FOR IMMEDIATE RELEASE

Hong Kong Computer Society Welcomes and Supports The Legislative Council passed the third reading of "Protection of Critical Infrastructures (Computer Systems) Bill"

March 19, 2025. Hong Kong ──The Hong Kong Computer Society (HKCS) has voiced its support and appreciation for the pass of third reading of "Protection of Critical Infrastructures (Computer Systems) Bill" by The Legislative Council today.

Dr. Rocky Cheng, President of HKCS, remarks: "Hong Kong Computer Society, as the largest and longest-established ICT professional organisation in Hong Kong, strongly supports the legislation of "Protection of Critical Infrastructures (Computer Systems) Bill". Given Hong Kong's status as an international financial hub and its critical role as one of the super connectors between China and the rest of the world, this Bill is instrumental. It establishes a cybersecurity baseline for critical infrastructure operating in the city, which is essential for maintaining the security and integrity of our financial systems and other critical services."

Dr. Cheng said: "HKCS greatly appreciates the open and accommodative approach adopted by various Government units, including but not limited to Security Bureau, Data Policy Office, Hong Kong Police Force, Monetary Authority and Communication Authority, throughout the consultation process. The final Bill is a result of consolidating best practices from International markets, including but not limited to China, Macao SAR, Australia, Singapore, Canada, the EU, the US and the UK. Additionally, it incorporates valuable inputs from local industry practitioners, including comments and recommendations provided by various specialist groups such as the HKCS. For example, the time requirement to notify a reportable cyber incident has been extended to not later than 48 hours in consideration of practical constraints such as investigation and impact analysis in the final version of the Bill."

"Furthermore, a number of key industrial practices will be further defined and made available in the Code of Practices, which is to be chartered by the Commissioner Office as the next immediate deliverable. HKCS is looking forward to continuing its active participation in the consultative process for the formation of the Code of Practices for the Bill. We believe that our involvement will help ensure that the Code of Practices is comprehensive, effective, and aligned with the needs of the industry." Stated Dr. Cheng.

About the Hong Kong Computer Society (HKCS)

Founded in 1970, the Hong Kong Computer Society (HKCS) is a recognised non-profit professional organisation focused on developing Hong Kong's Information Technology (IT) profession and industry. Their members come from a broad spectrum of Hong Kong's IT community, from corporations to like-minded individuals, all coming together to raise the profile and standards of the IT profession and industry. As a well-established IT professional body, the Society is committed to professional and industry development as well as community services to ensure the IT sector continues to make a positive impact on peoples' lives with three main goals, namely, 1) talent cultivation and professional development, 2) industry development and collaboration, and 3) the effective use of IT in our community.

For more details, please visit http://www.hkcs.org.hk.

# # #

Issued by: Hong Kong Computer Society
For Media Enquiry, please contact Mr. Davis Man of Man Communications Limited at 852-2862 0042

Appendix: About "Protection of Critical Infrastructures (Computer Systems) Bill"

Appendix: About “Protection of Critical Infrastructures (Computer Systems) Bill”

Purpose of Legislative

"The legislative purpose of the 'Protection of Critical Infrastructures (Computer Systems) Bill' is that critical infrastructures are essential facilities for maintaining the normal functioning of society and the daily lives of citizens. In fact, critical infrastructures worldwide are at risk of malicious cyberattacks, and regulations to safeguard the security of critical infrastructure computer systems are common in other jurisdictions.

In the Policy Address delivered by the Chief Executive in October 2022, it was announced that legislation would be enacted to enhance the cybersecurity of critical infrastructures. The 'Protection of Critical Infrastructures (Computer Systems) Bill' aims to impose statutory requirements on designated operators of critical infrastructures, ensuring they take appropriate measures to protect their computer systems, reduce the likelihood of essential services being disrupted or compromised due to cyberattacks, and maintain the normal functioning of Hong Kong society and the daily lives of its citizens."

Legislative Principles

The regulated "operators of critical infrastructures" are those that are essential for providing necessary services or maintaining key social and economic activities in Hong Kong. Most of these are large organisations, and small and medium-sized enterprises as well as the general public are not subject to regulation.

The purpose of imposing statutory responsibilities is to ensure the security of computer systems that are crucial to the core functions of critical infrastructures. This is not aimed at personal data or business secrets, nor does it relate to citizens' online activities.

Regulated Entities

The "Protection of Critical Infrastructures (Computer Systems) Bill" stipulates that only designated "operators of critical infrastructures" and their designated "critical computer systems" will be subject to regulation. The draft Protection of Critical Infrastructures (Computer Systems) Bill adopts an "organisation-based" approach, where each institution responsible for operating a critical infrastructure is treated as a unit and must fulfill the responsibility of ensuring the security of its computer systems.

Since the government already has relevant policies and guidelines in place to ensure the security of computer systems for essential services operated by the government, it is deemed appropriate to continue using existing methods to regulate government-operated essential services, without including them in the proposed bill.

Statutory Responsibilities

The statutory responsibilities under the "Protection of Critical Infrastructures (Computer Systems) Bill" are categorized into three main types:

1. Structural Responsibilities: These include operators reporting changes in operational rights to the government; establishing a computer system security management department and appointing a dedicated, professionally knowledgeable manager.
2. Preventive Responsibilities: These involve developing and implementing a computer system security management plan, conducting regular risk assessments, audits, and drills.
3. Incident Reporting and Response Responsibilities: When a computer system security incident occurs, operators must report it to the government within a specified timeframe and take their own response measures to restore the system. The government may provide timely assistance when needed, take remedial measures, control the situation, and minimize the impact on other critical infrastructures.

Dedicated Office and Designated Authorities

The government proposes establishing a dedicated office under the Security Bureau to enforce the ordinance:

Since some essential service industries are already fully regulated by their statutory industry regulators, the government suggests designating individual industry institutions as "designated authorities" to oversee compliance with the first category of responsibilities (organizational responsibilities) and the second category of responsibilities (preventive responsibilities) within their regulated sectors.

Currently, the government proposes designating the Hong Kong Monetary Authority to regulate service providers related to banking and financial services, while the Communications Authority will be responsible for regulating service providers related to communications and broadcasting. The dedicated office will oversee incident reporting and response situations for all operators, reducing the likelihood of incidents affecting other sectors or causing widespread service delays.

Offenses and Penalties

Since the legislative intent is not to punish operators, but to balance the impact of regulation on operators of critical infrastructures with ensuring the ordinance has sufficient deterrent effect, the government proposes that penalties will be imposed on organizations only. Offenders may face fines ranging from HK$500,000 to HK$5 million, with additional daily fines for continuous non-compliance. There will be no imprisonment penalties.

Although the ordinance suggests fines for organizations only, if the violating behavior involves committing existing criminal offenses, such as making false statements, using false documents, or other fraud-related offenses, the individuals involved may also face personal criminal liability.

# # #