香港特別行政區政府
保安局

香港添馬添美道 2 號

The Government of the
Hong Kong Special Administrative Region
Security Bureau

2 Tim Mei Avenue, Tamar, Hong Kong

本函檔號 Our Ref.: SBCR 1/3231/2022 Pt. 5
來函檔號 Your Ref.:

電話號碼 TEL. NO. : 2810 2632
傳真號碼 FAX. NO. : 2810 7702

Miss Joyce CHAN
Senior Assistant Legal Adviser
Legal Service Division
Legislative Council Secretariat
Legislative Council Complex
1 Legislative Council Road, Central, Hong Kong

Miss CHAN,

Protection of Critical Infrastructures (Computer Systems) Bill

Thank you for your letter dated 6 January 2025. After consulting the relevant departments, our reply is as follows:

Part 1: Interpretation

The meaning of "adverse effect" for the purposes of "computer-system security incidents" and "computer-system security threats" (paragraph 2 of your letter)

2. The definitions of "computer-system security incident" and "computer-system security threat" are set out in clause 2 of the Protection of Critical Infrastructures (Computer Systems) Bill (the Bill), both of which includes reference to one element, i.e. an event or act that has or is likely to have an "adverse effect" on the computer-system security of the "critical computer system (CCS). "Computer-system security" is also defined in clause 2. In brief, the term refers to the **ability** of a "CCS" **to resist** when encountering events and acts that will compromise the

availability, integrity and confidentiality of system information or services, and **the state** in which the system is **protected from compromises**. In line with the definition of "computer-system security", the "adverse effect" on "computer-system security" can generally be understood as the compromising or undermining of the availability, integrity and confidentiality of the information or services of a CCS or its protection ability. As such, the proposed definitions and the scope of coverage of "adverse effect" for the purposes of "computer-system security incidents" and "computer-system security threats" are sufficiently clear and there is no need for an express provision. Further defining "adverse effect" in the legislation may unduly restrict its coverage. We also noted that in the Network and Information Systems Regulations 2018 of the United Kingdom and the Cybersecurity Act 2018 of Singapore, "incident" is defined by adopting the concept of "adverse effect" and its meaning is not further provided for. The codes of practice (CoPs) will provide guidelines and examples for the meaning of "computer-system security incidents" and "computer-system security threats".

Part 4: Proposed obligations of critical infrastructure (CI) operators

Obligation to notify operator changes (paragraph 3 of your letter)

3. The main purpose of requiring CI operators to report changes in operators of critical infrastructures (CIs) is to enable the Commissioner's Office to keep abreast of the list of organisations responsible for discharging the statutory obligations of CIs and to change the designation of CI operators when necessary, so as to ensure good communication between CI operators and the regulating authorities and facilitate the smooth implementation of the regulatory regime. Under clause 20(4) of the Bill, "operator change" refers to a change of the organisation that operates a CI. Examples include the sale of operatorship of facilities by the existing operator to another operator, termination of the operating contract of the existing operator, and the cessation of the existing operator or the transfer of operatorship of facilities to another operator due to the merger or acquisition of the operator. Changes in ownership of the operator (e.g. routine stock transfers of a listed company) and staff movements within the organisation (e.g. replacement of company directors) do not affect the continuation of operation of the CI operator itself and hence do not require notification to the regulating authority.

Requirements on the head of the computer-system security management unit (paragraph 4 of your letter)

4. Clause 21(4) of the Bill requires that the person appointed by a CI operator to supervise the computer-system security management unit (unit head) must be an employee of the CI operator who has adequate professional knowledge on computer-system security. According to clause 21(2) of the Bill, a CI operator may set up the computer-system security management unit by itself or engage a service provider to do so. In fact, it comes to our knowledge that many operators have outsourced the management unit to cybersecurity companies. The professional knowledge required of a unit head varies depending on whether the computer-system security unit is an in-house or outsourced one. Moreover, given the rapid development in technology, the academic qualifications, certifications and areas of expertise expected of professionals in the field of computer-system have been updated from time to time to keep pace with technological advancement. As such, we intend not to impose rigid qualification requirements in the Bill so as to provide CI operators with greater flexibility in recruiting suitable candidates. We will incorporate recommended qualifications and professional requirements (e.g. internationally recognised professional qualifications and certifications) on the unit heads into the CoPs. This will serve as a reference for CI operators to ensure that their unit heads meet the requirement of having adequate professional knowledge.

