have been scammed. Because they do not expect whichever authority they report to, to be able to do anything about it. And so, when these kinds of ranking are a function of reporting, what this really tells us is that reporting levels in Singapore are very high. This is, of course, not to trivialise the amounts lost. But I think we have to recognise that fact.

60. In this regard, I think we also have to recognise that our members of the public have been quite remarkable in terms of their openness and willingness to pay attention to public education efforts on scams. I appreciate that it sometimes makes them quite anxious – because they keep hearing about it when they are at the bus stop; when they are at the void deck and they see the digital display panels; and then they go to a grassroots event and the Member of Parliament is also advising them to listen to the Police talk about anti-scam measures. So, I appreciate that it gives a certain sense of anxiety.

61. But it is an essential part of our overall scam defence which we cannot avoid and which we aim to fortify through a variety of means. And so, the question is: what more can we do?

62. First, let us take a step back and acknowledge that all countries recognise that when it comes to dealing with scams, there is really no silver bullet. There is not a single measure that you can implement and be done with it. In the trade, they call this a wicked problem. In cyber as well as in scams, you solve one problem, the bad actors are driven somewhere else and you have to start again.

63. Therefore, an agile approach is critical and a very good example is how we had to very quickly pivot to dealing with the malware-enabled scams which had not been conceived of before and had not been seen before. It is very easy to say: "You should have anticipated it." Not so easy in reality.

64. The last thing to do, in this context, is for us to politicise the debate or to vilify any group, because you do not know - when the next scam variant comes around – who you need to work with to try and solve the problem. So, vilifying any group is not a good idea and we should very consciously try to avoid this. This is a problem that has emerged and we have observed in other countries. This is one lesson that we are taking away. Do not go around vilifying various groups and saying: “You should have done this, you should have done that”. We will need them at some point. It is better to preserve the relationship and find ways to work together.

65. So, in this context, I was listening carefully to Members' contributions and I appreciate all of them a great deal. I could not help but notice that, amongst the Members who spoke from the Workers' Party, there was this term that was repeated quite a few times. This is what Mr Vikram Nair also responded to – he said that he disagreed with this idea that there is a crisis of confidence.

66. Now, I am not sure what the purpose of describing this problem in this way is. We do have a situation that we are dealing with, and we are taking it very seriously. But let me perhaps offer a viewpoint from the agencies and the officers who are looking at this problem and listening to this debate, and share what comes across to them.

67. This is almost like firefighters on the frontline. They are trying all ways and means to, firstly, figure out what is the terrain that they are working with, and trying to push back the fire, to not let it spread. And we have a group of bystanders who, instead of praying for them or encouraging them, are saying to them: “You should be doing this, you should be doing that” – pontificating.

68. And then, when they do manage to put out some fires with great effort, and are actually getting ready to fight the next fire – because they know it is coming– the very same bystanders say: "Thank goodness, I said that, how wonderful!”

69. I say to Members, have a care. This is a tough fight, for our agencies and all the people involved. There are not just public officers. Recognise the fact that there are also private sector players involved. It is hard work. And one of the Members said it is quite thankless. I believe it was Ms Hany Soh who said so and I appreciate her for acknowledging that. So, let us cheer them on. It is not so easy.

70. So, Sir, overall, I am still very glad that all parties support the Motion and have largely avoided grandstanding. I call on Members to please use your own networks and your social media influence not to spread these very easy labels to tag onto something like this, but to spread awareness of the tools that can really help people. I think that is a far better use of your social media influence. Use it appropriately.

71. And my humble appeal to all Members who have contributed your ideas and suggestions, please give our agencies time to consider the feedback and to prioritise what is most needle-moving. Because, actually, it will not be a matter of doing more, but doing more of the right things continuously. At any one time, we will be

introducing new measures while designing some more. In fact, I would like to announce three today.

72. As apps are the most common way to transact online, we also need app developers to design for security. This is why CSA is publishing a new recommended Safe App Standard that app developers should adopt to ensure that high-risk monetary transactions performed on their apps are secure.

73. The Standard will set out best practices that reduce the risk of malicious actors exploiting weaknesses in the app design. For example, apps could be designed to require additional authentication of a user before authorising high-risk transactions, such as those providing access to our assets or savings.

74. The Standard will also recommend that developers build in malware detection capabilities on their apps, since this feature has proven to be effective in disrupting scammers' unauthorised transactions using compromised devices. CSA will incorporate more of such effective practices in the Standard as they emerge or as the technologies evolve.

