HKGCC

Hong Kong General Chamber of Commerce
香港總商會1861

香港總商會
香港金鐘道統一中心廿二樓
Hong Kong General Chamber of Commerce
22/F United Centre,
95 Queensway, Hong Kong
Tel (852) 2529 9229
Fax (852) 2527 9843
Email chamber@chamber.org.hk
www.chamber.org.hk

*Helping Business since 1861*

12 August 2024

Mr Tang Ping-keung, GBS, PDSM, JP
Secretary for Security
Security Bureau
10th Floor, East Wing, Central Government Offices
2 Tim Mei Avenue, Tamar
Hong Kong

Dear Chris,

**Re: Security Bureau Consultation on the Proposed Legislative Framework to Enhance Protection of the Computer Systems of Critical Infrastructure**

The Hong Kong General Chamber of Commerce is pleased to put forward our views on the Government's proposals to introduce new legislation to strengthen the security of the critical computer systems of critical infrastructure.

We recognize the importance of safeguarding the cybersecurity of Hong Kong's essential services in maintaining the city's stability and status as a leading international financial centre, and largely support the implementation of statutory requirements to achieve the foregoing goals. Given the business impact of the proposed law, we suggest that consideration be given to the introduction of balanced and proportionate legislation, which is principle and risk-based, technology-neutral and aligned with internationally-recognized standards, so as to promote stakeholder trust and support the city's innovation & technology advancements. Further clarity on the scope and targets of regulation would also be welcomed to provide certainty for local and international enterprises.

We look forward to the opportunity of providing further input on the new legislation as the drafting progresses.

Yours sincerely,

Patrick Yeung
CEO

*Encl.*

# Proposed Legislative Framework to Enhance Protection of the Computer Systems of Critical Infrastructure (July 2024)

## Submission by The Hong Kong General Chamber of Commerce ("HKGCC")

HKGCC welcomes this opportunity to comment on the above proposal, as set out in the paper presented to the Legislative Council (LegCo) Panel on Security on 2 July 2024 ("the Paper"). Given the relatively short consultation period for the proposed legislation, this submission should not be regarded as an exhaustive or final list of our views. Instead, we have highlighted some salient points which we suggest that the Government consider when drafting the proposed legislation. We trust that the Government and LegCo will continue to consult, and consider comments from, Hong Kong businesses as the legislative process progresses, in particular regarding the drafting of the proposed legislation, subsidiary legislation (if any) and the Code of Practice.

Our main points are as follows (referring to the relevant paragraphs in the Paper).

*General*

1. Paras 3-9. In principle, we agree that statutory requirements should be introduced with the aim of protecting the Critical Computer Systems of Critical Infrastructure Operators (both concepts as defined in the Paper), and to establish a Commissioner's Office to oversee the implementation of the new requirements. This is in line with developments in other jurisdictions, as the Paper notes, and it is important that businesses in Hong Kong, and those that may wish to establish operations here, have sufficient comfort that the essential services on which they rely will not be disrupted by a cyberattack.

2. At the same time, we would encourage the Government to work with the industry towards establishing regulation that, while building trust, also helps (not hinders) Hong Kong's digital transformation and IT development, by ensuring that the new requirements are realistic and practicable, and do not impose unduly burdensome or disproportionate compliance costs to business given the current economic climate. We also suggest that the proposed legislation be reviewed regularly to ensure that it keeps pace with advancements in innovation and technology (I&T), as well as new and emerging economies (such as the lower altitude economy).

*Scope and Targets of Regulation*

3. Para 14. We note that the eight sectors whose *infrastructures* are proposed to be covered by the new legislation include information technology. It is particularly important, as regards this sector, to ensure the drafting clearly addresses only organisations that control the critical IT infrastructures and computer systems themselves, and does not inadvertently include IT service providers which use those infrastructures to provide their services or those merely acting as a service provider to other critical infrastructures and computer systems. As such, we suggest clarifying the scope of regulation to give more certainty to the market.

