August 1, 2024

Security Bureau [Attn: E Division]
10/F, East Wing
Central Government Offices
2 Tim Mei Avenue
Tamar, Hong Kong

The American Chamber of Commerce in Hong Kong
22/F, Hong Kong Diamond Exchange Building
8-10 Duddell Street, Central
Hong Kong

RE: Proposed legislative framework to enhance protection of the computer systems of critical infrastructure

Dear Sir/Madam,

The American Chamber of Commerce in Hong Kong ("AmCham") acknowledges the HKSAR Government's recent proposal of a legislative framework ("the legislation") to strengthen the security of the computer systems of critical infrastructure thereby enhancing the overall computer system security in Hong Kong. Recent high-profile security incidents have demonstrated the need for the Government to step up and address some widely-shared concerns in the IT industry and also for the interests of the general public. Our members recognize the importance of such a legislation and believe it is a timely one.

As the largest international chamber in Hong Kong with a mission to maintain Hong Kong's stature as an international business center, AmCham appreciates the opportunity to provide comments and suggestions for the Bureau's consideration. In summary, AmCham recommends the following:

- A principle-based and technology-neutral legislation with a robust and risk-based approach to cybersecurity - in consideration of different nature and levels of complexity of each critical infrastructure operator ("CIO") - that align with international standards. The Government should seek to harmonize the requirements with sector-specific requirements and grant reciprocity when a CIO can demonstrate that it meets similar requirements through another regulation or policy.
- Re-evaluating the list of sectors under Category 1 of infrastructures delivering essential services and the factors in determining a CI, considering the objectives of the legislation.
- The legislation should only apply to CIs and critical computer systems ("CCSs") located within Hong Kong. This aligns with the main purpose of the legislation, and is consistent with the practice of similar legislations in other jurisdictions.
- A specific and narrowly-scoped investigation power of the Commissioner's Office, with conditions and procedures of such power to be clearly set out.
- Removing the power to connect equipment to or install program in CCS as this is likely to have a chilling effect on technology investment and Hong Kong digital economy, which will undermine trust in service providers who operate in Hong Kong.

Enclosed is the full list of suggestions for your consideration. We look forward to the opportunity to discuss with you and your office in detail as our members prepare to comply with final regulations. For enquiries, your office may contact Ms. Queenie Tsui, Director of Corporate Affairs at qtsui@amcham.org.hk.

Best regards,

Dr. Eden Woon
President

Encl. AmCham's Comments on the new cybersecurity legislation

AmCham Comments for the Proposed Legislative Framework to Enhance Protection of the Computer Systems of Critical Infrastructure ("Protection of Critical Infrastructure (Computer System) Bill")

1. Determining a CI, CIO and CCS

(a) We recommend to remove "Information Technology" from Category 1 of infrastructures delivering essential services. The nature of "Information Technology" is different from the other seven sectors listed out. In most circumstances, information technology service providers might be providing services to support other CIOs. Information technology service providers also usually just act as vendors of the owners of the relevant computer systems and do not have the necessary control over the computer systems which the Government intends to protect. By using a broad and vague term as "information technology", it may inadvertently capture a large array of technology companies and lose the focus on regulating organizations who control the critical infrastructures and computer systems and should be the one responsible for implementing the cybersecurity requirements under the proposed legislation.

(b) We suggest the proposed legislation clarifies that CIs and CCSs should be identified in parallel in order to determine a CIO. 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 significant impact to the normal functioning of the relevant businesses and industries if interrupted or damaged. It is not feasible and also inconsistent with the main purpose of the proposed legislation if an organization is determined as a CIO before deciding whether it owns or operates any CCS.

