For information
on 8 October 2024

Legislative Council Panel on Security

Proposed Legislative Framework to Enhance Protection of the Computer Systems of Critical Infrastructures

Consultation Report

PURPOSE

On 2 July 2024, the Security Bureau (SB) launched a one-month consultation on the Proposed Legislative Framework to Enhance Protection of the Computer Systems of Critical Infrastructures. The consultation period ended on 1 August 2024. This paper aims to brief Members on the findings of the consultation and set out the way forward for implementing the legislative work.

LEGISLATIVE BACKGROUND

2. With the rapid development in information and communication technologies, the operation of critical infrastructures (CI) has become more dependent on the secure and smooth operation of computer systems, and at the same time faces increasing risks of cyberattacks. In the event that the computer systems of CI are being disrupted or sabotaged and cannot operate normally, the essential services delivered by such CI will be affected. This may even have a rippling effect affecting the entire society, seriously jeopardising the economy, people's livelihood, public safety and even national security.

3. In recent years, laws and regulations protecting the security of computer systems of CI have become increasingly common in other jurisdictions. Similar legislation has been enacted in the Mainland China, Macao Special Administrative Region, Australia, the European Union (EU), Singapore, the United Kingdom (UK) and the United States (US). A relevant bill is also under deliberation by the Parliament of Canada.

4. As announced by the Chief Executive (CE) in his Policy Address published in October 2022, legislation would be enacted for the enhancement of the cybersecurity of CI. Having regard to the circumstances in Hong Kong, and with reference to the practices in other jurisdictions (see paragraph 3) as well as the latest international standards, SB proceeded to draft a new piece of legislation to strengthen the security capabilities of computer systems of CI, thereby enhancing

the overall computer system security in Hong Kong. The proposed legislation is tentatively entitled the Protection of Critical Infrastructures (Computer Systems) Bill (the proposed legislation).

5. As the proposed legislation mainly affects potential organisations to be designated as critical infrastructure operators (CIOs), cybersecurity service providers, audit firms and sector regulators, we had initiated preparatory discussions with these stakeholders before officially launching the consultation, so as to consider their views in drawing up the proposed legislative framework.

Preparatory Discussions with Stakeholders

6. Since 2023, SB has organised more than 15 preparatory discussion sessions for over 115 stakeholders to solicit their views on the preliminary proposed legislative framework. They unanimously supported the legislation in principle and agreed that it was the common responsibility of all sectors of the community to safeguard the security of computer systems.

Consultation Exercise

7. On 2 July 2024, SB submitted the discussion paper on Proposed Legislative Framework to Enhance Protection of the Computer Systems of Critical Infrastructures **(Annex I)** to the Legislative Council (LegCo) Panel on Security for comments, and received unanimous in-principle support from Members. A one-month consultation was launched on the same day. The legislative proposals are summarised below:

(a) with regard to the need, the legislative purpose and the principles for protecting the computer systems of CI, proposes that only those expressly designated as CIOs and critical computer systems (CCSs) will be regulated and subject to statutory obligations;

(b) the scope of regulation of the proposed legislation should cover infrastructures for delivering essential services in Hong Kong or other infrastructures for maintaining important societal and economic activities;

(c) to lay down requirements concerning the CIOs' obligations, i.e. organisational, preventive, and incident reporting and response;

(d) to set up a Commissioner's Office headed by a Commissioner appointed by the CE to be responsible for implementing the legislation;

(e) to designate sector regulators as designated authorities, which will be responsible for monitoring the discharging of organisational and preventive obligations by CIOs in their respective sectors;

(f) to adopt an "organisation-based" approach in introducing the relevant offences and financial penalties;

(g) to establish an appeal board to handle appeals lodged by CIOs who disagree with a designation or written directions issued by the Commissioner's Office;

(h) to empower the Secretary for Security to introduce subsidiary legislation to specify or amend the service sectors that may be designated as CI, the list of designated authorities and the types of material changes and incidents required to be reported to the Commissioner's Office; and

(i) to establish Codes of Practice (CoPs) with reference to internationally recognised methodology and standards, in which the proposed standards and scope of various statutory obligations, including independent computer system security audits and risk assessment reports, will be set out.

8. SB has set up a **dedicated webpage** to introduce the proposed legislative framework in the form of frequently asked questions and infographics. Relevant legislation in other jurisdictions has also been uploaded to the webpage to facilitate the public's understanding of the content of the proposed legislation.

(1) Consultation Sessions

9. During the consultation period, SB organised **five consultation sessions** for the industry, covering highlights of the proposed legislation. The **consultation sessions** were attended by nearly 200 stakeholders, including potential organisations to be designated as CIOs, cybersecurity service providers and audit firms. Representatives of the Hong Kong Monetary Authority (HKMA) and the Communications Authority (CA), i.e. proposed designated authorities under the proposed legislation, were also invited to two of the consultation sessions. During the consultation sessions, stakeholders enthusiastically raised constructive

questions and views, while representatives of SB and designated authorities made active responses. Views received in these five consultation sessions are summarised below. It was suggested that the proposed legislation should:

(a) clearly elaborate the definitions of CIO and CCS and set out the information that must be reported to the Commissioner's Office in case of material changes to CCSs;

(b) set out the functions of computer system security management units to be set up by CIOs;

(c) give detailed descriptions of "serious computer system security incidents", "other computer system security incidents" and "serious data leakage";

(d) as regards the statutory obligation of making a report within the specified time frame after becoming aware of a computer system security incident, refine the definition of "becoming aware of";

(e) clarify the CIOs' statutory obligations on compliance when third-party service providers are employed;

(f) streamline the procedures for discharging statutory obligations under the proposed legislation, so as to avoid unnecessary costs and duplicated efforts of CIOs regulated by designated authorities; and

(g) list the types of information that shall be submitted to the Commissioner's Office by CIOs, and the mode and confidentiality measures for submission.

(2) Written Submissions

10. During the consultation period (i.e. ending 1 August), SB received a total of 53 submissions by means of email and post, among which 52 (accounting for 98.1%) supported the legislation and the framework of the bill, or raised positive suggestions; 47 submissions, which were received from the industry, unanimously supported the legislation or raised positive suggestions. The only objection came from a human rights organisation registered in the UK, which raised objections regarding the protection of freedom of speech, powers of the Commissioner's Office, designated sectors, etc. SB immediately made a rebuttal to clarify the misconceptions. Other views received covered different

areas of the legislative proposal, which served as valuable reference in formulating the proposed legislation.