4. Para 17. The Paper lists three factors that will be taken into account by the Commissioner's Office in deciding whether to designate an organisation as a Critical Infrastructure Operator (CIO). It is not clear from this paragraph whether the number of providers of relevant infrastructure in the sector in question - i.e., the degree of reliance by customers on a particular operator or a limited number of operators - will be a relevant factor.

5. Para 18. The Paper states that one of the factors the Commissioner's Office will take into account for the purpose of designating an organisation as a CIO is "the degree of control of an organisation over the CI concerned". It is not entirely clear what this means, and it would be useful to elaborate on the meaning and purpose of this factor.

6. Para 19. The Paper proposes that the legislation only sets out the names of the eight essential services sectors, and does not disclose the list of CIOs, to "prevent the CIs from becoming targets of a cyberattack". While we understand this objective and agree with it, we imagine that the identity of the designated CIOs will become a matter of public knowledge at some point once the designations have been made, and therefore the omission of the names of CIOs from the legislation will not in itself protect them from the risk of cyberattacks.

7. Paras 20-23. The Paper proposes that only computer systems of CIOs that are designated as Critical Computer Systems (CCSs) will be regulated. We believe it is important that the designation of CIOs and CCSs be made in parallel. Computer systems and infrastructures are closely related, and organizations use a variety of computer systems to operate their infrastructures and deliver services. Both CIs and CCSs are critical for the provision of essential or important services, and could have a significant impact on the normal functioning of the relevant businesses and industries if interrupted or damaged. It would not be feasible, and would be inconsistent with the main purpose of the proposed legislation, if an organisation were to be designated as a CIO, before determining whether it owns or operates any CCS.

8. Para 21. We question the proposal that the legislation will extend to CCSs located outside Hong Kong. This appears to be disproportionate, may result in unnecessarily high compliance costs, may have potential conflicts with overseas regimes, and may deter multinationals from setting up operations and investing in Hong Kong, contrary to the Government's vision of developing Hong Kong as an international I&T centre under its I&T Development Blueprint. Even if the proposal was justified, it might be difficult to enforce in any case.

*Obligations of the CIOs*

9. Para 24. As a general point, we recommend that the legislation be principle-based and risk-based, instead of setting out prescriptive requirements. CIOs should be given the flexibility to achieve the desired risk-control objectives and minimise the risks through the methods best-suited to their individual organisations. Otherwise, CIOs could be subject to an excessive regulatory burden, thereby increasing their costs unnecessarily. The legislation should also be technology-neutral and should align with internationally-recognized standards to ensure the development of a

defragmented, consistent and balanced regulatory regime. Furthermore, the Government should provide a reasonable grace period for compliance with the requirements in the legislation after CIO and CCS designation.

10. Para 24 (b). The Paper proposes that CIOs report to the Commissioner any changes in the "ownership and *operatorship*" of their CIs. It is not entirely clear what "operatorship" means for this purpose, and clarification would be welcome. We also suggest the CIO is only required to report significant or material changes that may have an adverse impact on the operation of the relevant CCS.

11. Para 24 (d). As with changes in CIs, we suggest that only material changes in CCSs that may have an adverse impact on the operation of the relevant CCS should need to be reported.

12. Para 24 (g). We question whether an independent computer system security audit is necessary. Such a requirement can be extremely disruptive and costly, and there are other means of achieving the desired objective in a less disruptive and costly way, such as reviewing the CIO's international standard certifications validated by a qualified independent third-party. To reduce the compliance burden on CIOs, we also suggest that the scope of any audit be limited to verification of whether the security requirements under the proposed requirements have been met, and that the frequency of any audit should be determined by the CIO according to the risk-based approach.

13. Para 24 (h) and 36. It should be made clear that the CIO's obligation in respect of third-party service providers is limited to ensuring that its contract with the relevant third party requires the latter to comply with the relevant statutory obligations in respect of the CCS. The CIO cannot guarantee that the third party will comply with its contractual obligations.