Obligation to make notifications on material changes in certain computer systems (paragraph 5 of your letter)

5. Clause 22 of the Bill stipulates that a CI operator must notify the regulating authority of changes in certain computer systems. Changes that require notification include (clause 22(2)) material changes to the design, configuration, security or operation of a CCS; removal of a CCS; addition of a new system that may be designated as CCS; and changes that may lead to an existing system being designated as CCS. In response to the questions raised in paragraph 5 of your letter, our reply is provided seriatim as follows:

(a) The design, configuration, security or operation of a CCS should be interpreted literally. Depending on the circumstances, examples of material changes include application re-design (involving design), platform migration (involving configuration and operation), server virtualisation (involving configuration and operation) and integration or change in interdependency with

external systems or other computer systems (involving security, configuration and operation);

(b) The purpose of requiring a CI operator to notify the regulating authority of changes in a CCS is to enable the regulating authority to keep abreast of the changes that may affect the computer-system security of a CI, to add or change the designation of a CCS when necessary, and to assess, prepare for or respond to potential computer-system security threats or incidents. The events requiring notification covered in clause 22 are sufficient to achieve this purpose;

(c) Whether a change is "material" may vary subject to time, technology and societal development. Therefore, regulating authorities will provide more interpretation notes and guidelines on "material change" by means of CoPs;

(d) Clauses 22(3)(a) and (b) are not adequately wide to cover all events that require notification. We need to keep pace with the times and maintain flexibility. Therefore, it is necessary to stipulate that the meaning of "material change" is given "without limiting the meaning of "material".

<u>The party bearing the costs of computer-system security audit (paragraph 6 of your letter)</u>

6. The costs of the audit to be carried out in accordance with clause 25 of the Bill will be borne by the CI operator. The costs arisen from the regulated party's compliance with statutory requirements to be borne by the party regulated by the legislation or the user is a matter of course and a common practice without the need for express provision in the legislation. Likewise, section 78 of the Road Traffic Ordinance (Cap. 374) empowers the Commissioner for Transport to require that a vehicle be produced for examination, without specifying by which party the examination fee is payable. Such fee is in fact to be borne by the vehicle owner, which is also a matter of course without the need for express provision in the legislation.

<u>The definition of "independent auditor" in respect of computer-system security audit (paragraph 7 of your letter)</u>

7. Clause 25(8) of the Bill requires that a computer-system security audit be carried out by an independent auditor. The purpose of this requirement is to ensure that the audit is impartial and objective.

"Independent" should be given a literal interpretation. According to the Oxford Dictionary, the word "independent" carries the meaning of "not subordinate or subject to someone or something else". In the CoPs, we will provide CI operators with more detailed guidelines on the recommended qualifications, professional requirements as well as requirements in relation to "independence" (including absence of conflict of interest) of the auditor.

The threshold for proving that a CI operator has become aware of a computer-system security incident (paragraph 8 of your letter)

8. Clause 28 of the Bill requires that the CI operator must, after becoming aware of a computer-system security incident, notify the Commissioner of such incident as soon as practicable and in any event within the specified time. "Becoming aware" involves subjective knowledge, while whether or not the CI operator is aware of the occurrence of a computer-system security incident is a factual issue that should be considered on a case-by-case basis, so there is no need for express provisions. The CoPs will set out guidelines and examples regarding the definition of "computer-system security incident" and the scenarios requiring notification to the Commissioner. In general, a preliminary investigation in order to establish whether or not a computer-system security incident has occurred will not be regarded as "becoming aware" of the occurrence of an incident.

Whether consideration will be given to providing "reasonable excuse" defence for the offence of failing to comply with written directions or categories 1 to 3 obligations (paragraph 9 of your letter)

9. Clause 65 of the Bill provides that a CI operator may raise the "due diligence" defence for the offence of failing to comply with categories 1 to 3 obligations and written directions of the regulating authority, i.e. the commission of the offence was due to a cause beyond the CI operator's control, and that the CI operator has taken all reasonable precautions and exercised all due diligence to avoid the commission of the offence.