(c) In determining whether an infrastructure is a CI under the proposed legislation, while we agree that the three factors listed in the Legislative Council paper should be taken into account, we propose the Government should also consider a number of other factors. For example, the Government should take into account the availability of alternative operators and feasibility for users to migrate from one operator to another. If there are multiple organizations providing substantially the same services or operating similar infrastructures in a particular sector, the severity, intensity, and magnitude of the impact of the disruption of the services or infrastructures would be limited, and therefore the targeted infrastructure should not be regarded as a CI.

2. Extraterritorial effect

(a) We recommend that the proposed legislation should only apply to CIs and CCSs located within Hong Kong. This aligns with the main purpose of the proposed legislation to protect the maintenance of normal functioning of the Hong Kong society and the normal life of the people, and is consistent with the practice of similar legislations in other jurisdictions. By extending the proposed legislation to infrastructures and computer systems situated outside Hong Kong, it is disproportionate to the regulatory purpose, and may result in regulatory fragmentation and lead to higher compliance costs and deter multinational companies from operating businesses and investing in Hong Kong, thereby undermining the vision of developing Hong Kong as an international I&T center under the Government's I&T Development Blueprint.

(b) When the proposed legislation and these other laws applicable to an entity conflict, the entity would be left having to arbitrate between them or decide whose laws to violate, knowing that in doing so they might risk civil penalties or criminal liabilities. We recommend that the proposed legislation should not require an entity to take action or provide assistance in a way that may violate the laws of other countries in which the entity operates, and should include a defence to non-compliance with the proposed legislation on that basis.

3. Obligations on CIO

(a) General:

i. We propose that the proposed legislation should be principle-based and risk-based instead of setting out prescriptive requirements, and should allow for the use of compensating controls and measures that could equivalently or comparably reduce the cybersecurity risk. Overly specific requirements that do not allow for compensating or alternative controls undercut the primary objectives of the CI regime and also expose CIOs to an excessive regulatory burden. The proposed legislation should also be technology-neutral and should not effectively force CIOs to use a particular type of IT services or infrastructure. CIOs should also be permitted to adopt a risk-based approach in determining what specific measures they adopt to protect the CCS and the frequency of conducting relevant preventive measures.

ii. The proposed legislation includes specific timeframe for certain security requirements, such as timeframe for notification of changes, submission of reports. Considering that each CIO and CCS are of different nature and have different level of complexity, requiring all CIOs to follow the same standard timeframe may not be reasonable and practicable. We suggest that the proposed legislation should adopt a more flexible approach without specifying a standard timeframe for such security requirements, and should only require CIOs to comply with such security requirements in a timely manner.

iii. We propose a robust, risk-based approach to cybersecurity that is sufficiently flexible to support resilience and foster continued innovation and technological development, and the requirements under the proposed legislation should align with international standards (such as ISO 27001). Where possible the Government should seek to harmonize the requirements with existing sector-specific requirements and grant reciprocity when a CIO can demonstrate that it meets similar requirements through another regulation or policy. Harmonization and reciprocity support the larger goal of fostering a defragmented, consistent, and balanced regulatory framework as the foundation of a thriving and innovative economy. Ensuring interoperability of cybersecurity standards across the globe could also benefit both local businesses venturing into the international market and international companies investing in Hong Kong with lower legal thresholds. Conversely, disproportionate and burdensome cybersecurity measures and a lack of cybersecurity regulatory harmonization and reciprocity divert resources away from technological and cybersecurity innovation and pose a challenge to both cybersecurity outcomes and to business competitiveness. A flexible and globally interoperable cybersecurity regime is paramount in resisting existing cyber threats and advancing digital resilience for the future.

iv. To avoid duplicative efforts, we recommend an approach to cybersecurity obligations, such as security risk assessment, vulnerability assessment, and penetration test, that integrates reliance on independent certifications, attestations, third-party audit reports (such as SOC reports), and industry standards. Third-party attestations, certifications, and third-party audit reports provide visibility and independent validation of the control environment. When validated by a qualified independent third-party, attestations, certifications, and third-party audit reports help address requirements to perform validation work on CCS and can help ensure the design and operational effectiveness of controls and their underlying objectives.

v. The Government should clarify that CIOs should only be required to disclose generalized operational information to the Commissioner's Office, rather than disclosing specific confidential or protected operational information whenever possible. While we acknowledge that the Commissioner's Office would treat the information received confidentially, we are concerned that the disclosure of operational details and confidential information would create incremental risks to a CIO's security and proprietary information.

vi. We propose that the requirements under the proposed legislation should be compatible and do not conflict with similar requirements in other outsourcing guidelines or vertical-specific regulations.

