SPEECH BY DR JANIL PUTHUCHEARY, SENIOR MINISTER OF STATE, MINISTRY OF COMMUNICATIONS AND INFORMATION AT THE MINISTRY COMMUNICATIONS AND INFORMATION COMMITTEE OF SUPPLY DEBATE, 2 MARCH 2021

1. Mr Chairman, I thank the various members for their cuts and questions and hope to address several of them in my response, especially those from Ms Jessica Tan, Mr Alex Yam, Mr Seah Kian Peng and Mr Xie Yao Quan and Mr Chris De Souza.

2. The digital space has had a deep impact on our daily lives. And this transformative effect will continue for some time. For many Singaporeans, digitalisation carries the promise of more convenience, efficiency and options. And as we do more online we face an increased risks of cyberattacks, online scams, and data breaches. We need safe and secure digital spaces. We need the online environment to be an enabler, so that our people can benefit from the opportunities of this digital age.

3. Today, I will focus on how we develop online safety and security - the strong foundations of our plans for digitalisation. Our strategies, have to cover a broad range, from infrastructure development, regulations, and partnerships. We need to address a wide variety of issues so our companies and our people can trust the digital systems that are so central to our lives.

4. Beyond assurance, we want people to step up, to be empowered, to take charge of their online safety, and to embrace the digital age with confidence. Strong foundations depend on a robust digital infrastructure. Our past investments in this digital infrastructure have recently enabled workers to switch to telecommuting, and students to attend online lessons with relative ease during the pandemic.

5. Looking ahead, we will need world-class, secure and resilient 5G networks. It was thus a policy priority for our nationwide 5G networks to be standalone - new standalone networks, 5G, all the way through from end-to-end. 5G standalone networks unlock the full suite of capabilities including network slicing, and ultra-reliable low latency communications, necessary for applications such as cloud gaming and smart factories. 5G deployment has started and by the end of next year, we will have at least 50% standalone outdoor coverage for 5G. And nationwide 5G standalone coverage will arrive by end-2025.

6. However, robust digital infrastructure alone cannot guarantee safe and secure spaces. Other keys to a strong foundation are a robust regulatory regime, and an approach to remain relevant, and fit-for-purpose amidst the evolving technological landscape.

7. Data is a critical resource used to inform business decisions and also power emerging technologies such as Artificial Intelligence. Personal data requires strong safeguards and accountability.

8. There is a balance we need to strike. Overcorrecting for business innovation could undermine consumer protection, privacy and trust; on the other hand, pursuing consumer interest narrowly could hamper business development. The public may ultimately suffer from poorer and more costly services. Our strong foundations, therefore alsoneed us to be agile and calibrated.

9. We recently amended the Personal Data Protection Act (PDPA). You may subscribe, for example, to the mailing list of an online shop, and as a result, you can receive customised recommendations based on your browsing history or based on your prior transactions, this is a benefit to you as the customer, as the consumer, for having shared your data.

10. Under the amended PDPA, if there is a data breach which may cause significant harm to affected individuals, you are to be notified directly by the shop so you can take timely, proactive measures to protect your data, such as by changing your passwords. If you choose to opt out of the mailing list, the shop is required to remove your details from the mailing list, and stop sending you recommendations within a reasonable period. So, businesses are now held to a higher standard with more transparent and accountable practices.

11. Like data, electronic transactions are also central to the global economy. To support wider digitalisation, Parliament passed the amendment to the Electronic Transactions Act this year to adopt the Model Law on Electronic Transferable Records from the United Nations Commission on International Trade Law (UNCITRAL).

12. The shipping, logistics and finance sectors now stand to benefit from faster and more secure electronic transactions, compared to the paper-based transactions. We expect to see benefits in terms of efficiency, productivity and hopefully cost savings as well.

13. One concern arising from our digital push is the rise in online scams. In Singapore the most common type of scams relates to E-commerce, and these increased by almost 20% from 2019. Overall, victims to scams lost more than $200 million last year .

14. We take this matter very seriously and are working across Government to tackle these scams. For example, we require telcos to attach the “+” symbol for all incoming overseas calls. IMDA also requires Telcos to enhance capabilities to block calls from commonly spoofed numbers. As a result, 28 million suspected scam calls were blocked in the fourth quarter of last year.