10. The object of the Bill is to protect the security of the computer systems of Hong Kong's CIs by clearly delineating the obligations for CI operators. Considering the significant roles played by CI operators in protecting computer-system security and the utmost importance of this issue, it is reasonable and necessary to set a higher threshold for requiring CI operators to exercise all diligence to meet the statutory requirements. To include a "reasonable excuse" defence with a relatively low threshold

for the offence of failing to comply with categories 1 to 3 obligations and written directions of the regulating authority will be inappropriate, as this will run contrary to the legislative intent of the Bill to impose requirements on CI operators to protect the security of their computer systems.

11. As regards other offences under the Bill, including those provided for under clause 18 (failure to comply with the regulating authorities' requirements to provide information for the purpose of making designations), clause 42 (failure to comply with requirements made by the Commissioner for the purpose of investigating computer-system security incidents or threats) and clause 45 (failure to comply with requirements made by the Commissioner for the purpose of investigating offences under the Ordinance), the targets are not limited to CI operators. Since other organisations may also be subject to the relevant requests, it is reasonable to allow the relevant organisations to provide "reasonable excuse" as a defence.

12. Regarding the requirement to participate in computer-system security drills as mentioned in paragraph 9 of your letter, clause 26(2) of the Bill provides that the Commissioner must give reasonable notice in writing before conducting computer-system security drills. In actual operation, the Commissioner will also maintain close communication with CI operators to balance the need for drills and the impact on CI operators. Simulated cyber incident scenarios will be designed having regard to the characteristics of the sector and the operating organisations. Allowing CI operators to use "reasonable excuse" as a defence will in effect allow them more room for not participating in drills, which runs contrary to the legislative intent.

<u>Elements of the proposed offences under the Bill (paragraph 10 of your letter)</u>

13. In criminal law, "strict liability offences" refer to offences in which criminal liability is imposed upon proof of the proscribed act or circumstances. It is not necessary for the prosecution to prove the existence of *mens rea*. "Strict liability offences" are common in regulatory legislation. In response to the questions raised in paragraph 10 of your letter, our reply is provided seriatim as follows:

(a) The offences stipulated in clause 7 and Part 4 of the Bill are "strict liability offences", i.e. a CI operator commits an offence if it fails to comply with the requirements stipulated by the legislation. It is not necessary for the prosecution to prove the existence of *mens*

rea. In addition, the offences stipulated in clauses 18 (failure to comply with the regulating authorities' requirements to provide information for the purpose of making designations), clause 42 (failure to comply with requirements made by the Commissioner for the purpose of investigating computer-system security incidents or threats) and clause 45 (failure to comply with requirements made by the Commissioner for the purpose of investigating offences under the Ordinance) are also "strict liability offences". If a written notice or requirement has been duly served, the organisation commits an offence if it fails to comply with the notice or requirement concerned. Offences under clause 58 of the Bill, which are related to the breach of the clauses on the preservation of secrecy, are not strict liability offences. It is necessary for the prosecution to prove the existence of *mens rea*.

(b) "Due diligence" and "reasonable excuse" (whichever applicable) have been provided in the Bill as statutory defences. In respect of the offences stipulated in clause 7 and Part 4 of the Bill, CI operators may raise the defence of "due diligence", for which the defendants only have to bear the "evidential burden", i.e. sufficient evidence is adduced to raise an issue regarding the aforementioned circumstances, while the contrary is not proved by the prosecution beyond reasonable doubt (clause 65). The prosecution always has to bear the burden of proof in respect of the charge. As for the offences stipulated in clauses 18, 42 and 45 of the Bill, relevant organisations may raise a defence of "reasonable excuse" and, similarly, they only have to bear the "evidential burden" (clause 66);

