19 June 2019

Ms Aileen Chia
Director-General (Telecoms and Post)
Deputy CE (Policy, Regulation & Competition Development)
Infocomm Media Development Authority
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

Via e-mail to: Consultation@imda.gov.sg

RE: Second Consultation on 5G Mobile Services and Networks

Palo Alto Networks appreciates the opportunity to comment on IMDA's "Second Consultation on 5G Mobile Services and Networks." As the global cybersecurity leader, Palo Alto Networks will answer those questions in the consultation related to secure and resilient 5G networks. We commend the consultation's focus on this topic. Specifically, we strongly agree with IMDA that Singapore should undertake a proactive approach to create a secure and robust 5G ecosystem (para 30) and ensure Singapore's 5G networks are designed to be trusted and resilient (para 51). IMDA understands that the telecommunications sector is integral to Singapore's economy, underlying the operations of businesses, public safety organizations, and the government. Singapore citizens rely on telecom networks for the Internet and other communications daily.

With the evolution to 5G, cybersecurity is a key concern globally. Cybercriminals continue to introduce and update new attack tools, using automation, exploit toolkits, and cloud technology to attack mobile operators' infrastructure, communications tunnels, and end-users (consumers and enterprises). Palo Alto Networks believes that the mobile network operators' (MNOs') networks are used to carry attacks launched by cybercriminal, nation/state-sponsored and cyber espionage groups. If Singapore is successful in delivering on IMDA's vision, the attack surface will grow with the connection of billions of new devices. 5G will open new areas of cybersecurity risk that need to be protected, and 5G networks will need to guarantee a high level of security. The threat and potential damage is not only relevant to the telecom sector, but to the many others to which the sector is closely linked, including energy, finance, healthcare, transportation, IT, government, manufacturing, and retail.

We therefore propose that IMDA should adopt a position similar to that proposed by the Next Generation Mobile Networks (NGMN) Alliance:

- Big Data needs to be protected against unauthorized modifications, access, attacks;
- Core requirement for 5G networks - guarantee a high level of security; and

- 5G should be designed to protect users' data and prevent or mitigate any possible cybersecurity attack.

If IMDA adopts such a position, Singapore will be in a better position to deliver trusted and resilient 5G systems and services.

Palo Alto Networks has conducted numerous "proof of concept" (POC) tests in APAC (and around the world), where we have worked with network operators to lawfully deliver capabilities that find and block malware and other cyberattacks within mobile tunnels. The forensic intelligence gathered has provided us with unique insight to the threats currently traversing MNOs' networks in the region, and our comments are based on that insight.

Answers to select consultation questions

Question 1: IMDA would like to seek the industry's views on skills requirements and the potential job demands in the future of networks and next generation of application/use-cases with 5G technology.

Cybersecurity is a key skill that will be required and will drive potential job demand. This includes technical skills. Asia-Pacific, with its growing economies, is experiencing a large shortage in the field of cybersecurity. The lack of skilled cybersecurity personnel is doing more than putting organizations at risk. To keep pace with the latest from the world of cyberthreats, organizations need to be cyber-governance-skills savvy, in areas related to digital threat management, malware analysis, business continuity, disaster recovery planning, cloud security, to name a few. Singapore also needs researchers, engineers, and the like to design and deploy secure networks and the innovative products, services, apps, and experiences that will run on and leverage these networks in a secure way.

However, cybersecurity education and skills development—in 5G as in other domains—should not be limited to IT professionals. Such skills should also be integrated into other technical and professional domains related to the rollout of 5G networks such as town planners, architects, and engineers who may be engaged as part of the design of the 5G network. Finally, there is also a need to raise awareness among senior management. It will be important for corporate directors and board members running Singapore's mobile operators, MNOs, MSSPs, and other organizations with a role in building and running 5G to understand that cybersecurity is a business issue, not simply an IT issue, and to understand the risks inherent in the move to 5G and how they can be mitigated and allocate financial and human resources accordingly.