15. However, given the dynamic and evolving behaviour of scammers, existing solutions to block scam calls from overseas will never be foolproof. Today, no telco can verify with absolute certainty that a given incoming call is fraudulent. So, IMDA is working with the telcos to build new analytic capabilities within their networks to better identify and block spoofed calls with numbers that appear local, without blocking legitimate calls. These measures fit into what the Ministry of Home Affairs (MHA) is doing in terms of their broader approach to mitigate scams. We will continue to work closely with MHA through the Inter-Ministry Committee on Scams.

16. Cybersecurity threats are growing in both number and sophistication. Members have just heard about the recent SolarWinds breach. This cyberattack compromised a network management software used extensively by major companies and Governments worldwide. Notably, the software that was compromised was trusted and had privileged access to internal networks. It was a very sophisticated attack that went undetected for months. Closer to home, Singtel reported that some files were taken as a result of a breach to FTA, a third-party file sharing system that Singtel uses.

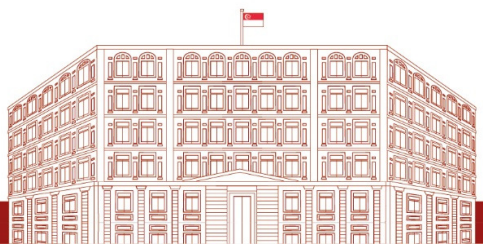
17. Singaporeans are concerned about whether our systems are safe, so are we, and sensitive information needs to be sufficiently protected. With more activities taking place online, it is important that people trust the digital systems we use to store, collect and transfer our information.

18. The reality is that we will not be able to prevent every cyberattack - malicious actors only need to exploit one vulnerability to compromise our systems, while defenders must safeguard systems under their charge against all threats, all the time.

19. Consistent and deliberate efforts to strengthen our cybersecurity are thus critical. Many essential services like banking and healthcare are powered by information and communications technology. These systems are our Critical Information Infrastructure or CIIs. Today, all CII owners must maintain a mandatory level of cybersecurity as part of the Cybersecurity Act.

20. However, we also recognise that most organisations, including CII owners, engage vendors to support their operations. Therefore, we also need to manage cybersecurity risks across the supply chain. Doing so requires CII owners to have a better understanding of their vendors to identify systemic risks and improve the level of cyber hygiene with the vendors.

21. To this end, we are developing a CII Supply Chain Programme - a partnership involving all stakeholders - CSA, CII owners, and their vendors.This programme will provide recommended processes and sound practices for all stakeholders to manage cybersecurity risks in the supply chain. In the discussions that we will have



with the stakeholders as a result of this programme, will also help the Government improve our policies around supply chain risks.

22. In the longer term, our CII sectors and the companies will also need to adopt a zero-trust cybersecurity posture. This shift in mindset is necessary to defend against supply chain attacks by highly sophisticated threat actors, such as those behind the SolarWinds breach. In concrete terms, this means that CII owners should not trust digital activity in their networks without verification. They should also authenticate continuously, detect anomalies in a timely manner, and validate transactions across network segments.

23. This work will continue and will become increasingly complex in the future. Cybersecurity, therefore has to be a collective effort and a core part of our lives in this digital age - integrated into the products we use and the way that we behave online.

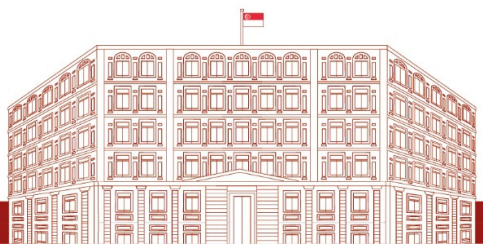
24. As more enterprises go digital, our exposure to cyber threats grows in parallel. Cyber attacks on companies have a far-reaching impact on our wider economy. So, as part of the Safer Cyberspace Masterplan, CSA will launch the SG Cyber Safe Programme to support companies in strengthening their cybersecurity. It comprises two parts:

25. First, we will provide informational resources and educational material for key roles including C-suite executives, cybersecurity teams, and frontline employees, based on their specific roles and knowledge needs. We need to shift attitudes and raise cybersecurity awareness through in-house training.

