Ministry of Communications and Information
An Engaged and Connected Singapore

OPENING ADDRESS BY SENIOR MINISTER OF STATE, MINISTRY OF COMMUNICATIONS AND INFORMATION, DR JANIL PUTHUCHEARY AT INTERNATIONAL IOT SECURITY ROUNDTABLE 2022

20 OCTOBER 2022

Strengthening the Security of our Internet of Things Ecosystem

Ladies and gentlemen,

1. Good afternoon. Thank you for joining us at the International IoT Security Roundtable event of the 7th Singapore International Cyber Week (SICW).

2. This is the first time since the pandemic that we have been able to gather everyone in person for this roundtable. I thank everyone for your support and contributions to securing our IoT ecosystem. Especially those of you that have taken the trouble to come here to Singapore in person, not just to attend the events, but also to meet your counterparts and fellow cybersecurity professionals from around the world.

The Rapidly Growing IoT Market

3. The IoT market has been growing rapidly. It is estimated that there will be some 50 billion IoT devices in use around the world by 2030. IoT is very much part of our lives now.

    a. More and more smart devices are appearing in our homes – from digital locks, lighting, to kitchen appliances such as refrigerators, microwaves and coffee machines. Many of us use smart home hubs to control all these with a touch on your mobile app.

    b. Outside the home, IoT devices are also being used to make cities smart. In Singapore, we are deploying smart lamp posts to help detect environmental conditions, traffic conditions etc., which would in turn give us more data and make better decisions for urban planning. Looking abroad, smart traffic lights in Pittsburg are used to monitor and control traffic flows. This reduced intersection wait times by 41%, which led to a 21% reduction in vehicle emissions [1],
    c. Our medical devices, such as ECG monitors, pacemakers, are also getting smarter as healthcare companies and professionals seek to leverage technology to improve their ability to collect patient data, deliver therapy, or customise therapy.

4. When we think about IoT devices, convenience and efficiency are top of mind, but not necessarily security and safety of the users. The lack of strong IoT security can pose serious risks. Many consumer IoT devices contain a cache of consumer data and information that, if leaked, could compromise consumer privacy. There were cases over the last couple years where some unsecured home security cameras in Singapore were hacked, and the stolen footage were sold online.

5. In more severe cases, IoT hacks can lead to serious physical harms, even risking lives.

    a. For example, in 2017, the FDA discovered a serious vulnerability in pacemakers made by St Jude Medical which made it possible to hack pacemakers and alter its functioning, deplete its battery and potentially even administer fatal shocks to the wearer.

[1] IoT in Smart Cities in 2022, 17 Jan 2022, Datamation

Expanding the CLS for a more secure IoT ecosystem

6. This is why we need to take IoT security seriously. In Singapore, we introduced the Singapore's Cybersecurity Labelling Scheme (CLS) in 2020 to provide a way for consumers to make more informed choices when buying IoT devices. A higher rating means a more secure device. In this way, we hope to encourage IoT device manufacturers to make more products with cybersecurity in mind, and differentiate themselves from their competitors. The CLS is open for all consumer IoT devices, such as Wi-Fi Routers, Smart Home Hubs and household appliances. Since then, CSA has received more than 300 applications, and has certified more than 200 products.

7. The CLS has also gained much traction internationally. Singapore and Finland now have an agreement to mutually recognise each other's IoT cybersecurity labels, and I am proud to say that since the signing, ASUS' products have received the Finnish Cybersecurity Labels, while Signify's and Polar's products have received the Singapore Cybersecurity Labels. They are all recognized in both Singapore and Finland.

8. This year, **I am pleased to announce that Singapore will be signing a Mutual Recognition Agreement (MRA) with Germany after this Roundtable, to mutually recognise the cybersecurity labels issued by the Cyber Security Agency of Singapore (CSA) and the Federal Office for Information Security (BSI)**. This mutual recognition will further promote the harmonisation of standards, reduce duplicated testing and costs for manufacturers globally, and improve market access for consumer IoT manufacturers between Germany and Singapore. This MRA will first start with consumer devices, such as smart cameras, smart TVs, health trackers etc, and this list will grow over time as CSA and BSI work through the various product categories.

9. In addition to signing these MRAs with countries with similar schemes, **Singapore has been working with industry and government partners to put up a proposal to develop an international standard**, ISO 27404, which defines a Universal Cybersecurity Labelling Framework (UCLF) for consumer IoT. The UCLF will serve as a guide for countries that are looking to implement and set up their own labelling schemes for consumer IoT. This will facilitate future MRAs across various countries, as existing standards would be harmonised through the UCLF.

10. As mentioned by Senior Minister Teo at his Welcome Remarks for the SICW, **CSA, in collaboration with the Ministry of Health (MOH), Health Sciences Authority (HSA) and Integrated Health Information Systems (IHiS), will be extending the CLS to Medical Devices, or what we will call CLS (MD).** This scheme was developed in consultation with MNC and SME representatives from Asia Pacific Medical Technology Association (APACMed) and the Singapore Manufacturing Federation – Medical Technology Industry Group (SMF – MTIG), and will apply to medical devices that handle sensitive data or are able to connect to other devices, systems, and services. Like the CLS, the new CLS(MD) label will enable consumers and healthcare providers to identify more medical devices with better in-built cybersecurity, and incentivise manufacturers to develop more secure medical devices the same way it has done so for consumer IoT devices. For a start, medical devices meeting HSA's cybersecurity requirements would be deemed compliant to Level 1, while devices with more stringent cybersecurity standards should receive a higher level. An industry consultation will be held to seek feedback on the proposed requirements to obtain the higher levels. More details will be announced in due course.

Conclusion

11. I would say that we are making good strides in IoT security, but we cannot rest on our laurels. The technology landscape is constantly evolving, accelerating perhaps, as digitalisation became

more urgent under the shadow of the COVID-19 pandemic. It is therefore of utmost importance that we continue to work together to identify the risks and threats in our IoT ecosystem, and transform them into opportunities.

12. I am heartened and grateful to have friends and partners from the government and industry who are committed to our joint cause and have given your unwavering support. On this note, I wish you all enriching conversations and discussions at this Roundtable today. Thank you.