In cybersecurity skills or job development, it will be essential for IMDA/the government to leverage and build upon the numerous innovative industry initiatives. At a technical level, Palo

Alto Networks already collaborates with five academic institutions in Singapore and we would be pleased to expand this effort to target students planning for jobs related to 5G. At a board level, Palo Alto Networks, in conjunction with Forbes and regional thought leaders from the public and private sector, came together to write a how-to guide and anthology aimed at Singapore's c-suite: *Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers – Singapore.* Launched in 2017, this Guide includes advice and cybersecurity best practices from CEOs, CISOs, lawyers, consultants, and former government officials. We would welcome discussion with IMDA about how to expand these efforts, specifically targeting Singapore's mobile operators.

Question 2: IMDA would like to seek views on:
i) The types of innovative use-cases that could capitalise and further enhance Singapore's competitive advantages, trigger new growth potential and/or strengthen Singapore's existing strategic pillars; and
ii) Areas of government support that the industry require in order to enable innovation and development in 5G.

5G promises transformative mobility by offering enhanced mobile broadband experience and enabling industrial digitalization through customer value creation. With 5G, use cases for life-critical and business-critical services catering to key enterprise verticals will have more definite requirements on connectivity, security and targeted service level agreements (SLAs). Massive IoT, smart utilities and smart cities, in particular, are seen to be among the first transformative industry applications of 5G, according to NGMN Alliance. Securing 5G becomes critical, giving a chance for mobile operators to move up in the value chain from being only connectivity providers to secure business enablers.

Question 6: IMDA would like to seek views, comments and suggestions on:
iii) The network design and resilience challenges of 5G (in particular, enabling technologies, such as SDN, NFV and Cloud Computing that may fundamentally change how the network would be designed and deployed) and possible measures to address them, and whether there are other aspects that should be considered to enable trusted and resilient 5G network;

IMDA's vision (paragraph 30) "is for Singapore to have a thriving Digital Economy, where every business is a digital business, every worker is empowered by tech, and every citizen a connected citizen. World-class connectivity infrastructure will be essential to achieving these objectives." To achieve this vision, it is imperative that IMDA adopt a more forward-leaning position with respect to securing the networks that will connect this new world. To this end, we provide the following suggestions:

- Encourage 5G operators to have visibility of their networks, not simply encrypt their networks. The consultation states that IMDA will "propose certain baseline regulatory requirements for compliance to ensure that 5G networks are trusted and resilient" ***(paragraph 52c).*** In setting these baseline requirements, proper end–to-end encryption (IPSEC) should be expected on critical segments of the network. However, IPSEC is not enough and should not be the only technology encouraged. IMDA should also encourage Singapore's mobile operators to have visibility of their networks and take steps to detect and prevent cybersecurity threats to those networks in real time. Cybersecurity threats (malware, viruses, command-and-control, others) regularly traverse telecom networks. These threats may harm the operator's infrastructure or end-users (consumers or enterprises). To stop these threats, operators need complete visibility of the traffic on their networks, so they can then take steps to prevent attacks in real time. This can complement the use of encryption— while encryption provides security against tampering of data travelling through the network, it does not provide visibility into whether the encrypted traffic passing through the encrypted tunnel is malicious or not.

- Encourage 5G operators to include in their designs references to security technology able to handle high-volume traffic, with automated orchestration and response, allied with an ability to reliably identify and report on specific targeted attacks. 5G will require a dense network of small cell base stations managing high-volume, high-speed traffic across complex network slices. To achieve proper fault management and resiliency, prospective 5G operators should be expected to design into their networks a high reliance on automation, machine learning, and artificial intelligence (AI). Cybersecurity technology and management choices made by operators should reflect this reliance and be fit for purpose to manage risks associated with this approach.

- Encourage 5G operators to adopt a "Zero Trust" approach to security. Zero Trust is an alternative architecture for IT security that aims to help organizations reliably prevent the exfiltration of sensitive data and improve their ability to defend against modern cyberthreats. Conventional security models operate on the outdated assumption that everything on the inside of an organization's network can be trusted, but given increased attack sophistication and insider threats, new security measures need to be taken to stop them from spreading once inside. Because traditional security models design to protect the perimeter, threats that get inside the network are left invisible, uninspected and free to morph and move wherever they choose to successfully extract sensitive, valuable business data. Zero Trust, rooted in the principle of "never trust, always verify," is designed to address lateral threat movement within the network by leveraging micro-segmentation and granular perimeters enforcement, based on user, data and location.