(c) The Bill seeks to protect the security of the computer systems of CIs, thereby maintaining the normal functioning of Hong Kong society and the normal life of the people. Having regard to the great importance of this legislative intent and the regulatory nature of the above offences, as well as the fact that the penalties concerned are limited to fines only, we are of the view that if we allow organisations to rely on the defence of "honest and reasonable belief" under the common law in respect of the above offences, it will not be in line with the policy objective of strictly requiring CI operators to fulfil their statutory obligations. Applying the principles laid down by the Court of Final Appeal in respect of offences of "strict liability" as in the cases of *Kulemesin v HKSAR* (2013) 16 HKCFAR 195 and *Hin Lin Yee v HKSAR* (2010) 13 HKCFAR 142, the statutory defence of "due diligence"

or "reasonable excuse" (whichever is applicable) under the Bill has already precluded the defence of "honest and reasonable belief" under the common law. The relevant provisions do not violate the principle of presumption of innocence. They also satisfy the four-step proportionality test[1] laid down by the court in *Hysan Development Co Ltd v Town Planning Board* (2016) 19 HKCFAR 372 (*the Hysan case*), fully meeting the relevant requirements of the Basic Law (BL) and the Hong Kong Bill of Rights (HKBOR).

Parts 5 and 6: Enforcement related matters

Whether designating overseas systems means the Bill has extraterritorial effect (paragraph 11 of your letter)

14. The Bill does not have extraterritorial effect in its enforcement. Regulating authorities cannot enforce the provisions outside Hong Kong. Under today's technology, information networks have become borderless. In fact, organisations located in Hong Kong often use servers located outside Hong Kong to store data or support the core function of a CI. In response to the questions raised in paragraph 11 of your letter, our reply is provided seriatim as follows:

(a) A regulating authority may designate a computer system that is essential to the core function of a CI and accessible by the CI operator in or from Hong Kong as a CCS (clause 13 of the Bill). The purpose is to ensure that the CI operator fulfil the statutory obligations under the Bill to protect the security of its computer systems. In other words, systems controlled by overseas cloud providers may also be designated as CSSs if they meet the above criteria;

(b) Moreover, the CI operator is required to produce information in accordance with other relevant provisions (including clauses 30, 35 and 37, which are related to computer-system security investigation), but such information must be accessible in or from Hong Kong. Hence, while the relevant information may be

[1] The four steps of the proportionality test are as follows:
(a) the restriction must pursue a legitimate aim;
(b) the restriction must be rationally connected to that legitimate aim;
(c) the restriction or limitation must, depending on the rights engaged: (i) be no more than is necessary to accomplish that legitimate aim; or (ii) not be manifestly without reasonable foundation; and
(d) a reasonable balance has to be struck between the societal benefits of the encroachment and the inroads made into the constitutionally guaranteed rights of the individual, asking in particular whether pursuit of the societal interest resulted in an unacceptably harsh burden on the individual.

located outside Hong Kong, it is the CI operator in Hong Kong which is subject to the regulation of and the obligations imposed by the Bill. This fully aligns with the "territorial principle" and does not involve extraterritorial effect. As for clause 37, which relates to acts imposed on organisations other than CI operators, authorised officers of the Commissioner will apply for a magistrate's warrant while taking into account the actual circumstances where the CCS can be accessed in or from Hong Kong. The powers conferred by the magistrate's warrant cannot be exercised outside Hong Kong;

(c) In practical terms, the officers will not directly exercise the above powers vis-a-vis overseas cloud providers.

Requirement to obtain a magistrate's warrant for the Commissioner to exercise investigation powers (paragraphs 12-13 of your letter)

15. Part 5 of the Bill sets out the Commissioner's powers when responding to and investigating computer-system security threats and computer-system security incidents. The provisions stipulate in detail the conditions for exercising the powers, among which the purpose of making enquiries and investigation must be fulfilled. Depending on the nature of the investigation powers, the restrictions to be imposed and the applicable procedures may vary.

16. Regarding the question in paragraph 12 of your letter, in general, the preliminary powers of investigation on a threat or an incident are confined to requiring the CI operator to produce information and answer questions (clauses 30(1) and 35(1)). The degree of intrusiveness is relatively low. The exercise of such investigation powers without authorisation from a magistrate's warrant is in line with the exercise of similar powers under other legislation in Hong Kong, such as section 25 of the Accounting and Financial Reporting Council Ordinance (Cap. 588), section 112 of the Private Healthcare Facilities Ordinance (Cap. 633) and section 73 of the Travel Industry Ordinance (Cap. 634). In respect of such investigation powers, reference is also drawn from relevant provisions in the Australia's Security of Critical Infrastructure Act 2018. As for organisations other than CI operators, which are not the Bill's main target of regulation, we propose establishing a more stringent threshold. In responding to and investigating computer-system security threats and incidents, the Commissioner must obtain authorisation from a magistrate's warrant before requiring organisations other than CI operators to produce information, answer questions or do other designated acts (clause 37(2)).