(3) Data Analysis of Written Submissions

11. The written submissions are from the following categories:

Category of Respondents			Number
(a)	**Organisations that may be designated as CIOs**		
	Category 1	Energy	3
		Banking and financial services	5
		Land transport	1
		Air transport	3
		Healthcare services	2
		Communications and broadcasting	7
	Category 2	Research and development parks	3
		Exhibition venues	2
		Sports venues	1
	Sub-total of Category (a) (% of the overall)		**27 (50.9%)**
(b)	**Political parties and LegCo members**		**2 (3.8%)**
(c)	**Sectoral professional bodies, professional institutions, associations and chambers of commerce**		
	Information technology		8
	Communications		1
	Engineering		1
	Banking		1
	Commerce		2
	Sub-total of Category (c) (% of the overall)		**13 (24.5%)**
(d)	Cybersecurity service providers		4
	Information technology audit companies		1
	Statutory bodies		2
	Sub-total of Category (d) (% of the overall)		**7 (13.2%)**
(e)	Uncategorised members of the public		3 (5.7%)
(f)	Foreign human rights organisations and others		1 (1.9%)
Total (% of the overall)			**53 (100%)**

(4) Content Overview of Written Submissions

12. We have collated the above comments and suggestions received. The major comments and suggestions with the relevant remarks are summarised in **Annex II**. The key points are set out in paragraphs 13 to 25 below.

A. Legislative Purpose and Principles

13. We received a total of 57 items of submissions or views in relation to the legislation purpose and relevant principles. The key comments are as follows:

> There was overall support for the Government's legislation for protecting the CI of Hong Kong, or positive suggestions to improve the content of the proposed legislation. It was agreed that CIOs should take on and fulfil their statutory obligations.
>
> [**Remarks:** We thank sectoral stakeholders for their valuable views and professional suggestions, all of which will be given careful consideration. The Government will continue to maintain communication with stakeholders in various sectors to improve the legislative framework and the content of the CoP in an ongoing manner.]

B. Scope of Regulation

14. We received a total of 31 items of comments, suggestions for enquiries. Respondents mainly took the view that the information technology sector should be clearly defined. There were also suggestions that more sectors should be covered and extraterritorial jurisdiction should be removed. The key comments are as follows:

(a) The scope of regulation of the proposed legislation covers infrastructures for delivering essential services in Hong Kong (eight sectors, i.e. energy, information technology, banking and financial services, land transport, air transport, maritime, healthcare services, and communications and broadcasting) or other infrastructures for maintaining important societal and economic activities (e.g. major sports and performance venues, research and development parks, etc.). There were views that since information technology was involved in the operation of CIs in different sectors, there should be clearer criteria

to define whether individual operators fall into the "information technology" sector.

[**Remarks:** Drawing reference from relevant legislation of other jurisdictions (including the US, Australia, Singapore and the Mainland), SB considers it appropriate to categorise "information technology" as one of the CI sectors. As for whether an individual organisation and its operator should fall into the "information technology" sector, SB will, before making a decision based on the definition, maintain close communication with the potential operators to be designated.]

(b) The proposed legislation empowers the Commissioner's Office to, in the course of investigating an incident or offence related to the statutory obligations of CIOs, require CIOs to submit relevant information available to them, even if such information is located outside Hong Kong. There were concerns that the proposed legislation may involve law enforcement actions against computer systems located outside Hong Kong.

[**Remarks:** The proposed legislation does not have extraterritorial effect. The Commissioner's Office will ensure that it will only request information that is accessible by operators with offices set up in Hong Kong, and will allow them reasonable time for preparation.]

C. Targets of Regulation

15. We received a total of 74 items of comments, suggestions or enquiries. Respondents largely took the view that there should be clear definitions, conditions and scopes for CI, CIO and CCS, so that they could assess the need for preparation. The key comments are as follows:

(a) Under the proposed legislation, only computer systems that are relevant to the provision of essential service or the core functions of CIs, and those systems which, if interrupted or damaged, will seriously impact the normal functioning of the CIs will be designated as CIOs and CCSs. Some suggested that other pertinent considerations, such as quantifiable indicators, should be included to ensure that objective standards are attained.

[**Remarks:** CIOs and CCSs will be designated on a definition basis. The Commissioner's Office will, through mutual communication and

understanding with the operators and with due consideration given to other relevant factors, determine whether a designation is suitable.]

(b) Regarding the consideration that an interconnected computer system will be designated as CCS if the loss of its functionality may affect the provision of essential services by the operator, there were views that such a coverage will be too broad.

[**Remarks:** We have defined CCS under the proposed legislation after taking into account the situation of Hong Kong and drawing reference from the relevant legislation in other jurisdictions. We consider such definition appropriate. The Commissioner's Office will, based on the definition, only designate a computer system necessary for the operator's provision of essential services as a CCS after adequate communication with the operator and thorough consideration. However, as "interconnected" may not accurately reflect the factors of consideration in designating a CCS, SB will seriously consider deleting the term.]

D. Obligations of CIOs

I. Organisational Obligations

16. We received 36 items of comments, suggestions or enquiries. Respondents mainly expressed concerns that there may be practical difficulties in making timely reports of changes in ownership. Some also suggested that the definition of operatorship should be clarified, and proposed ways to optimise resources in establishing the computer system security management unit. The key comments are as follows:

(a) Under the proposed legislation, we originally proposed that CIOs should report changes in the ownership of their CIs. There were views that it would be difficult for organisations (in particular listed companies) to report frequently to the Commissioner's Office about the changes in ownership.

[**Remarks:** SB understands the practical difficulties that the operators may encounter in reporting the changes in ownership and will seriously consider removing such requirement.]

(b) Under the proposed legislation, CIOs are required to set up a dedicated unit to manage the security of computer systems and to follow up on

the directions given by the Commissioner's Office. There were concerns that it was difficult nowadays to hire competent computer system security personnel, and suggestions for relaxing the qualification requirements of relevant talents.

[**Remarks:** The proposed legislation will not stipulate the statutory qualification requirements of computer system security personnel to be appointed by the operators. In drawing up the CoP, SB will compile a detailed list of eligible professional qualifications to facilitate the operators' appointment of suitable personnel.]

II. Preventive Obligations

17. We received a total of 105 items of comments, suggestions or enquiries. The major views were that there should be clearer criteria and requirements for reporting changes to CCSs. Besides, there were enquiries on how to safeguard the confidentiality of system information disclosed, and whether international or industry standards could be adopted in formulating the computer system security management plans and conducting the risk assessments or audits, so as to minimise duplication of efforts. The key comments are as follows:

(a) The proposed legislation requires CIOs to conduct computer system security risk assessments and audits regularly. Some expected clearer descriptions of the scopes of assessments and audits (in particular industrial control systems involving operational technology and interconnected computer systems located outside Hong Kong), the standards to which reference could be made and the format of incident reports.