- Add the GSMA to the list of standards bodies and forums to be consulted for security standards and best practices. ***Paragraph 112*** notes that 5G networks must be designed to

be secure and resilient at the outset, "minimally based on best practices and technical specifications from relevant standards bodies and forums, such as 3GPP, IETF, ETSI, and IEEE, and the regulatory requirements imposed by IMDA." Another important industry forum that develops technical security specifications for mobile networks—including 5G— is the GSMA.[1] The GSMA represents mobile operators worldwide, including more than 750 operators with almost 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and Internet companies. The GSMA regularly issues a range of security-related standards and best practices, including those relevant to 5G.

Question 7: IMDA would like to seek views, comments and suggestions on the spectrum assignment framework, including:
iii) The evaluation criteria, sub-criteria and weights to assess the proposals;

Comments on 7iii – evaluation criteria, sub-criteria, and weights:

- We support IMDA's proposed 40% allocation of evaluation weight to network design/resilience when assigning spectrum if certain elements are included (see next paragraph). ***Paragraph 126*** proposes that IMDA will use certain percentages of evaluation criteria when allocating spectrum to applicants. "Table 6: Evaluation Criteria" would provide a 40% weight to "Network Design and Resilience," which is described as "whether the proposed 5G network is designed with trust and security in mind."

  We support this weighting assuming it includes elements of product security related to small cell base stations, design issues related to the management and location of physical elements of the 5G network, and elements of network, cloud, and general cybersecurity principles. The evaluation criteria should include documentation on processes and procedures which incorporate the concept of "secure by design" for developing new services and technology as part of any roadmap submitted by the operator. Given the cybersecurity challenges that 5G will face, planning for, designing, and building 5G networks with security built in from the outset is an imperative. 5G will open new areas of cybersecurity risk that need to be protected, and 5G networks will need to guarantee a high level of security. Government agencies like IMDA have a key role to play in making their expectations clear in this regard. Cybersecurity cannot be an afterthought in 5G networks, or the potential of 5G will not be realized.

- Add GSMA: Under the "Evaluation Criteria" section, ***paragraph 125 (b)*** states that "As mentioned earlier, IMDA's baseline regulatory requirements are… b. Design and build 5G networks based on best practices and technical specifications from relevant standards

[1] https://www.gsma.com/

bodies and forums, such as 3GPP, IETF, ETSI, and IEEE and comply with IMDA's regulatory requirements…" Per our comment above, we suggest the GSMA be added to this illustrative list of standards bodies and forums.

Conclusion and About Palo Alto Networks

As Singapore continues upon its digitalization journey, 5G will play an increasingly critical role in connecting all aspects of a modern Singapore society. Ensuring telecom networks are secure and can be trusted should be a priority of IMDA and the Singapore government generally. Without that trust and security, bad actors – including nation states – will be in a better position to infiltrate 5G networks and gain access to and/control of information and devices connected to them. By focusing on the importance of secure and resilient 5G networks, Singapore can improve its own cyber resilience, and further enhance the country's leadership role in ASEAN and the international community.

For more information

Palo Alto Networks looks forward to supporting Singapore's successful rollout of 5G mobile networks, and we stand ready to provide our expertise and experience to IMDA, the Singapore government, and other stakeholders on how to do so securely. We would be happy to discuss our ideas further.
For more information please contact:
Peter Molloy, Director, APAC Service Providers at pmolloy@paloaltonetworks.com; Kevin O'Leary, Field Chief Security Officer (CSO), APAC at koleary@paloaltonetworks.com; or Danielle Kriz, Senior Director, Global Policy, at dkriz@paloaltonetworks.com.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before.

Palo Alto Networks has a strong and growing presence in Singapore and has demonstrated commitment to the country and the region. Singapore is also home to Palo Alto Networks Asia Pacific Headquarters. In recent years, we have undertaken a range of activities to contribute to

Singapore's cybersecurity posture, including entering into a cybersecurity Memorandum of Collaboration with CSA; gathering actionable insights and advice from key cybersecurity stakeholders in Singapore in our book *Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers – Singapore*; and launching the Republic Polytechnic (RP) - Palo Alto Networks Cyber Security Lab in 2017. Further, five Singapore institutions of higher learning are Palo Alto Networks Authorized Academy Centres (AAC) as part of our Cybersecurity Academy Programme.