SPEECH BY MR AUBECK KAM, PERMANENT SECRETARY, MINISTRY OF COMMUNICATIONS AND INFORMATION AT THE ABS-MAS TECHNOLOGY RISK CONFERENCE 2016 ON 17 NOVEMBER 2016 (THURSDAY) AT 9.00 A.M. AT MARINA BAY SANDS

Mr Wee Ee Cheong, Chairman of the Association of Banks in Singapore

Ladies and Gentlemen

Thank you very much for the invitation and the opportunity to speak at your Technology Risk Conference. It is in my view very fitting that while the first two days of the FinTech Festival have rightly focused on innovation in FinTech, we approach the end of the Festival with a conference dedicated to the deliberation of security and risk in FinTech.

2 This is symbolic of the judicious balance between innovation and security, and all of us have to maintain this balance at all times. If the FinTech sector succeeds in this, then we can all look forward to a trusted, smart and secure financial sector.

3 Last month, Prime Minister Lee Hsien Loong launched Singapore's Cybersecurity Strategy. The Cybersecurity Strategy outlines Singapore's vision, goals and priorities in this very vital domain. It was produced by the Cyber Security Agency of Singapore, which is an agency in the Prime Minister's Office, and is managed by the Ministry of Communications and Information.

4 The Strategy is a 50-page publication. Please don't worry – it is not my plan this morning to walk you through the entire 50 page strategy. Instead, from the many ideas described in the strategy, I want to pick out three points for reflection. These are:

(a) Firstly – the concept of "security by design"
(b) Secondly – how do we create the right incentives and structure that enable security to be part of the corporate and organisational agenda
(c) Thirdly – how do we avoid fighting the last war

5 Let me start with security by design. Security by Design is the approach that Singapore has decided it must adopt, in order to secure its critical information infrastructure, or CII. What do we mean by security-by-design? It is a simple concept, but implementation requires persistence, discipline and rigour. In security-by-design, we strive to develop a system with security considerations integrated from the design stage, and all the way through its lifecycle, to disposal.

6 Our belief is that security-by-design is superior to the alternative. What is the alternative? Piecemeal security which requires retrofitting after delivery, and which is not only more likely to be costly, but also more likely to be ineffective.

7 I am reminded of something that Winston Churchill said, at the end of the Second Battle of El Alamein. He said (I quote): "This is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning."

8 The same can be said for security-by-design. If, by the end of the beginning, it still has not made an appearance and influenced the system design, then I am afraid it will not take very long before one finds that it is the beginning of the end.

9 Recently, the DNS servers of US Internet Service Provider DYN were overwhelmed in a Distributed Denial of Service attack. The botnet was traced to insecure Internet-of-Things devices such as web cameras that have become commonplace in homes. As we all learnt, for some of these IoT devices, it was impossible to patch them, even after discovering they were compromised. So much so that one manufacturer had to issue a product recall. I think this case establishes a very interesting precedent – that an IoT device that is not secure-by-design, is potentially not fit for purpose. If you think about it, there isn't any reason why the same principle would not apply to a financial product, service or platform.

10 Thus, given all the excitement around innovative FinTech, I am heartened that my colleague Mr Ravi Menon, the Managing Director of the Monetary Authority of Singapore, said in June 2015 that: "The first priority on our journey towards a Smart Financial Centre is to continually strengthen the industry's cybersecurity".

11 Secondly, even as the industry embraces innovative FinTech solutions, I would encourage the financial sector to give thought to how it can provide the incentives and structure to keep security in the corporate and organisational agenda.

12 In our Cybersecurity Strategy, it was noted that Government systems are one of the critical sectors and that the Government has undertaken to work towards the goal of setting aside up to 8% of our ICT expenditure on cybersecurity. Here, I should credit our Israeli friends, in particular, Professor Isaac Ben-Israel, for pointing us in this direction.

13 Why did we commit ourselves to this doing this? The first thing I would say is that the 8% figure is not a spending target. Spending more money does not guarantee you greater security.

14 The real value to establishing this 8% figure, is to change the mindset towards cybersecurity expenditure. It should be something that you make a budgetary allocation for, so that you can be assured that your priorities are reflected not just in words, but in action. You cannot have security-by-design, if the underlying mindset is that for every $100 you have, you'd like to spend it all on the fanciest user features.

15 Instead, what we hope to bring about, at least in Government IT, is that for every $100 available, we set aside $92 dollars to deliver the best bang for the buck in user experience, features, and so on. But to have $8 available for necessary cybersecurity measures. And if it turns out that it is not necessary to spend all of the $8, then it is not a bad thing to return that to the Treasury as savings. After all, I am sure many of you will agree that rare is the IT project that actually comes in under the budget!

16 What does it mean for the private sector? Well, we hope that the Government's practice provides a point of comparison for board directors, risk committees, and those involved in strategic company discussions. I believe there are many other approaches that will be discovered, if organisations are prepared to

explore and experiment. And we in Government would be happy to learn from. For example, would organisations be prepared to set aside some funds to support a bug bounty program for their services? Software companies already do this today, and some car companies have reportedly begun to offer the same.

17 Thirdly, how do we avoid fighting the last war. I think this is especially pertinent for the financial sector. The financial sector is one of the pathfinders in building up capabilities to safeguard the Financial CII. But even as the CSA, MAS and financial institutions work hard to enhance the resilience of the Financial CII, we are already beginning to realise that the financial sector is so globally networked, that it is no longer sufficient to conceive of defending CII. Instead, the financial sector may be one type of Supra Information Infrastructure (or SII). Cyber threats directed at another major financial centre may have knock on effects on Singapore, and vice versa. This makes international cooperation between states and between private organisations even more important.

18 In conclusion, I would like to end with a vote of confidence in the ability of the financial sector to rise to the challenge posed by varied and evolving cyber threats. Over the years, the industry, working closely with the MAS, have built up a strong and credible cyber-response plan. They have been validated through sectoral and cross-sector cyber security exercises. MAS's regulatory measures covering areas such as regular vulnerability assessments and penetration tests, and regular onsite inspections of financial institutions' technology risk management processes and controls also help to maintain high standards overall. I am also happy to note that the financial sector is one of the leading sectors in the practice of information sharing, through channels such as the Financial Services Information & Analysis Centre.

19 It remains for me to congratulate the ABS and the MAS for organising this Conference. I hope that the discussions here will be fruitful and ultimately lead to an even more cyber-secure financial industry, for the benefit of all.

20 Thank you.