Duplicative, overlapping and contradictory requirements from regulations that (1) directly apply to CIOs and (2) apply to users/customers of CIOs and flow down to CIOs could result in regulatory fragmentation and cause onerous compliance costs.

vii. We recommend to grant a grace period of 2 years for full compliance with the requirements of the proposed legislation after an entity is designated as a CIO and a computer system is designated as a CCS, considering that the designated entities, especially those operating complex businesses, will need time to take significant actions to implement compliance with the cybersecurity requirements which would have a material or significant impact on their business, operations, or customers.

(b) Organizational:

i. We recommend to provide an exemption for listed companies to report change in ownership, as their shares are open to trade on stock exchanges and so the ownership may change every day.

ii. The Government should clarify what is a change in operatorship for the reporting purpose. It is burdensome for a CIO to track and report any changes in operation, and we therefore suggest only those significant or material changes that may have an adverse impact on the operation of the relevant CIs and CCSs would need to be reported. Also, reporting three months in advance is impracticable and unnecessary, and we propose the reporting for operatorship change should also be made within 30 days after the date of change.

(c) Preventive:

i. It could be burdensome for and increase the compliance cost of CIO to report any material change of CCS to the Commissioner's Office, no matter what is the impact of such change. We suggest that CIO is only required to report significant or material changes that may have an adverse impact on the operation of the relevant CCS.

ii. Independent computer system security audit: We suggest regulators to use other means and have more flexibility in conducting audit, such as reviewing international standard certifications (e.g., ISO certifications) and third-party audit reports (e.g., SOC reports), to fulfil the audit requirement in order to avoid business disruption and affect the overall security of the CCS and the workload of CIOs. For the same reasons and to reduce the compliance cost of the CIOs, the scope of any audit should also be limited to verification of whether the security requirements under the proposed legislation have been met and the frequency of any audit should be determined by the CIO based on the risk-based approach.

(d) Incident reporting and response:

i. For the drill requirement, given that different CIO and CCS are unique and have different nature, CIO, rather than the Commissioner's Office, should be the most appropriate party to organize drills for its own CCS and to determine the way to conduct the drills. Also, some of the industry sectors (such as banking) are already conducting similar drills, and so having the CIO to organize the drills could avoid duplication of efforts. CIOs should also have flexibility in determining the frequency of the drill based on the risk-based approach.

ii. Cybersecurity incident reporting requirements should be careful to not duplicate or conflict with privacy or data protection laws.

iii. 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.

iv. We recommend that the deadline for notification of any security incident should only be triggered on confirmation rather than awareness of an incident. We also recommend giving entities at least 72 hours after such confirmation to make the report. Once aware of a potential issue, CIOs typically identify the cause of the problem, recreate it, 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 prioritizing customer needs in the immediate aftermath of the incident.

v. The incident reporting obligation should also be limited to the entity with the responsibility for monitoring and securing the environment. This distinction is necessary especially for the scenario when an entity lacks the visibility into the choices made by its customers and is not in a position to detect and respond to security incidents in the customer's area of responsibility.

4. Engagement with third-party service providers

(a) We agree with the position in the Legislative Council paper that CIOs, having ultimate control over the relevant CIs and CCSs, should bear the responsibility in complying with the cybersecurity requirements under the proposed legislation. We agree that CIOs could put in place appropriate contractual terms with third-party service providers to have third-party service providers assist the CIOs in complying with the relevant requirements under the proposed legislation.