[**Remarks:** In developing the content of the CoP, SB will make reference to the latest technology and international standards, and draw up recommended standards that conform to the statutory requirements.]

(b) The proposed legislation requires CIOs to report material changes concerning the design, configuration, security or operation of CCSs. There were views that the information reported should not involve sensitive or confidential information.

[**Remarks:** The proposed legislation is not targeted at the personal data or commercial confidential information in the CIOs' computer systems. The aim of requiring operators to provide information is to

ensure that the operators properly fulfil their obligations in protecting their CCSs, and to enable the Commissioner's Office to, when a CCS incident arises, effectively assess the severity of the incident to the society and the threats to other operators. In carrying out its functions under the proposed legislation. Therefore, the Commissioner's Office will request CIOs to provide the necessary information in accordance with the legislation.]

(c) The proposed legislation requires CIOs to conduct security audits and submit reports regularly. There were views that clearer criteria should be laid down on the independence of the audits and the qualifications of audit staff.

[**Remarks:** We consider independence one of the fundamental principles of audits. Thus, the auditing parties should be independent of the audited parties to avoid conflicts of interest and to ensure the impartiality and objectivity of audits. The Commissioner's Office will set out in detail the qualification requirements for audit staff in the CoP by making reference to internationally recognised standards and relevant professional qualifications.]

III. Obligations on Incident Reporting and Response

18. We received a total of 88 items of comments, suggestions or enquiries. The comments were mainly about setting clear criteria and requirements for incident reporting, relaxing the time frame for reporting, minimising efforts to avoid repeated reporting, and allowing flexibility for security drills. The key comments are as follows:

(a) There were views that it will be difficult for organisations to conduct a timely investigation into the nature and cause of a serious computer system security incident within two hours after becoming aware of the incident (or within 24 hours after the occurrence of other incidents) and report to the Commissioner's Office, as required in the proposed legislation.

[**Remarks:** SB understands the actual difficulties that operators may encounter in incident reporting and has made reference to the relevant requirements in the UK, the EU and the US. SB will seriously consider relaxing the time frame for reporting serious computer system security incidents from 2 hours to 12 hours after being aware of the incident, and from 24 hours to 48 hours after being aware of other incidents. Meanwhile, to ensure effective and early response to

incidents, we have made reference to the practices in Singapore and Australia, and propose that when a CCS necessary for an operator's provision of essential services has been or is likely to be disrupted, or its services interrupted, the Commissioner's Office should be empowered to proactively investigate the cause directly with the operator, so as to ascertain whether it is caused by an attack.]

(b) As for the requirement under the proposed legislation that CIOs should notify the Commissioner's Office within 24 hours after becoming aware of other computer system security incidents, some suggested refining the definition of incidents required to be reported.

[**Remarks:** In the proposed legislation, a computer system security incident refers to an act or activity carried out without lawful authority on or through a computer or computer system that jeopardises or adversely affects its cybersecurity or the cybersecurity of another computer or computer system. The CoP will elaborate on the coverage of "incidents required to be reported" and give examples.]

(c) The proposed legislation requires CIOs to participate regularly in computer system security drills organised by the Commissioner's Office. Some suggested setting a minimum requirement or scale for the drills, so as to minimise the impact on services due to participation in the drills.

[**Remarks:** It is proposed under the proposed legislation that operators will be required to participate in a computer system security drill organised by the Commissioner's Office at least once every two years. This requirement is set after making reference to the practices in different jurisdictions, including Singapore, as well as international standards. We consider such requirements and arrangements for the computer system security drills appropriate.]

E. The Commissioner's Office

19. We received a total of 35 items of comments, suggestions or enquiries. Respondents mainly enquired about the circumstances under which the Commissioner's Office would issue a written notice, ways of data protection and division of work with the Police or the Office of the Privacy Commissioner for Personal Data (PCPD Office). There were also suggestions that the Commissioner's Office should proactively gather intelligence relating to cybersecurity risks. The key comments are as follows:

(a) Some expressed concerns over the confidentiality of the data and the measures taken by the Commissioner's Office to ensure security in the collection, storage and destruction of the data received.

[**Remarks:** The proposed legislation is not targeted at the personal data or the commercial confidential information in the CIOs' computer systems. The Commissioner's Office will handle the data in accordance with the relevant legislation and internal guidelines, and will establish an internal confidential system to ensure security in the transmission and storage of data.]

(b) Considering that CIOs may need to report a computer system incident to both the PCPD Office and the Commissioner's Office if personal data was leaked in the incident, some suggested putting in place a set of work procedures to avoid duplication of efforts by the operators.

[**Remarks:** The purposes for reporting an incident to the Commissioner's Office and to the PCPD Office are different, and so are the details of the reports. While the Commissioner's Office is responsible for identifying the reasons for data leakage and plugging the loopholes as soon as possible, the PCPD Office focuses on the protection of personal data. Hence, where an incident involves cyberattack on a computer system resulting in leakage of personal data, the operator does need to report it to both the Commissioner's Office and the PCPD Office, but "duplication" of efforts does not exist, for the purposes of reports submission and the follow-up actions taken will be different.]

F. Designated Authorities

20. We received a total of 20 items of comments, suggestions or enquiries. The major views were that the needs for individual sectors should be coordinated in order to avoid duplication of compliance work. The key comments are as follows:

Individual statutory sector regulators are familiar with the operations and needs of their sectors and operators, and have the proper structures and capabilities of monitoring the operators in protecting the security of the computer systems of CIs. In this regard, it was proposed in the proposed legislation that the HKMA be designated for regulating some organisations in the banking and financial services sector, and the CA be designated for regulating some organisations in the communications and broadcasting

sector. There were views that the existing regulatory mechanisms of the sectors should be adopted, or the compatibility of the mechanisms should be enhanced, so as to reduce the compliance costs of the industries.

[**Remarks:** CIOs of designated sectors will discharge their organisational and preventive statutory obligations as stipulated in the proposed legislation by complying with the guidelines issued by the designated authorities of the sectors. In addition to the baseline requirements that are applicable to all sectors, standards and methodologies that are applicable to relevant operators will be formulated and set out in the CoP through close communication with various sectors and risk assessment, thereby assisting them in meeting the statutory requirements.]

G. Offences and Penalties

21. We received a total of 96 items of comments, suggestions or enquiries. Respondents mainly expressed concerns about possible legal liabilities resulting from non-compliance by third-party service providers. There were suggestions to introduce a grace period for adequate preparation and to allow circumstances for reasonable excuse. The key comments are as follows:

(a) There were views that the penalties under the proposed legislation are excessive. Some suggested setting out clear criteria for imposing the penalties, as well as the circumstances under which "reasonable excuse" could be given. There were also suggestions that the fines should be imposed according to the scale and financial capability of the operators.