17. Regarding the question raised in paragraph 13 of your letter, to ensure that the powers exercised are proportional and rational, a list of conditions must be satisfied before the Commissioner can exercise such powers (clause 36(1)) and further require the investigated CI operator to do specified acts (for instance, taking remedial measures or giving assistance) (clause 36(2)). That said, considering that the main targets of regulation of the Bill, i.e. designated CI operators have the obligation to protect the security of their CCSs, it is reasonable to require them to do specify acts without needing to obtain authorisation from a magistrate's warrant. On the other hand, for organisations other than CI operators, which are not the main targets of regulation of the Bill, the exercise of powers upon them will be subject to conditions that are more stringent than those for the CI operators. A magistrate's warrant must be obtained.

18. It should be noted that unlike Part 5, which provides for the powers to investigate incidents, Part 6 of the Bill sets out a regulating authority's powers to investigate offences under the Bill. With conditions stipulated in clause 43 being met, a regulating authority may require an organisation (whether a CI operator or not) to provide information and answer questions. In clause 44, however, a mechanism is put in place to prevent the answers provided by the investigated organisation from being unduly used as incriminating evidence against the organisation in criminal proceedings. The right to fair trial, which is guaranteed under the BL and the HKBOR, is thereby effectively safeguarded. Examples of similar powers and protection in other legislation can be found in sections 183 and 187 in the Securities and Futures Ordinance (Cap 571).

<u>Whether the right to enter premises is consistent with the BL (paragraph 14 of your letter)</u>

19. In the case *Keen Lloyd Holdings Limited v Commissioner of Customs and Excise* [2016] 2 HKLRD 1372, the Court of Appeal laid down the principle of proportionality test, which is applicable to the protection of privacy right under Article 29 of the BL and Article 14 of the HKBOR. Among others, the Court of Appeal held that although in general, the prior vetting of a search warrant for any premises by a judicial officer may provide an important safeguard, an obvious case for exception is a situation where it would not be reasonably practicable to obtain a warrant.

20. Hence, clause 40 of the Bill stipulates that in emergencies, the Commissioner may, for the purpose of any computer-system security investigation, enter any premises without a magistrate's warrant and do

one or more of the acts specified in clause 38(2) (including a list of remedial measures). This is consistent with the above legal principle. Such power is subject to strict requirements and must not be exercised unless the following conditions are met:

(a) the Commissioner has reasonable grounds to suspect that there is on the premises any documents or computer systems relevant to the investigation;

(b) there are reasonable grounds for believing that the CI operator concerned or the organisation in control of the system is unwilling or unable to take all reasonable steps to assist in the investigation or respond to the computer-system security threat or incident;

(c) it is not reasonably practicable to obtain a warrant in the circumstances of the case; and

(d) it is in the public interest to enter the premises and do the acts (having regard to the potential harm and disruption that could be caused by the investigated threat or incident to the CI concerned and its core functions; whether or not the investigation purposes could be effectively achieved if the entry is not made and the acts are not done; the benefits likely to accrue from making the entry; and the potential impact of making the entry and doing the acts on the core function of the CI and any person who may be affected).

21. The power to enter in emergencies is strictly subject to the above conditions. It satisfies the four-step proportionality test laid down by the court in *the Hysan case* and fully meets the relevant requirements of the BL and the HKBOR.

Circumstances warranting the use of force to enter premises (paragraph 15 of your letter)

22. Clauses 31, 38 and 46 of the Bill, which provide for entering premises with a magistrate's warrant, stipulate that a magistrate may issue a warrant authorising an authorised officer of the Commissioner, and any other person whose assistance is necessary for the execution of the warrant, to enter premises by force when necessary. Such stipulation is common in other legislation in Hong Kong where entry into premises with a magistrate's warrant is provided for. Examples are the Unsolicited Electronic Messages Ordinance (Cap. 593) and the Payment Systems and Stored Value Facilities Ordinance (Cap. 584). In response to the questions raised in paragraph 15 of your letter, our reply is

provided seriatim as follows:

(a) To give an example, investigation officers may hold a warrant authorising them to enter certain premises, but the main entrance is locked and the person-in-charge cannot be found to unlock the door, or even the entry is obstructed by on-site staff. In such case, entry by force may be necessary;

(b) Investigation officers will only exercise such power when necessary and, depending on the actual circumstances, use such force as may be reasonably necessary to enter the premises. Therefore, the provisions fully satisfy the requirements of the BL and the HKBOR, including the proportionality test; and

(c) When necessary, the regulating authority will provide clear enforcement guidelines to the investigation officers.

