Ministry of Communications and Information
An Engaged and Connected Singapore

OPENING ADDRESS BY DR JANIL PUTHUCHEARY

SENIOR MINISTER OF STATE (SMS), MINISTRY OF COMMUNICATIONS AND INFORMATION, SMS-IN-CHARGE OF CYBERSECURITY AND GOVTECH

AT INAUGURAL ASSOCIATION OF INFORMATION SECURITY PROFESSIONALS (AISP) INTERNET-OF-THINGS (IOT) INNOVATION DAY 2022

ON 11th MAY 2022

A Balanced Approach to Harness IoT Innovation for Smart City Building

President of AiSP Executive Committee Mr. Johnny Kho
Distinguished guests
Speakers and delegates
Ladies and gentlemen

1. It is my pleasure to speak to you today at AiSP's inaugural IoT Innovation Day 2022. Let me begin by thanking everyone in attendance today for your continued efforts and contributions to support our mission in building a secure and trusted IoT ecosystem.

Balancing Security and Innovation in building Smart Cities

2. COVID-19 is still the factor that has driven digitalisation faster than anything else in our recent history and has also catalysed new trends. This is especially so in the IoT space, as nations and cities are transforming into smart cities and the experience of the public health issues over the last couple of years and the experience of the population in urban environment has led leadership in cities to understand that there is a greater need for connectivity and the ability to harness the data that this generates. By 2025, the estimated amount of data generated every day is expected to reach 463 exabytes, or 463 billion gigabytes, which is equivalent to roughly 60 hours of Netflix movies, per person daily, which is a phenomenal amount of surface area and volume of material to manage, govern and most importantly, protect.

3. IoT is becoming an increasingly integral part of our daily lives, as much of our work and social interactions are taking place online. We have smart home devices to help us automate our daily tasks, sensors that help city planners gather accurate data on traffic, temperature and other municipal indicators, and personal trackers to help monitor our health. Our lives have been made more convenient and productive with innovations in IoT.

4. Notwithstanding the opportunities that IoT and digitalisation bring, we need to also think about the downsides and risks that come with such pervasive adoption of these devices. We need to mitigate, counter, adapt to these risks. Unfortunately, a majority of the consumer IoT devices are built and developed to optimise functionality and cost usually at the expense of the security of the device. What we need to do, whether in government, as professionals or a community of practice, is to persuade people that IoT security cannot be an afterthought, but instead a key consideration and a design fundamental. Without the requisite security in IoT, end users are exposed to malicious cyber threat actors seeking to compromise the devices. Aside from just the loss of data, privacy and trust will also be compromised. Therefore, while we continue to push the boundaries in IoT and development of smart cities, we should find ways to ensure that our solutions can also remain secure and safe.

Two Ways to Promote IoT Innovation

Putting in the right enablers to support Innovation

5. IoT innovation can support our Smart Nation vision, and cybersecurity will need to be in the heart of such innovation. This can be done by tapping on three enablers:

a. First, a deep understanding of the problems and challenges that people face in their use of IoT devices;
b. Second, partnerships and work with the industry to generate innovative, yet secure ideas and solutions for IoT applications and devices; and
c. Third, ensure that the people building and overseeing these solutions have the appropriate skillsets to safeguard our IoT ecosystems.

6. As a first step, the government partners with industry and citizens to gather views and problem statements on how IoT technology can be improved to better impact their businesses and lives. For example, earlier this year, we launched the Smart Nation Ambassadors Citizen Co-Creation Group. This group comprises Smart Nation Ambassadors, who are community leaders representing diverse groups. Communities represented include persons with disabilities, low-income families, seniors, clan associations and SMEs. Through these discussions, we have a better understanding of how IoT solutions can be used in future Smart City planning and identify new ways to address gaps on digital inclusion.

7. On the same note, the industry can have the ability to generate innovative ideas and translate them into implementable solutions for future smart cities. One way we do this is through the Cybersecurity Industry Call for Innovation, whereby the public and private sectors jointly identify cybersecurity challenges, match them with industry proposals and support the development of customised solutions that can meet national needs. Since 2018, we have supported close to 20 innovative projects and provided them with more than $10 million in funding. Their innovations have benefited multiple industries, from the maritime to the healthcare sectors, which can impact our daily lives.

8. One example of an innovative IoT project that we supported through the Cybersecurity Industry Call for Innovation was the Micro Public Key Infrastructure (or Micro-PKI) project by MicroSec Private Limited – a cybersecurity solutions company based in Singapore. The technology that was developed was eventually deployed to secure large and complex commercial IoT systems from cyber threats around the world.

9. Finally, we also make sure to the equip our workforce with the appropriate skillsets to not only be able to manage our day-to-day operations, but also ensure that our systems remain secure. This is not just the responsibility of cybersecurity professionals, but also those in adjacent roles such as IT specialists, auditors and engineers, and also those in leadership positions need to be equipped with the

necessary cybersecurity knowledge. We have several initiatives to support our ICT workforce at different points of their career.

a. The Cybersecurity Associates and Technologists Programme (CSAT) helps to bridge the skills gap for mid-career professionals looking to do a career conversion into cybersecurity roles by equipping them with practical, in-demand skills, through a combination of on-the-job training, networking and industry attachments.

b. At the same time, our SG Cyber Talent programme also support our cybersecurity workforce with upskilling opportunities in emerging technologies, such as IoT.