[**Remarks:** The legislative intent is not to punish the CIOs. The purpose of the offences and penalties is to ensure that the legislation can be effectively implemented and enforced. The offences and penalties under the proposed legislation have taken into account the situation of Hong Kong and relevant legislation in other jurisdictions. Therefore, we consider the penalties currently proposed are appropriate. The Commissioner's Office will make positive efforts to assist the operators in improving their organisation structure and capability of preventing security incidents so as to avoid breaching the law.]

(b) The proposed legislation also requires CIOs to take measures to ensure that even with the hiring of third-party service providers, their CCSs still comply with the relevant statutory obligations. There were

concerns that it is difficult to ensure that the third-party service providers (in particular service providers located overseas) will comply with the agreement and legislation. In this regard, some called for clarifications on the legal liabilities to be borne by the operators in the event of non-compliance by the third-party service providers.

[**Remarks:** Under the proposed legislation, CIOs could be allowed to engage third-party service providers, but the operators still need to fulfil the relevant statutory obligations under the legislation. SB will draw reference from the experience of other jurisdictions. More guidelines on "due diligence" performance and "reasonable endeavor" will be included in the CoP, which will serve as reference for CIOs when they draw up and enforce contracts with third-party service providers.]

(c) Some expected a grace period regarding the effective date of the legislation, so as to allow the industry ample time for assessing system risks, devising incident response plans, hiring talents and discussing contract terms with third-party service providers.

[**Remarks:** The Government aims to set up the Commissioner's Office within one year upon the passage of the proposed legislation, after which to bring the proposed legislation into force within half a year's time. In the meantime, SB and the Commissioner's Office will maintain close communication with potential operators to be designated, and will designate CIOs and CCSs in a phased manner having regard to the risk and level of readiness of organisations, while developing relevant content of the CoP. As for statutory obligations under the proposed legislation such as risk assessment, independent audit and submission of relevant reports, the time frames will be calculated from the time of designation. Therefore, potential organisations to be designated as CIOs should have ample preparation time.]

H. Investigation Powers of the Commissioner's Office

22. We received a total of 25 items of comments, suggestions or enquiries. The enquiries were mainly in relation to the scope of request for information from, investigation on and on-site collection of evidence from CIOs. The key comments are as follows:

There were concerns that the connection of equipment to or installation of programmes in CCSs by the Commissioner's Office, which is empowered by the proposed legislation, may impede the normal operation of CCSs.

[**Remarks:** The proposed legislation stipulates that only when a CIO is unwilling or unable to respond to a serious incident on its own would the Commissioner's Office consider applying to a Magistrate for a warrant to connect equipment to or install programmes in CCSs in view of necessity, appropriateness, proportionality and public interest, so as to respond to the incident. Relevant regulators in other jurisdictions (such as Australia and Singapore) also have similar powers.]

I. Appeal Mechanism

23. We received a total of 14 items of comments or suggestions, mostly concerning the method for forming the appeal board and details of the appeal procedures. The key comments are as follows:

It was proposed under the proposed legislation that an appeal board be established to handle appeals against designations of CIOs or CCSs and written directions issued by the Commissioner's Office. There were enquiries about the method for forming the appeal board, for example, whether the board members possess the relevant expertise of the sector, and ways to fulfil confidentiality and maintain independence of the board.

[**Remarks:** Drawing reference from the arrangements of various existing statutory appeal boards, SB proposed that under the proposed legislation, the appeal board will be a team comprising of about 15 experts from the industry, cybersecurity and legal profession (including one board chairperson) appointed by the CE. The board members should be independent of the Commissioner's Office. Each appeal hearing will be conducted by three board members. The three board members must make a declaration about the absence of conflict of interest (e.g. industry competitors) and sign a non-disclosure agreement on the content of the hearing.]

J. Subsidiary legislation

24. We received a total of three items of comments and suggestions, mainly concerning the legislative process and mechanism. The key comments are as follows:

The proposed legislation empowers the Secretary for Security to, by way of subsidiary legislation, supplement, update or amend in future, where necessary, details relating to the powers of the Commissioner's Office or the statutory obligations of the operators. There are concerns that the subsidiary legislation would be used to bypass the legislative process.

[**Remarks:** The enactment and amendment of a subsidiary legislation are subject to an established set of highly stringent procedures to ensure fairness, openness, impartiality and transparency, and such procedures are monitored by the LegCo.]

K. CoP

25. We received a total of 53 items of comments or suggestions. Respondents mainly suggested providing clear guidelines and requirements for computer system security training. There were enquiries and suggestions regarding the early formulation of the CoP in accordance with international or industry standards and expert advice from the industry. There were also suggestions regarding enhanced baseline requirements. The key comments are as follows:

(a) As regards the formulation of the content of the CoP, various sectors suggested inviting the participation of sectoral experts and widely consulting the industry, and that the content should be developed in accordance with international standards.

[**Remarks:** In formulating the CoP, the Commissioner's Office will take into full account the views of industry stakeholders. Practicable requirements will be imposed based on the prevailing international standards or characteristics of the industries, having regard to the uniqueness of the sectors. The Commissioner's Office will also review and improve the content of the CoP in an ongoing manner.]

(b) Regarding the computer system security training under the computer system security management plan as outlined in the summary of the CoP, it was proposed that the CIOs should provide training for vendors, contractors or service providers, etc. There were views that the scope, depth and methodology of training as well as the types of personnel to be trained should be clearly stated.

[**Remarks:** In formulating the CoP, the Commissioner's Office will set out in detail the requirements and scope of the computer system

security training and provide relevant information on training for reference.]

WAY FORWARD

26. By making reference to the views received during the consultation, SB will endeavor to finalise the Protection of Critical Infrastructures (Computer Systems) Bill soonest for introduction to the LegCo for scrutiny within this year. Our goal is to set up the Commissioner's Office within one year upon the passage of the legislation. In the meantime, we will continue to maintain liaison with stakeholders from various sectors and jointly develop a CoP that is applicable to the sectors. We will also closely communicate with potential operators to be designated and confirm whether they meet the criteria for designation, while identifying CCSs that are necessary for the operators' provision of essential services. We will designate CIOs in a phased manner having regard to the impact of their systems on the society and their level of readiness, thereby enhancing the overall computer system security in Hong Kong.

CONCLUSION

27. Members are invited to note the above findings of consultation and way forward.

Security Bureau
October 2024

For discussion on
2 July 2024

Legislative Council Panel on Security
Proposed Legislative Framework to Enhance Protection of the Computer Systems of Critical Infrastructure

PURPOSE

This paper briefs Members on the Government's proposed legislative framework for enhancing protection of computer systems of critical infrastructures ("CIs").