75. CSA will also consider how best to help end-users easily identify apps that meet the Standard. As the Standard is new, we will assess its usefulness in due course and whether to keep it voluntary or to make it mandatory.

76. Besides apps that people use, we must also better protect vulnerable segments. To strengthen safeguards against them being tricked into signing up and footing the

bills for phone lines used for scams, IMDA has published the Advisory Guidelines for telcos to protect vulnerable consumers.

77. It calls for measures to help frontline staff identify vulnerable consumers during service sign-up and handle cases of suspected exploitation. The Guidelines also encourage telcos to waive charges for vulnerable consumers who have fallen victim to scams. Arising from earlier cases encountered, MHA is also exploring ways to better protect the public, particularly those who continue to believe the scammers, despite being warned by the Police or even their own family members.

78. As the landscape evolves, we will need to grow new capabilities to keep pace with scammers and online risks. Several Members mentioned the misuse of deepfakes to create compelling pitches, such as the recent ads featuring our leaders' likeness to promote crypto scams. We are most concerned about this.

79. As a first step, MCI and the Agency for Science, Technology and Research (A*STAR) will officially launch the Centre for Advanced Technologies in Online Safety (CATOS). The Centre will be a platform to bring together our community of research partners, companies and practitioners in Singapore to build capabilities for a safer Internet.

80. Such capabilities may include tools and measures to: (i) detect harmful content, such as deepfakes and non-factual claims; (ii) inject watermarks or trace the origin of digital content; and (iii) empower vulnerable groups with resources to verify information they encounter online.

81. These research efforts will also help inform new legislation or regulations that we will need for issues, such as deepfakes, and which we are studying. As Ms Tan pointed out, even with extensive efforts by the Government and businesses, we must each do our part as individuals to remain vigilant online.

82. First, we should adopt measures that can mitigate the risk of scams, even if they may seem inconvenient or unnecessarily strict. This could mean downloading and enabling the ScamShield app or turning on multi-factor authentication for online services. We should avoid downloading apps from unfamiliar sources and avoid responding to suspicious videos promising guaranteed returns on investments or giveaways. When accessing websites, individuals should also exercise vigilance by always checking the URL in the address bar of their web browser.

83. We agree with Mr Ong that consumer banking and messaging service providers can do more to prompt users to adopt such habits. The Government will continue working with key industry players to further strengthen efforts to raise public awareness.

84. Second, we should educate ourselves on the latest scam trends and anti-scam measures such as those on ScamAlert.sg. We should use available tools to make more informed decisions when transacting online. These include the E-commerce Marketplace Transaction Safety Ratings (TSR), which provide information on how secure an e-commerce platform is against scams.

85. Even as we continue our efforts to stop scams and recover losses, we must not forget about the trauma experienced by victims. We understand the panic and anxiety that

victims go through. That is why the SPF has trained volunteer Victim Care Officers to provide emotional and practical support to victims. The Anti-Scam Resource Guide on SPF's website also sets out additional avenues of community support.

86. Mr Sharael Taha suggested reviewing the process of freezing bank accounts for the entire duration of the investigation period. SPF only freezes bank accounts when there is reason to suspect that they are involved in criminal activities. The time taken for investigations can differ from case to case.

87. Victims with frozen bank accounts may be offered new ones by banks, which may come with restricted access to certain facilities, or be subject to enhanced monitoring measures. But these will still meet basic banking needs such as receiving salaries and Government support. Victims can also make an application to the Courts to withdraw money for reasonable living or other legitimate expenses. Mr Speaker, please allow me to conclude in Mandarin.

88. 议长先生，我首先要重申支持陈佩玲女士所提出的动议。

89. 新加坡的数码化进程，确实让国人和本地企业受惠，创造了许多新机遇。可是，数码科技让生活更加便利的同时，也带来了新风险。这包括许多人都担心的数码诈骗。

90. 因此，政府在确保国人与时并进，把握机遇的同时，也竭尽所能加强数码领域的安全性，增强国人对于数码化进程的信心。

91. 为此，政府将打击诈骗列为重点工作，并落实了许多有效的措施。但是，骗子不会轻易放弃。 因此，我们也必须不断 “见招拆招”，提高整体的防卫能力，及时推出新措施，打击诈骗。

92. 政府即将推出三项新措施，以加强手机应用程序的安全性、对弱势用户的保护，以及研发先进的防诈科技。

93. 对付骗子，我们不可能一招制胜；也不能单靠政府来完成。这是一场持久的战役，更需要大家的配合。我相信，只要我们上下一心，携手对抗数码诈骗，骗子终究要打退堂鼓。

94. 谢谢。

###