

**OPENING REMARKS BY SENIOR MINISTER TEO CHEE HEAN
AT THE PUBLIC SECTOR DATA SECURITY REVIEW COMMITTEE
PRESS CONFERENCE ON 27 NOVEMBER 2019**

Good morning everyone and thank you for attending the press conference.

Work of the PSDSRC

2 As you know, in 2018 and 2019, we uncovered a number of data-related incidents in the public sector. In response to these incidents, the government had immediately introduced additional IT security measures. Some of these measures included network traffic and database activity monitoring, and endpoint detection and response for all critical information infrastructure. But, there was a need for a more comprehensive look at public sector data security.

3 On 31 March this year, the Prime Minister directed that I chair a Committee to conduct a comprehensive review of data security policies and practices across the public sector.

4 I therefore convened a Committee, which consisted of my colleagues from government - Dr Vivian Balakrishnan, Mr S Iswaran, Mr Chan Chun Sing, and Dr Janil Puthucheary - as well as five international and private sector representatives with expertise in data security and technology. If I may just provide the background of these five private sector members:

- We have Professor Anthony Finkelstein, Chief Scientific Adviser for National Security to the UK Government and an expert in the area of data and cyber security;
- We have Mr David Gledhill who is with us today. He is the former Chief Information Officer of DBS and has a lot of experience in applying these measures in the financial and banking sector;
- We have Mr Ho Wah Lee, a former KPMG partner with 30 years of experience in information security, auditing and related issues across a whole range of entities in the private and public sector;
- We have Mr Lee Fook Sun, who is the Executive Chairman of Ensign Infosecurity. He has long experience in both the private and public sector in infosecurity and other information and C4I-related matters;
- We have Sir Andrew Witty, who is the Chief Executive of Optum. He has extensive experience in the healthcare industry. The healthcare industry is one of the critical areas where data security is particularly sensitive.

These were the reasons why we chose these particular members to join us in the Committee.

5 Over the last eight months, the Committee has carried out an in-depth inspection of 336 systems in all 94 public sector agencies. The Committee also considered the best international data security practices in the finance and health sectors, and studied the practices in other countries, including Canada and the United Kingdom.

6 These countries face the same challenges as we do:

- a. To use data securely and effectively to make better policy decisions
- b. To deliver high quality public services to citizens, and
- c. To assure the public that their data entrusted to public agencies is well protected.

Key Recommendations

7 The Committee has made five key recommendations to achieve this:

- First, we will enhance technology and processes to effectively protect data against security threats and prevent data compromises.
- Second, even as we do the utmost to prevent data incidents, these can never be fully eliminated; we will strengthen processes to detect and respond to data incidents swiftly and effectively and learn from each incident.
- Third, we will build data security competencies and inculcate a culture of excellence around sharing and using data securely for the whole Public Service.
- Fourth, we will enhance frameworks and processes to improve the accountability and transparency of the public sector data security regime.
- Fifth, we will ensure that our data security efforts are not one-off, but sustained and continue to evolve to address future challenges. As you know, this is a very rapidly evolving sphere.

Government Accepts the Committee's Recommendations

8 The Prime Minister has accepted the Committee's recommendations and action plan to implement the recommendations. The Public Sector will

implement these recommendations expeditiously and thoughtfully so that Singaporeans can be confident that the Government takes data security seriously and will do the utmost to protect citizens' data.

9 Three of the technical measures recommended have already been implemented in October this year. By end 2021, we will implement all the relevant recommended measures in 80% of government systems. By end 2023 we will implement them in the remaining 20% of government systems. These systems are the ones which are most complex or will require significant redesign. In the meantime, we will have processes and measures to cover the risks.

Ensuring that Recommended Measures will address Existing and Future Threats

10 These measures will significantly enhance safeguards and hold officers to account. They are comparable to international and industry best practices. The public sector will also ensure that our data security efforts are not one-off, but sustained and continue to evolve to address future challenges.

11 The way that we will do so is to have the Digital Government Executive Committee, an existing committee chaired by the Permanent Secretary of the Smart Nation and Digital Government Office, who oversee all public sector data security and drive the implementation of the Committee's recommendations.

12 GovTech will build up capabilities in data protection and privacy preservation to deepen the Government's expertise in these areas and keep abreast of the latest developments.

13 The Committee checked and satisfied itself that the recommended measures would have prevented or minimised the impact of the past data incidents in the public and public healthcare sectors.

14 While we will do our utmost to reduce the risk of data breaches, we cannot completely eliminate the threat. When such breaches do occur, we will detect them and respond quickly and effectively to limit the breach and damage.

15 Ensuring that we can use and share data effectively and do so securely is a continuing effort. Our public officers and agencies will continue to work closely

with industry, experts, and members of the public to maintain public sector data security, and deliver high quality services to our citizens.

16 Finally, I would like to thank the members of the Committee. We also have an Expert Group, one of its members is with us today - Professor Simon Chesterman who is an expert in privacy law. I would also like to thank all those who have contributed their views and ideas to the work of the Committee in one way or another. Thank you.