LEGISLATIVE BACKGROUND

2. CIs refer to the facilities that are necessary for the maintenance of normal functioning of the Hong Kong society and the normal life of the people, such as banks, financial institutions, telecommunications service providers, electricity supply facilities, railway systems, etc. In the event that the information system, information network or computer systems of CIs are being disrupted or sabotaged, the normal operation of their main facilities may be affected. This may have a rippling effect affecting the entire society, seriously jeopardising the economy, people's livelihood, public safety and even national security. For example, when essential services such as power and fuel supply, communications, large-scale transportation, finance, etc., are brought to a halt due to cyberattack, the normal functioning of society will be seriously affected, bringing the whole society to a standstill.

3. At present, we do not have any statutory requirements on the protection of the computer systems of CIs. However, with the rapid development in information and communications technologies, the operation of CIs has become more dependent on the Internet, computer systems, telecommunications infrastructure and smart devices, etc. Their computer systems are, therefore, more vulnerable to cyberattacks.

4. In fact, CIs around the world are at risk of being cyberattacked maliciously. There have been incidents where CIs were attacked and caused major impacts on societies. For example, in 2021, a fuel transportation pipeline operator in the United States ("US") suffered from a ransomware attack, which

hindered nearly half of the fuel supply on the east coast of the US. In 2024, a medical insurance company in the US was also attacked by ransomware. Medical services were partly suspended, and a large amount of personal and medical information were at risk of being leaked. In 2024, a data centre in Sweden was attacked by hackers, disrupting the operations of the government and businesses. Similar incidents happened in Hong Kong as well. In 2024, the computer system of a private hospital in Hong Kong was attacked by hackers using ransomware, causing the computer system to malfunction and affecting medical services.

5. In recent years, laws and regulations protecting the security of computer systems of CIs have become increasingly common in other jurisdictions. Similar legislations have been enacted in the Mainland China, Macao Special Administrative Region ("Macao SAR"), Australia, the European Union ("EU"), Singapore, the United Kingdom ("UK") and the US, etc. A relevant bill is also under deliberation by the Parliament of Canada. Details are listed in (a) to (h) below:

(a) **Mainland China**: Cybersecurity Law (2016) and Regulation for Safe Protection of Critical Information Infrastructure (2021);

(b) **Macao SAR**: Cybersecurity Law (2019);

(c) **Australia**: Security of Critical Infrastructure Act 2018;

(d) **UK**: Network and Information Systems Regulations 2018;

(e) **Singapore**: Cybersecurity Act 2018;

(f) **EU**: Directive on the measures for a high common level of cybersecurity across the Union 2022;

(g) **US**: There are different federal laws, state laws and certain industry rules, including:

- Cybersecurity and Infrastructure Security Agency Act of 2018 ("CISA")

- Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"); and

(h) **Canada**: The Parliament of Canada is scrutinising a bill submitted by the government in June 2022, which, upon passing, will become the Critical Cyber Systems Protection Act.

6. Notwithstanding the differences in the legislative approach and coverage in the various jurisdictions, all legislations explicitly require operators of CI to comply with a set of obligations, implement measures to protect their computer systems, enhance their capabilities to respond to cyberattacks, and report to the regulatory authority in the event of a security incident on computer systems. Response measures should be taken as soon as possible.

7. As announced by the Chief Executive in his Policy Address published in October 2022, legislation would be enacted for the enhancement of the cybersecurity CIs, so as to promote the establishment of good preventive management systems by operators of CI and secure the operation of their computer systems, enabling the smooth operation of essential services and consolidating Hong Kong's favourable business environment and status as an international financial centre.

PROPOSED LEGISLATIVE REGIME

8. Having regard to the circumstances in Hong Kong, and with reference to the practices in the jurisdictions mentioned in paragraph 5 above and the views received during the consultation with various stakeholders (including potential organisations to be designated as CI Operators ("CIOs"), cybersecurity service providers and audit firms, and sector regulators, etc.) since early last year, we **propose** to enact a new piece of legislation tentatively entitled the **Protection of Critical Infrastructure (Computer System) Bill** ("the proposed legislation").

9. As all the above jurisdictions we made reference to have set up a dedicated body to oversee the implementation of the relevant legislations, we also **propose** to establish a new **Commissioner's Office** for the implementation of the proposed legislation (see paragraph 25 of Part E below for details).

A. Legislative Purpose and Principles

10. Our legislative purpose is to require CIOs to fulfill certain statutory obligations and take appropriate measures on various fronts, so as to strengthen

the security of their computer systems and minimise the chance of essential services being disrupted or compromised due to cyberattacks, thereby enhancing the overall computer system security in Hong Kong.

11. We must emphasise the following legislative principles:

(a) the proposed legislation sets out a regulatory model that is suitable for Hong Kong with reference to legislative approaches of other jurisdictions (including Mainland China, Macau SAR, Australia, the EU, Singapore, the UK and the US);

(b) the proposed legislation seeks to regulate CIOs that are necessary for (i) the continuous delivery of essential services or (ii) maintaining important societal and economic activities in Hong Kong. In other words, operators to be regulated will mostly be large organisations, small and medium enterprises and the general public will not be affected;

(c) the proposed legislation will only require CIOs to bear the responsibility for securing their Critical Computer Systems (CCSs), and in no way will it involve the personal data and business information therein; and

(d) the statutory obligations are intended to be baseline requirements, from which CIOs can build up and enhance their capabilities for securing their computer systems with regard to their own needs and characteristics. Although the legislative intent of the proposed legislation is not to punish CIOs, in order to ensure effective implementation and enforcement of the proposed legislation, relevant offences and appropriate penalties must be stipulated. After balancing the impact of the proposed legislation on institutions and the need to ensure sufficient deterrent effect, penalties will be imposed on an organisation basis. That said, if the relevant violation involves infringement of existing criminal legislations, such as making false statements, using false instruments or other fraud-related crimes, as is the current situation, the officers involved could be held criminally liable personally.

B. Scope of Regulation

12. Having made reference to the practices of the UK and Australia, we **propose** that the proposed legislation should clearly provide that only expressly designated **CIOs** and **CCSs** will be regulated. Definitions of the key concepts are elaborated in paragraphs 13 to 23 below.

