Opening address by Acting SITI at Opening Ceremony of Cyber Security Summit 2023 (English only)

Following is the opening address by the Acting Secretary for Innovation, Technology and Industry, Ms Lillian Cheong, at the Opening Ceremony of the Cyber Security Summit 2023 today (September 11):

éf□ä¸»ä»»(Director-General of the Information Centre of the Liaison Office of the Central People's Government in the Hong Kong Special Administrative Region, Dr Hao Yinxing), Mohamed (Executive Director of Hong Kong Productivity Council, Mr Mohamed Butt), æ—¹é™¢å£«(Academician of the Chinese Academy of Engineering, Professor Fang Binxing), Dale (Chairman of the Cyber Security Summit 2023 Organising Committee, Mr Dale Johnstone), Jason (Acting Deputy Government Chief Information Officer, Mr Jason Pun), distinguished guests, ladies and gentlemen,

Good morning. I am delighted to join you all today at this much-anticipated Cyber Security Summit 2023. Firstly, I would like to extend my heartfelt appreciation to the Hong Kong Productivity Council for orchestrating this remarkable summit, which presents us with an invaluable platform where we can meet up with a number of global cyber security experts and benefit from the wealth of experiences and insights from the industry players.

AI (artificial intelligence), is bringing changes to most, if not all aspects of our daily life, and its convergence with quantum computing holds immense promise. It will revolutionise industries, unlock unprecedented opportunities, and reshape our very existence. However, as what Mohamad just introduced, as these technologies are advancing at a rapid pace, we have to face the profound security implications that arise from these groundbreaking developments.

The pace of AI development and its adoption rate differ across regions, and the impact of AI technology on various industries and sectors may vary. That said, different regions and organisations have begun to explore diverse approaches to address the implications and challenges associated with AI, and at the same time, to strike a balance between fostering technological innovation and adhering to relevant regulatory obligations.

In Hong Kong, the Office of the Privacy Commissioner for Personal Data (PCPD) published in 2021 the Guidance on the Ethical Development and Use of Artificial Intelligence (the AI Guidance) to assist organisations in their understanding and compliance with the personal data privacy protection requirements as suggested by the Personal Data (Privacy) Ordinance when developing and utilising AI that involves the use of personal data. The AI Guidance covers a range of crucial aspects including the data stewardship

values and ethical principles that organisations should uphold when dealing with AI. The AI Guidance also aids organisations in formulating appropriate AI strategies and management models that align with ethical considerations.

Besides the PCPD, the Office of the Government Chief Information Officer (OGCIO), as represented by Jason today, has also developed the Ethical Artificial Intelligence Framework. This framework serves as a practical guide for government bureaux and departments when undertaking projects that incorporate AI technologies. Its primary objective is twofold: to offer clear and comprehensive guidance on best practices and to manage potential risks and issues associated with such projects, including privacy, data security, and management concerns.

As technology continues to advance at an unprecedented pace, as what I have just introduced, so do the threats that lurk in the shadows of cyberspace. With quantum computing bringing much more speed, its emergence enhances the ability of attackers to break traditional encryption algorithms that have long been the bedrock of our digital security. "AI takeover" is no longer a hypothetical scenario. It is just a matter of time.

Cyber security is a matter of significant concern for the Government. It is given high priority and is viewed as a critical aspect of governance. We have been closely monitoring the development of post-quantum cryptography, and its impact on cyber security, in particular on the evolution of quantum-resistant encryption algorithms. We will review and revise relevant policies and guidelines suitably, and assess the cyber security risks and countermeasures brought about by this development trend. We strive to ensure that these risks are effectively managed and that our cyber security measures remain resilient in the face of technological progress.

It is not going to be easy, as securing ourselves in this post-quantum and AI world demands our collective attention, collaboration, and innovation. The defence against cyber security threats does call for a holistic approach, not just by the Government, but from all walks of life, and most importantly, to co-operate with our industry players and talent like all of you here, to work together and transcend traditional boundaries, encompassing the realms of technology and human expertise. Let's work together with concerted efforts towards this goal. Lastly, may I wish you all a fruitful and very rewarding summit. Thank you very much.