New and Innovative Ways to Promulgate Cybersecurity Practices

10. Beyond just creating the right enablers, the Government also constantly finds new ways to ensure that our innovative ideas can be translated directly into impact in our daily lives. At the end of the day, we do not just protect systems, but people and communities.

11. First, we are working closely with our industry partners and developers to signal that cybersecurity must be one of the core considerations when coming up with IoT devices. One example of how Singapore is working with the industry towards investing more in innovative cybersecurity practices is through the use of the Cybersecurity Labelling Scheme, which helps consumers to select – and hence reward – companies that produce more secure products. This has attracted international attention and interest. Since its launch in 2020, we have received more than 250 applications and there are now close to 150 labelled IoT products available in physical stores and online shops. Some of the products include routers, smart home appliances, IP cameras and door locks, which are used pervasively by households. In my role as the MP in Punggol, where SIT and the Punggol Digital District will be located, I do see a lot of new flats when I do my block visits. Over the years, I have noticed more of these new BTO flats have smart digital home locks and connected devices. Sometimes when I press the

doorbell button, the door is answered but the person is not home, but they are meeting their MP remotely through this smart technology while they are visiting their parents or still at work. This is an encouraging start, to see the pervasive adoption of such technology, and that people have the trust in this technology, to use it in a very personal way, at the front of their home. So it is a good start, we are getting it going. And as more products and companies come onboard, I am certain that we can develop more products that are innovative and yet ensure that our cybersecurity posture is not compromised.

12. We are also investing heavily in the Government to ensure that cybersecurity measures are made simpler and easier to understand for our users. For example, our government cyber specialists at GovTech developed AI-enabled automated tools that can send out mock phishing emails customised to different public officer profiles. This allows us to conduct more realistic, personalised, yet scalable training exercises to better educate our public service officers. Ideas like these were inspired by research on the performance of AI-generated content online, and they demonstrate how we can be creative in our approach towards online security.

The Importance of Partnerships in Cybersecurity

13. I have said several times that it is for the government to work closely with local companies and partners to build up our national cybersecurity capabilities, while we constantly innovate to develop new IoT applications. This is especially since cybersecurity is a team sport, and it is not something the government or any one organisation can achieve alone. We look to partners and the industry to spur us on to greater excellence.

14. For example, our whitehats regularly participate in internationally-renowned Capture the Flag competitions to pit themselves against hundreds of international participants. We also run bug bounty programmes, the most recent being the Vulnerability Rewards Programme (VRP). Launched in Aug 2021, VRP offers rewards of up to US$150,000 to any ethical hacker reporting vulnerabilities in critical

government systems. These efforts cannot be done by government alone, but with industry partnership, professionals and associations who see the value and bring others along to the table. Through our earlier bug bounty and vulnerability disclosure programmes, we have engaged over 1000 white-hat hackers and discovered over 700 valid vulnerabilities. These programmes ensure that government systems are continuously tested. They enable the government to benchmark our defences against the global community of ethical hackers and build greater confidence in our digital solutions.

15. To develop the broader ecosystem, we also have ongoing programmes such as the National Cybersecurity R&D Programme, launched in 2013. Under the Programme, R&D Centres will work together to establish longer-term receptacles and help Singapore build deep capabilities. The Programme will also continue to support shared research infrastructure, such as realistic testing environments and high-end equipment. We will also fund scholarships and grants for translating innovations into capabilities – bring the ideas out of the university and into the real world. To date, several cybersecurity spin-offs have been generated from this, such as Zilliqa, which created the world's first sharding-based blockchain platform, and Datakrew, which provides IoT device security via an integrated platform for large-scale IoT applications.

Signing of Memorandum of Understanding (MoU) between AiSP and Singapore Institute of Technology (SIT)

16. Given the importance of partnerships, it makes me happy to be able to witness the signing of the Memorandum of Understanding (MoU) between AISP and SIT. SIT offers Singapore's first undergraduate degree programme that majors in information security and trains students to take on real cyber threats in an authentic environment. This MoU is a step towards enhancing the cybersecurity ecosystem in Singapore, as we work towards building of smart cities in towns such as the Punggol Digital District.

17. Through this MoU, both organisations will work together to conduct training courses to raise the professional competency of information security personnel in

Singapore, as well as share best practices in the cybersecurity community. SIT students will benefit from initiatives such as IoT events, AiSP's Ladies in Cyber mentoring programme, and the Student Volunteer Recognition Programme for them to contribute to the ecosystem, making them part of the ecosystem while they are still engaged in their studies.

18. Come 2024, these activities will progressively be anchored in Punggol Digital District (PDD) – Singapore's first tech-enabled Smart District. PDD will house digital leaders in key growing tech sectors such as Blockchain and Fintech, and cybersecurity. The Government Technology Agency, Cyber Security Agency of Singapore, as well as many of our most prominent professional associations in the cybersecurity and tech sectors like AiSP, will add vibrancy to the growing ecosystem in PDD with their partnerships, programmes and activities. With AiSP's move into PDD, the co-location with businesses and student talents in PDD will provide AiSP access to companies and young talents at close quarters, so students will not only have this opportunity to train but also to practice with industry, which is one of the key value propositions of the design of PDD.

19. On this note, I would like to thank you all for your attendance and support for the AISP IoT Innovation Day. Thank you to all of you for coming and getting together in person. This is an important step in our confidence in getting real world events going again, just as we have to build confidence in our online cybersecurity world as well. I will now hand the time back to AiSP and SIT for the MOU signing. Thank you, and I look forward to seeing the fruits of this collaboration and the active participation from the cybersecurity community.