14. Para 24 (i). We suggest that CIOs should organise the proposed computer security drill, not the Commissioner's Office as the Paper proposes. Different CIOs and CCSs have their own particular characteristics, and the CIO itself is therefore better-placed than the Commissioner's Office to conduct the drills, which should be more effective taking into account specific nuances relevant to the industry in which the business operates. In addition, some industry sectors such as banking are already conducting similar drills. For the Commissioner's Office also to conduct such drills would result in duplication of efforts, and therefore higher costs and inefficiency. CIOs should also have the flexibility to determine the frequency of such drills based on the risk-based approach, and not be subject to an obligation to conduct them at least once every two years (as the Paper proposes).

15. Para 24 (k). We recommend that a reportable incident should be narrowly-defined and limited to certain significant incidents. Having too low a threshold for reportable security incidents overburdens security teams with reporting duties, distracting them from defending data and systems. It can also reduce the effectiveness of the reporting scheme by flooding the Commissioner's Office with less relevant and low-quality data. As the policy objective is for early warning, any notification requirement should only be triggered if there are significant security incidents with the highest-level impact, such as threats to economic

stability, public health and safety, and national security as a result of a third party's malicious actions. Also, an incident should only be reportable if there is systemic or broad impact to the relevant CCS, but not if it only affects a portion or a few users of the CCS.

16. Para 24 (k). We also recommend that the deadline for notification of any security incident should only be triggered upon *confirmation*, rather than awareness, of an incident. Once aware of a potential issue, CIOs typically identify the cause of the problem, determine the scope of potentially affected customers, and start to mitigate the harm to customers. A deadline that begins on awareness is likely to distract from this time-sensitive and critical work, and may require CIOs to provide incomplete reports just to meet the deadline. Additionally, CIOs understandably want their reports to be accurate, because inaccurate reports risk causing unnecessary concern and reputational harm. Giving CIOs sufficient time to investigate and compile the facts will facilitate higher quality reports, thereby avoiding abortive efforts by the Commissioner's Office due to inaccuracy and missing information in the reports, while also appropriately prioritising customer needs in the immediate aftermath of the incident. We also recommend giving entities at least 72 hours after such confirmation to make the report.

17. Para 25 (a). We recommend that CIOs are given the flexibility to designate their own CCSs and report them to the Commissioner's Office. CIOs are more familiar with their owns CCSs, and have existing frameworks for determining the most critical systems to their operations. This proposed timing would be more in line with data breach reporting obligations around the world, including the European Union's General Data Protection Regulation and Singapore's Personal Data Protection Act.

*Designated Authorities for Individual Sectors*

18. Paras 26-28. We welcome the Paper's acknowledgement of the key existing role of statutory sector regulators in mitigating cybersecurity risks, given their particular sectoral expertise. We note the Paper's proposal that the designated authority for the banking and financial services should be the Hong Kong Monetary Authority. However, it is not clear to us why it is not proposed that *all* banking and financial regulators (including the Insurance Authority, Mandatory Provident Fund Schemes Authority and Securities and Futures Commission) should be designated authorities, given their expertise on cybersecurity issues as they affect their particular sectors. We recommend that they be so designated. In addition, greater clarity needs to be given on the division of responsibilities between the proposed Commissioner's Office and sectoral regulators in terms of policy leadership, enforcement, issuing guidelines etc (on guidelines, see further below).

19. Para 45. Some of these authorities have already issued their own guidelines or codes of practice on cybersecurity. Great care needs to be taken to ensure that the new legislation, subsidiary legislation (if any), and the code of practice which it is proposed that the Commissioner's Office issues, do not conflict with these existing guidelines or codes of practice, to avoid confusion and duplication of effort. The legislation should make it clear which is to prevail if a conflict does arise between them.

20. In relation to the above, consideration could also be given to the establishment of a Steering Group between the Security Bureau and key Category 1 CIOs to establish an overarching code of practice that will apply.

*Investigation Powers of the Commissioner's Office*

21. Para 37-38. We recommend that specific and narrowly-scoped investigation powers be vested in the Commissioner's Office, with conditions and procedures of such power to be clearly set out to facilitate transparency and trust.

HKGCC Secretariat
August 2024