CIs

13. CIs are the linchpin of society and economy and are crucial to the normal functioning of the society. We **propose** that **CI** under the proposed legislation should cover two major categories as follows:

Category 1: Infrastructures for delivering essential services in Hong Kong

14. Essential services are services that are vital for our everyday life, which, if disrupted, compromised, or rendered unavailable for an extended period, will significantly impact the everyday life and functioning of the society. Drawing reference from the relevant legislation of the jurisdictions mentioned in paragraph 5 above and having regard to the circumstances in Hong Kong, we **propose** that the proposed legislation should cover the infrastructures of the following eight sectors of essential services:

(a) Energy;
(b) Information Technology;
(c) Banking and Financial Services;
(d) Land Transport;
(e) Air Transport;
(f) Maritime;
(g) Healthcare Services; and
(h) Communications and Broadcasting.

Category 2: Other infrastructures for maintaining important societal and economic activities

15. Apart from essential services, there are also other infrastructures (e.g. major sports and performance venues, research and development parks, etc.), where their damage, loss of functionality or data leakage may have serious implications on important societal and economic activities in Hong Kong. With reference to the practices of the UK, Australia, the US and the EU, we **propose**

that it is necessary to bring these facilities under regulation, with a view to protecting the secured operation of their computer systems.

C. Targets of Regulation

CIOs

16. Given that most of the CIs are operated by large organisations, with reference to the practices of the UK, Australia and the EU, we **propose** that the proposed legislation should adopt an "organisation-based" approach, i.e., using the organisation responsible for operating a CI as a basis in fulfilling its obligation to safeguard the security of its computer systems, so as to ensure that the overall computer system of each organisation is well protected and avoid loopholes.

17. As mentioned in paragraph 12 above, only operators which have been expressly designated as CIOs will be required to fulfill their statutory obligations. Having made reference to the practice of the UK, we **propose** that in deciding whether an infrastructure is a CI that needs to be regulated under the proposed legislation, the Commissioner's Office should take into account the following factors:

(a) as CIs are infrastructures that provide essential services or maintain important societal and economic activities in Hong Kong, consideration will be given to the implications on essential services and important societal and economic activities in Hong Kong if there was damage, loss of functionality, or data leakage in such infrastructures;

(b) as infrastructures use different methods and tools (including information technology) to deliver their services and maintain their operations, consideration will be given to the level of dependence on information technology of the infrastructures concerned. It will not be necessary to require them to comply with statutory obligations if information technology does not have significant implications on their operations; and

(c) as the second category of CIs covers infrastructures that could have serious implications on important societal and economic activities if there was damage, loss of functionality or data leakage, consideration

will be given to the importance of the data controlled by the infrastructures concerned.

18. Given that the proposed legislation adopts the "organisation-based" principle in requiring the bearing of statutory obligations, if the Commissioner's Office believes an infrastructure is a CI to be regulated under the proposed legislation according to the aforementioned reasons, the Commissioner's Office will take into account considerations such as the degree of control of an organisation over the CI concerned to decide whether to designate an organisation as a CIO under the proposed legislation that must undertake statutory obligations.

19. To prevent the CIs from becoming targets of cyberattack, we **propose** that the proposed legislation should only set out the names of the essential services sectors (viz. the eight sectors mentioned in paragraph 14 above), instead of disclosing the list of CIOs. This approach is in line with the practice of other jurisdictions (e.g. the UK and Australia).

20. For essential services operated by the Government (e.g. water supply, drainage, emergency relief, etc.), the Government has already put in place a set of detailed internal Government Information Technology Security Policy and Guidelines ("Policy and Guidelines"). The Policy and Guidelines are reviewed and updated regularly with reference to the latest international standards and industry best practices to ensure the security of Government information systems. The latest round of review and updating has been completed and the updated Policy and Guidelines were issued in April 2024. During the process, the Government has strengthened the Government's information security requirements with reference to the latest international standards on information security management to cope with the increasing cybersecurity risks. All Government departments must abide strictly by the Policy and Guidelines, and the Office of the Government Chief Information Officer (OGCIO) also regularly conducts compliance audits for Government departments. As the level of requirements in the Policy and Guidelines is comparable to the statutory requirements for CIOs under the proposed legislation, also, if a Government officer involved has breached any rules, the policy bureaux/departments will take appropriate disciplinary actions in accordance with the established procedures in the relevant regulations, such as the Civil Service Code, we **propose** to continue to regulate Government departments with the existing administrative approach without incorporating them into the proposed legislation.

CCS

21. Our primary objective is to regulate computer systems that are related to the normal functioning of the CIs, but not other systems. The CIs may have a large number of systems performing different functions at the same time. In order to enable the CIOs to focus their resources on the most important systems as required under the proposed legislation, and with reference to the relevant legislations in the jurisdictions referred to in paragraph 5 above, we **propose** to designate as "CCSs" only computer systems that are relevant to the provision of essential service or the core functions of computer systems, and those systems which, if interrupted or damaged, will seriously impact the normal functioning of the CIs. The requirements of the proposed legislation will apply to all CCSs, regardless of whether they are physically located in Hong Kong or not.

22. In terms of actual operation, the Commissioner's Office will consult the CIOs on what systems are essential to their operations and seek their assistance in considering whether any designation should be made.

23. As CIs are infrastructures that provide essential services or maintain important societal and economic activities in Hong Kong, the proposed legislation aims at allowing operators to focus their resources on the most important systems as required under the proposed legislation, other computer systems of CIOs that are not designated as CCS will not be subject to the provisions of the proposed legislation. For example, the personnel management system of an organisation will not be designated as a CCS if the loss of its functionality will not affect the provision of essential services by the organisation and it is not interconnected to the system through which the essential services are provided. This is in line with the practices of Australia, the UK and the EU.

D. Obligations of the CIOs

24. With reference to the relevant legislations in Australia, the UK and the EU, we **propose** that the obligations imposed on CIOs under the proposed legislation should be classified into three main categories: (I) organisational; (II) preventive; and (III) incident reporting and response. The objectives are to ensure that CIOs will put in place a sound management structure for protecting the security of computer systems, implement the necessary measures to prevent cyberattacks on computer systems of the CIs, and promptly respond to and recover

the affected systems in the event of computer system security incidents. The legislations in other jurisdictions also set out various obligations of the CIOs along this direction. These obligations include:

I. Organisational

(a) As CIOs operating CIs in Hong Kong shall comply with the following obligations on prevention of incidents as well as incident reporting and response, and to ensure that the Commissioner's Office can maintain communication with CIOs, CIOs shall provide and maintain an address and office in Hong Kong (and report any subsequent changes);

(b) To keep the Commissioner's Office updated on the ownership and operation of CIs and to allow the Commissioner's Office to make changes to the list of CIOs when necessary, CIOs shall report any changes in the ownership and operatorship of their CIs;

(c) To ensure that a dedicated unit is in place to manage the security of computer systems and to follow up on the directions given by the Commissioner's Office, a CIO must set up a computer system security management unit with professional knowledge (in-house or outsourced) and be supervised by the dedicated supervisor of the CIO.