Whether "electronic device" needs to be defined (paragraph 16 of your letter)

23. Clause 46 of the Bill empowers a magistrate to issue a warrant authorising an authorised officer of the regulating authority to access and inspect an electronic device; and to search for, inspect, make copies of and take extracts from any information that is stored in the electronic device. "Electronic device" should be interpreted literally. Further defining the term may unduly restrict its coverage and will likely render it inadequate as technology evolves. Similarly, in the Personal Data (Privacy) Ordinance (Cap. 486), which confers powers of accessing an electronic device, the term "electronic device" is not defined either.

Information and evidence to be considered by the Commissioner in deciding whether to exercise certain powers and whether the CI operator concerned or independent consultant(s)'s assistance is needed (paragraph 17 of your letter)

24. According to clause 36 of the Bill, if there are reasonable grounds for the Commissioner to believe that the investigated CI operator is unwilling or unable to take all reasonable steps to assist in the investigation or respond to the investigated threat or incident, and there are reasonable grounds to believe that it is in the public interest to make further authorisation, the Commissioner may further authorise an authorised officer of the Commissioner to exercise the powers specified in clause 36(2), which include "not to use the investigated system", to

investigate a threat or an incident. In deciding whether to make further authorisation, the Commissioner must take into account all relevant factors to consider whether the conditions specified in clause 36, including the potential impacts of exercising the power on the core function of the CI and the CI operator, are satisfied, so as to strike a balance between investigation needs and impacts on the CI operator. The required information and evidence differ depending on the actual circumstances of each threat or incident. In general, when investigating a threat or an incident, the Commissioner and his authorised officer will maintain close communication with the CI operator. Nevertheless, this is not made mandatory under the Bill, lest the capabilities of the Commissioner's office in promptly responding to a computer-system security threat or incident be undermined. The Government will ensure that the Commissioner's office has sufficient personnel with professional knowledge in relation to computer-system security, and may consult experts when necessary.

Factors to be taken into account by a magistrate in considering whether to allow exercise of certain powers (paragraph 18 of your letter)

25. Clause 39 of the Bill sets out the conditions for issuing a warrant. In order to obtain a magistrate's warrant, the Commissioner's authorised officer, in making the application, is required to satisfy the magistrate that the CI operator/the organisation concerned is unwilling or unable to take all reasonable steps to assist in the investigation or respond to the investigated threat or incident, and there are reasonable grounds to believe that it is in the public interest to issue the warrant. The considerations on public interest are set out in clause 39(b) as follows:

(a) the potential harm that could be caused by the investigated threat or incident to the CI concerned;

(b) the potential disruption that could be caused by the threat or incident to the core function of the infrastructure;

(c) whether or not the purposes of investigation could be effectively achieved if the warrant is not issued;

(d) the benefits likely to accrue from doing the acts to be authorised by the warrant; and

(e) the potential impact of doing the acts on the core function of the infrastructure and on any person who may be affected by the acts.

26. In the above considerations, proportionality, which includes a

balance between investigation needs and the impacts on the CI operator or third party, has been taken into account. The Commissioner and his authorised officers will help the magistrate make the decision by providing the magistrate with all relevant information. The required information and evidence differ depending on the actual circumstances of each threat or incident.

Part 7: Appeal matters

Rationale for not allowing all decisions to be appealable (paragraph 19 of your letter)

27. According to clause 48 of the Bill, any organisation may lodge an appeal against the following decisions made by a regulating authority in relation to the organisation:

(a) written directions (clause 7);

(b) designation of CI operators and CCS (clauses 12 and 13);

(c) requirement for CI operators to conduct additional computer-system security risk assessments and submit assessment reports (clause 24(5));

(d) requirement for CI operators to carry out additional computer-system security audits and submit audit reports (clauses 25(4) or (6)).