(b) We recommend that the proposed legislation should provide an exemption to allow CIOs to disclose their CIOs and CCSs designation status to their third-party service providers on a need-to-know basis, so as to facilitate the negotiation of appropriate contractual terms between CIOs and their third-party service providers when needed.

5. Investigation power

(a) General:

i. We recommend that the exercise of the investigation powers of the Commissioner's Office should be kept to the minimum extent necessary, and also be approportionate, practicable and feasible. The investigation powers should be specifically and narrowly scoped, and the conditions and procedures of each such power should be clearly set out. The exercise of the investigation powers should require prior judicial authorization or be appealable and subject to merits review by an independent party.

ii. The Government should provide assurance that information provided for investigation will be used only for specific use cases (e.g., for investigating a particular incident) and will not be used for other cases and disclosed to third parties.

(b) We suggest the Government to clarify that the investigation powers should be exercised against the CIOs as they are the ones regulated by the proposed legislation and have control over the CIs and CCSs, and only in limited scenarios where there is a definite necessity, the Commissioner's Office may request assistance from relevant non-CIOs. Such investigations should not impose undue economic or technical burdens on the non-CIOs, and the non-CIOs should have the right to reject providing the assistance if doing so is not technically feasible, or would conflict with the laws of its home jurisdiction or violate the contractual commitments made to their customers.

(c) Regarding the power to investigate security incidents, the Commissioner's Office would have the power to direct the CIO, or, with warrant, other person in control of the CCS, to take remedial actions, take action to assist in the investigation, and answer questions and furnish documents. On its face, the CIO or the person in control of the CCS could literally be required to do anything, that may result in situations where the CIO or the person in control of the CCS is instructed to take direct action to alter the existing technology or services, or implement new technology or services that may have a catastrophic impact on its existing assets or services. We recommend that the Government to clarify with an exhaustive list of actions that the CIO or the person in control of the CCS may be directed to do, so that the scope of the new powers is clear and affirmed by the Legislative Council.

(d) We also recommend removing the power to connect equipment to or install program in CCS by the Commissioner's Office. Such unprecedented power directly intervenes in, and could have a significant impact on, a CIO's operation and could harm the users of the services provided by the CIO. Moreover, as such power might be exercised within a third-party service provider's environment, it could further interfere with the operations of the third party, create potential vulnerabilities and weaknesses, and cause the third party to breach its contractual arrangements with its customers or to violate any applicable laws. Given the complexity and uniqueness of each CCS, it is unclear how the Government could ensure that such power could be exercised quickly, operate effectively, and achieve the Government's aim, without causing greater harm. We submit that introducing this power is likely to have a chilling effect on technology investment and Hong Kong digital economy and will undermine trust in service providers who operate in Hong Kong. If the Government insists to have such power, we recommend that sufficient guardrails should be put in place to ensure that such power would be exercised appropriately and proportionately. For example, (1) this power should only be exercised as a last resort to mitigate the harms caused by the security incident if the CIO is unwilling or unable to comply with the direction of the Commissioner's Office or to take direct action, (2) any action to be taken by the Commissioner's Office regarding this power should be consulted with the CIO and the relevant third-party service provider in advance, (3) conducting a balancing test to evaluate whether the benefits of exercising such power outweighs the potential harms that would be caused, and (4) the Commissioner's Office should not exercise such power if it is technically unfeasible or unpracticable to do so.

6. Consultation on proposed legislation, subsidiary legislation, and CoP

(a) Given that the proposed legislation would have extensive impact on different stakeholders and the subsidiary legislation and CoP would contain detailed cybersecurity requirements that may affect not only CIOs but also their third-party service providers, we suggest that the Government should conduct public consultation on the proposed legislation, the subsidiary legislation and CoP so that the broader public view could be considered.