II. Preventive

(d) To keep the Commissioner's Office updated on the CCSs of the CIOs and to allow the Commissioner's Office to make changes to or update the list of CCSs when necessary, CIOs shall inform the Commissioner's Office of material changes to their CCSs, including those changes to design, configuration, security, operation, etc.;

(e) To ensure that CIOs get prepared for possible incidents and make detailed plans on how to protect their computer systems, CIOs shall formulate and implement a computer system security management plan and submit the plan to the Commissioner's Office;

(f) To ensure that CIOs effectively monitor and control computer system security risks, CIOs shall conduct a computer system security risk assessment at least once every year and submit a report to the Commissioner's Office;

(g) To check CIOs' compliance of statutory obligations, CIOs shall conduct an independent computer system security audit at least once every two years and submit a report to the Commissioner's Office;

(h) To ensure CIOs' overall security posture and that their services will not be affected by security loopholes in systems of third-party service providers, CIOs shall adopt measures to ensure that their CCSs still comply with the relevant statutory obligations even when third party services providers are employed; and

III. Incident Reporting and Response

(i) To test the capabilities of CIOs in responding to attacks on CCSs, CIOs shall participate in a computer system security drill organised by the Commissioner's Office at least once every two years;

(j) To ensure an effective and proper response to emergency situations, CIOs shall formulate an emergency response plan and submit it to the Commissioner's Office;

(k) CIOs shall notify the Commissioner's Office of the occurrence of computer system security incidents in respect of CCSs within a specified time frame, so that the Commissioner's Office can promptly give directions on the response when necessary:

- Serious computer system security incidents (referring to incidents that have or about to have a major impact on the continuity of essential services and normal operating of CIs, or lead to a large-scale leakage of personal information and other data): report shall be made within 2 hours after becoming aware of the incident;

- Other computer system security incidents: report shall be made within 24 hours after becoming aware of the incident.

Upon request by the Commissioner's Office in the course of investigating an incident or offence related to obligation categories (I) to (III) above, CIOs must submit relevant information available to them, even if such information is located outside Hong Kong.

E. Commissioner's Office

25. With reference to the practices of various jurisdictions as mentioned in paragraph 5 above, to duly monitor computer system security of CCSs and ensure consistent implementation of the proposed legislation on CIs in different sectors, we **propose** to set up a Commissioner's Office under the Security Bureau (SB). The Commissioner's Office, headed by a Commissioner appointed by the Chief Executive, will perform the work under the proposed legislation. The key duties and functions of the Commissioner's Office include –

(a) designating CIOs and CCSs;

(b) establishing "Code of Practice" ("CoP") and giving advice on the measures to be adopted by CIOs;

(c) monitoring computer system security threats against CCSs;

(d) assisting CIOs in responding to computer system security incidents;

(e) investigating and following up on non-compliance of CIOs;

(f) coordinating with various government departments, e.g. the OGCIO, the Cyber Security and Technology Crime Bureau (CSTCB) of the Hong Kong Police Force (HKPF) and the Hong Kong Computer Emergency Response Team Coordination Centre, etc., in formulating policies and guidelines and handling incidents; and

(g) issuing written instructions to CIOs to plug potential security loopholes.

F. Designated authorities for individual sectors

26. Some of the essential service sectors to be regulated under the proposed legislation are already comprehensively regulated (e.g. through a licensing regime) by statutory sector regulators. In some sectors, there are even computer system security-related guidelines in place. Considering that these statutory sector regulators are the most familiar with the relevant operations and needs of their sectors, we **propose** to designate certain sector regulators as

designated authorities to monitor the discharging of organisational and preventive obligations by these essential services sectors (see the obligations set out in categories (I) and (II) at paragraph 24 above). The Commissioner's Office will take full charge of monitoring the CIOs of all the eight sectors in compliance of the obligations of incident reporting and response (see the obligations set out in category (III) at paragraph 24 above) (except with certain exemptions by the Commissioner's Office).

27. The above approach allows the designated authorities to establish sets of standards and requirements, on organisational and preventive obligations, under their existing regulatory regimes that best suit the sectors' needs. CIOs in these sectors will not need to fulfill additional requirements of the Commissioner's Office in relation to these two types of obligations. Furthermore, it ensures that the Commissioner's Office may fully grasp the incident and response arrangements of all CIOs for co-ordination, investigation and assistance, and to prevent the spread of the incident to other CIOs. Similar practice of delegating the regulation on sector regulators is also seen in relevant laws of the UK, Australia and the US.

28. At this stage, we **propose** to designate (1) the Monetary Authority ("MA") as the authority responsible for regulating some service providers in the banking and financial services sector, and (2) the Communications Authority (CA) as the authority responsible for regulating some service providers in the communications and broadcasting sector. The sectors overseen by these two designated authorities already have very mature and well-established regulatory regimes. They also have in place guidelines on computer system security, such as the "Cyber Resilience Assessment Framework" issued by the Hong Kong Monetary Authority, the "Code Practice on the Operation, Management of Internet of Things Devices" and "Security Guidelines for Next Generation Networks", etc., issued by the CA.

29. To be more specific, the designated authorities will be responsible for designating CIOs and CCSs under their respective groups/classes, monitoring and checking compliance and handling various reports submitted by CIOs according to their current regulatory approaches (such as licensing regime). In relation to the discharge of organisational and preventive obligations, CIOs only need to report to their respective designated authorities, and do not need to submit further reports to the Commissioner's Office. Designated authorities will issue guidelines based on the special circumstances of respective industries they regulate to achieve comparable standards set by the two categories of obligations

(i.e. organisational and preventive) under the proposed legislation, and impose appropriate penalties in the event of non-compliance.

30. However, in order to guarantee that the Commissioner's Office will have a full grasp of the situation of incident reporting and response of all CIOs, if computer security incidents are encountered, CIOs in these sectors must report to the Commissioner's Office under the requirements in the proposed legislation, in addition to reporting to designated authorities in accordance with the requirements of the existing regulatory regimes. This is to allow the Commissioner's Office to coordinate contingency plans and prevent the incident from spreading to other CIs. After receiving the report of the incident, the Commissioner's Office will investigate and address the incident together with CSTCB of the HKPF, and provide assistance to repair the relevant computer systems as soon as possible.

31. To ensure that the Commissioner's Office has full control over the security of CCSs in Hong Kong as a whole, the Commissioner's Office retains the power to issue written directions to all CIOs under the proposed legislation, irrespective of whether or not the CIO is under the supervision of a designated authority.