28. In specifying appealable decisions, the Bureau has given due consideration to the nature of each type of decision and the impact of allowing appeals on the effective implementation of the Bill. Considerations for not allowing CI operators to appeal against other decisions are as follows:

(a) Granting of time extension for submitting information or reports involves requirement on timeliness. It is not advisable to allow CI operators to lodge appeals against such decisions, otherwise the discharge of these statutory obligations would be prone to substantial delay;

(b) Exemption of CI operators from complying with certain obligations arises from the CI operators' statutory obligations under the Bill. Whether to allow exemption or not is at the Commissioner's discretion and involves policy considerations. The Commissioner is also in a better position than the appeal board in assessing

whether the exemption is in the public interest;

(c) As for requirements for computer-system security drills, clause 26(2) of the Bill provides that the Commissioner must give reasonable notice in writing before conducting computer-system security drills. In actual operation, the Commissioner will also maintain close communication with CI operators. Simulated cyber incident scenarios will be designed having regard to the characteristics of the sector and the operating organisations. Allowing appeals will likely lead to delays in drills, thus affecting the timely assessment and improvement of computer-system security and emergency response capabilities.

29. As for decisions not specified under the Bill to be handled by the appeal board, CI operators or other affected parties aggrieved by the decisions may apply for judicial review subject to the satisfaction of the general principles and conditions of judicial review.

Whether to set out in the Bill factors to be considered by the appeal board in granting a stay of execution of a decision under appeal (paragraph 20 of your letter)

30. Clause 48 of the Bill provides that lodging an appeal against a decision does not by itself operate as a stay of execution of the decision, but the organisation may apply to the appeal board for a stay of execution of the decision. In *PCCW-HKT Telephone Ltd v Telecommunications Authority* (2005) 8 HKCFAR 337, the Court of Final Appeal stated that the discretion for granting a stay of execution of decision involves the balancing of all its supporting and opposing factors for considerations.

31. The Bill does not set out the considerations for exercising the discretion to grant a stay of execution of a decision, so as to leave flexibility for the appeal board to decide whether to suspend the execution of decision based on the facts and circumstances of each case, having regard to all relevant factors. The appeal board may also consider all the factors mentioned in precedent cases in accordance with common law principles. This is in line with similar provisions in other Hong Kong legislation (for example, section 227 of the Securities and Futures Ordinance (Cap. 571) and section 69 of the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615)), in which the factors for consideration are not specified.

Whether the finality of the appeal board's decision is consistent with

Article 82 of the BL (paragraph 21 of your letter)

32. The provision in the Legislative Council Ordinance (Cap. 542) in relation to *Mok Charles v Tam Wai Ho* (2010) 13 HKCFAR 762 regarding the finality of the Court of First Instance's decision on an election petition is not comparable with the provision in clause 49 of the Bill. Clause 49 of the Bill provides that the decision of the appeal board is final, which is a common practice in appeal mechanisms stipulated in other ordinances (e.g. section 121 of the Financial Institutions (Resolution) Ordinance (Cap. 628) and section 134 of the Travel Industry Ordinance (Cap. 634)). This does not preclude the affected parties from applying for judiciary reviews regarding the relevant decisions, subject to the satisfaction of the general principles and conditions of judiciary reviews. Therefore, the provision do not affect the power of final adjudication vested in the Court of Final Appeal.

Part 8: Miscellaneous matters

Whether designated authorities have the power to exempt CI operators from taking statutory obligations (paragraph 22 of your letter)

33. Clause 55 of the Bill empowers the Commissioner to exempt CI operators from complying with certain statutory obligations. The objective of the Bill is to require CI operators to fulfil specified statutory obligations in order to protect the security of their computer systems. Such obligations should not be easily exempted. Whether it is in the public interest to exempt CI operators from fulfilling specific statutory obligations should be a matter for the Commissioner, who has complete knowledge of the implementation of the Bill, to decide upon full consideration. As the regulation of the designated authorities is confined to their specific sectors, it is not appropriate to grant them the right of exemption.

34. In practice, if the subject of exemption falls within the purview of the regulating authority, the Commissioner will consult the designated authority to ensure that the decisions made are well-informed and based on professional assessment. Such arrangements can strike a better balance between the statutory obligations and the CI operators' actual circumstances.