26. Second, we will roll out a voluntary SG Cyber Safe Trustmark to provide a mark of distinction for companies that invest in cybersecurity. What this means is that if you are looking for an HR processing service for instance, and care about the cybersecurity level of the service provider, you may look out for the trustmark for added assurance that the service provider takes its cybersecurity seriously. CSA will engage stakeholders regarding the specifics of the Trustmark from April this year.

27. Our cybersecurity talent base is a key enabler of these efforts and we are working closely with industry partners and Government agencies to nurture and grow our cybersecurity workforce

28. First, to meet near-term demand, we facilitate the training and upskilling of cybersecurity professionals, as well as fresh and mid-career non-cybersecurity professionals for cybersecurity jobs, through programmes such as IMDA's Tech Skills Accelerator.



29. Second, to strengthen our talent pipeline for the longer term, we encourage youths to pursue a career in the field through cyber outreach initiatives like SG Cyber Talent. We have engaged over 7,000 participants to-date.

30. Thirdly, to groom world-class cybersecurity leaders, we launched the SG Cyber Leaders programme to create a community for current and developing cyber leaders to exchange ideas, and learn about global best practices.

31. All of us need to play our part to create a safer, more secure cyberspace. There are things we can do as individuals. We should enable two-factor authentication, update our software in a timely manner, choose a passphrase rather than a password and staying vigilant to spot signs of phishing. But there are also things that we do as a country. Singapore participates actively in international discussions to develop and implement norms in line with our interests.

32. As cyber threats are global and transborder, we are working closely with international partners across the UN and ASEAN to develop and implement norms for responsible State behaviour. For instance, we are producing an implementation checklist with specific actions that countries can take to implement cyber norms. This effort contributes to a rules-based multilateral order in cyberspace, and gives all states, big or small, confidence, predictability, and stability, essential for economic progress, job creation, and technology adoption.

33. In terms of AI governance, Singapore takes an open and collaborative approach to govern the use of AI, recognising that we need to safeguard consumers' interest and facilitate innovation.

34. We launched the second edition of the Model AI Governance Framework in 2020, which incorporates feedback and examples from international and local companies across a diverse set of sectors, in response to the first edition of the Framework. It translates key ethical AI principles such as human centricity into practical measures, in line with our National AI Strategy.

35. Ultimately, we lay all of these strong foundations so that our people can look ahead, and reap the full benefits of the digital economy. We will remain open and integrated with the global economy to enable our companies to maximise opportunities beyond our shores.

36. While our existing trade agreements meet the needs of traditional trade in goods and services, we recognise the need for new norms and rules to support cross-border digital transactions like e-invoicing, data flows and digital identities. This is why Singapore pioneered Digital Economy Agreements, or DEAs, building on our existing networks and initiatives. These DEAs facilitate seamless end-to-end digital trade, enable trusted data flows, and build trust in digital systems. Beyond these

DEAs, businesses can look forward to further support for transferring data to and from overseas seamlessly and securely.

37. Regionally, Singapore led the development of an ASEAN Model Contractual Clauses, terms and conditions that may be included in legally binding contracts for the transfer of personal data across borders. We also led the development of an ASEAN Data Management Framework - a guide for businesses to implement a data management system with appropriate data protection safeguards. With ready-to-use and flexible templates to transfer personal data, businesses operating in ASEAN markets stand to benefit from shorter contract negotiations on data flows.

38. In conclusion, our success in digitalisation has also exposed new vulnerabilities. These will only grow as technologies evolve and become more complex.

39. Trust in our digital systems is key to the success of our digital economy efforts. And without trust to transact, or to innovate, our best efforts to develop our digital ecosystem and reap the dividends will fall short. Strong foundations such as I have described will fortify our defences against online threats, and support this trust that we need to grow But they are not sufficient. We need our companies and people to be aware of the risks, vigilant of their manifestations of these risks, and make informed choices to protect our safety.

40. We can and must make the online space more secure and more trusted, and thus create more opportunities, for all of us.

41. Thank you, Mr Chairman.