Reasons for not specifying the Commissioner's power to prosecute offences (paragraph 23 of your letter)

35. As the Commissioner and the authorised officers appointed by him

under clause 50 of the Bill are public officers, the Secretary for Justice may, pursuant to section 12 of the Magistrates Ordinance (Cap. 227), give directions to authorise the officers concerned to make prosecutions at magistrates. There is no need to specify their power of prosecution in the Bill. On the other hand, designated authorities and the authorised officers appointed by them under clause 51 of the Bill are not necessarily public officers. Section 12 of the Magistrates Ordinance is not necessarily applicable, and thus clause 56 of the Bill empowers designated authorities to prosecute offences specified in the clause.

Whether consideration will be given to prescribing the CoPs in the form of subsidiary legislation (paragraph 24 of your letter)

36. Clause 8(8) of the Bill states that a CoP is not subsidiary legislation. The CoPs seek to provide guidelines for CI operators in fulfilling their statutory obligations under the Bill. They have no legislative effect and do not involve the Legislative Council's (LegCo) exercise of powers and functions to enact, amend or repeal laws, as stipulated under Article 73 of the BL. Failure of CI operators to fulfil statutory obligations in accordance with the provisions of the CoPs does not in itself constitute an offence. As long as the objectives of the statutory obligations are met, it is open for CI operators to fulfil their statutory obligations by similar ways other than those set out in the CoPs. It is also common for similar guidelines to be set out in CoPs, which are not subsidiary legislation. Examples are section 201 of the Financial Institutions (Resolution) Ordinance (Cap. 628), section 6A of the Occupational Retirement Schemes Ordinance (Cap. 426), section 96 of the Private Columbaria Ordinance (Cap. 630) and section 102 of the Private Healthcare Facilities Ordinance (Cap. 633) etc. under the Hong Kong laws.

Whether consideration will be given to setting out in detail the regulations that may be made by the Secretary for Security (paragraph 25 of your letter)

37. Clause 69 of the Bill confers power upon the Secretary for Security (the Secretary) to make regulations for the better carrying out of the provisions of the Ordinance, which is a common practice under Hong Kong's legal system. The regulations are subsidiary legislation subject to LegCo's scrutiny. Primary legislation generally provides for important or critical matters in a legislative proposal. As for detailed and technical matters, such as implementation details to be formulated for

the execution of the primary legislation, administrative matters, provisions requiring the executive authorities' continuous review and improvements or matters that need timely enactment or amendments, it is appropriate to empower the executive authorities to make regulations by way of subsidiary legislation.

38. Clause 69 of the Bill confers power upon the Secretary to make regulations. Such power has a clear scope of authorisation and is subject to statutory restraint. According to clause 69 of the Bill, the making of regulations by the Secretary must be for the purpose of better carrying out of the clauses of the Bill. Meanwhile, in accordance with section 28(1)(b) of the Interpretation and General Clauses Ordinance (Cap. 1), the content of the subsidiary legislation must not exceed the scope of the matters regulated under the primary legislation.

39. Regulations made by the Secretary under clause 69 are subsidiary legislation subject to the "negative vetting procedure" by LegCo in accordance with section 34 of the Interpretation and General Clauses Ordinance (Cap. 1). Upon scrutiny, LegCo can, by resolution, make amendment to or even repeal the subsidiary legislation.

40. As regards amendments of Schedules to the Bill, the Secretary may make amendments by notice published in the Gazette in accordance with clause 70 of the Bill. The Gazette notice concerned will have legislative effect and will be subsidiary legislation. The "negative vetting procedure" also applies to such amendments.

41. We hope that the information above will facilitate the Bills Committee in its scrutiny of the Bill.

Yours sincerely,

(Michelle CHOI)
for Secretary for Security

13 January 2025

c.c.
Department of Justice
(Attn: Mr Ivan LEUNG Acting Principal Government Counsel
Mr Gary LI Senior Assistant Law Draftsman)

Hong Kong Police Force
(Attn: Mr Raymond LAM Chief Superintendent (Cyber Security and Technology Crime Bureau))

Digital Policy Office
(Attn: Ms Candy CHAN Assistant Commissioner)