G. Offences and Penalties

32. As mentioned in paragraph 11, although the legislative purpose is to cause CIOs to take up the corporate responsibility to enhance protection of the security of their CCS and the legislative intent is not to punish CIOs, in order to ensure effective implementation and enforcement of the proposed legislation, relevant offences and appropriate penalties must be formulated. Violations under the proposed legislation without reasonable excuse may be prosecuted by the Commissioner's Office. With reference to the practices of the UK, Australia and the EU, we **propose** that the offences under the proposed legislation should include:

(a) CIOs' non-compliance with statutory obligations;

(b) CIO's non-compliance with written directions issued by the Commissioner's Office;

(c) non-compliance with requests of the Commissioner's Office under the statutory power of investigation; and

(d) non-compliance with requests of the Commissioner's Office to provide relevant information relating to a CI.

33. As mentioned in paragraph 11(d) above, although we **propose** that the offences and penalties under the proposed legislation will only be applicable to organisations and their heads or staff will not be penalised at the individual level, if the relevant violations touch upon existing criminal legislation, such as submitting false information to the Commissioner's Office could lead to making of false statements, the using of false instruments or other fraud-related crimes, as is the current situation, the personnel involved may be held personally criminally liable.

34. In terms of the proposed penalties for the offences, taking into account the legislative intent and in line with the relevant legislations of the UK and EU, we **propose** that the penalties under the proposed legislation will only include fines. The level of fines will be determined by court trials, with maximum fines ranging from HK$500,000 to HK$5 million. For certain offences, additional daily fines for persistent non-compliance will be imposed.

35. Generally speaking, if the non-compliance can be rectified through the CIOs' follow-up actions and will not have serious implications on their computer system security or the regulatory capabilities of the Commissioner's Office, the financial penalty will be lower to reflect the relatively low severity of the non-compliance. For example, as a CIO failing to submit the computer system security management plan on time may subsequently submit it as a remedy, the maximum financial penalty in this case is HK$500,000. On the contrary, failure to report a computer system security incident to the Commissioner's Office within the specified time frame may lead to delay in tackling the incident, which may have serious implications on the security of the CI's computer systems or even Hong Kong as a whole. In this case, the maximum financial penalty is HK$5 million. The offences and their proposed penalties for non-compliance with the obligations of CIOs mentioned in paragraph 24 above and non-compliance with the directions of Commissioner's Office are set out in **Annex I**.

36. We understand that some CCSs may be owned or controlled by third-party service providers. To ensure that these CCSs do not become loopholes in computer system security, CIOs are obligated to ensure that the third-party service

providers have implemented security measures for the CCS under their control (see item II(h) in paragraph 24 above). If the inadequate action on the part of a third-party service provider leads to non-compliance with the statutory obligations, the CIO will still be held responsible for the non-compliance.

H. Investigation Powers of the Commissioner's Office

37. All the jurisdictions listed in paragraph 5 above are empowered to question, request information, enter premises, access and check the relevant computer systems, etc. We propose to empower the Commissioner's Office to exercise various investigation powers, including to investigate the offences under the proposed legislation so that the Commissioner's Office is able to investigate computer system security incidents to help the CIOs respond to the incidents and recover the CCSs, and to follow up on non-compliance.

38. Each of these powers is regulated in terms of specific conditions, officers that can exercise the powers and authorising authority (including whether magistrate's warrants are needed), etc., to ensure that these investigation powers are kept to the minimum extent necessary.

I. <u>Power to respond to security incidents</u>

39. Although generally speaking, CIOs should bear the overall responsibility for responding to computer system security incidents, with reference to the relevant laws of Australia, the UK and the EU, we propose to empower the Commissioner's Office to investigate an incident for the purpose of assessing its impact, reducing consequential harm, and preventing a further incident from arising. In this regard, the Commissioner's Office may request a CIO to answer questions and submit information on the incident after its occurrence. If the CIO is found unwilling or unable to respond to the incident, the Commissioner's Office may request the CIO to take remedial measures and may enter the relevant premises for investigation with the consent of the CIO. In more serious cases, the Commissioner's Office may, in the public interest, apply for a magistrate's warrant in order to require a person other than the CIO who appears to control the CCS to assist in the investigation. As for CIOs regulated by designated authorities, as mentioned in paragraph 30 above, when reporting an incident to the designated authorities, they must also report to the Commissioner's

Office so as to address the incident together with CSTCB of the HKPF and provide assistance after the incident.

II. Power to investigate the offences under the legislation

40. The Commissioner's Office is empowered to investigate offences under the proposed legislation (e.g. non-compliance with the statutory obligations by operators), including powers to question, request information, and enter premises for investigation with a magistrate's warrant. The proposed legislation will set out clearly the conditions and procedures for exercising these powers (e.g. notification period).

41. Salient points of these powers (including conditions and authorising authority) are set out in **Annex II**.

I. Appeal Mechanism

42. In actual operation, the Commissioner's Office will maintain close co-operation and communication with the organisations that are likely to be designated, with a view to reaching a consensus on the designation of CIO or CCS. Nevertheless, it cannot be ruled out that an operator may object to certain designations made by the Commissioner's Office. In addition, the Commissioner's Office may, by its power under the proposed legislation, issue written directions to designated CIO, requiring it to take further steps to fulfil the statutory requirements. Drawing reference from the practice in the UK, we **propose** that the proposed legislation should provide for an appeal mechanism by the establishment of an appeal board. This allows an operator, who disagrees with a designation of CIO or CCS, or a written direction issued by the Commissioner's Office, an independent avenue of appeal.

43. Members of the appeal board should include computer and information security professionals and legal professionals, etc., to ensure that there is balanced and independent third-party advice in considering an appeal. The board may decide to affirm, reverse or vary a decision. The procedures will be set out in detail in the proposed legislation. As for other decisions made by the Commissioner's Office, such as prosecution of a CIO for violation of a statutory requirement, they will be dealt with in judicial proceedings if the CIO feels aggrieved.

J. Subsidiary legislation

44. Apart from the principal legislation, as there are certain details relating to the powers of the Commissioner's Office or the statutory obligations of the CIOs that may need to be supplemented, updated or amended in future, we **propose** that the proposed legislation should empower the Secretary for Security to specify or amend by way of subsidiary legislation in respect of the following matters:

(a) the type of essential services sectors that may be designated as CI;

(b) list of designated authorities;

(c) information that may be required by the Commissioner's Office from a CIO;

(d) the type of material changes to CCSs that is required to be reported to the Commissioner's Office;

(e) the scopes of, and the manner for the carrying out of, computer system security management plan s and computer system security audits;

(f) the scopes of the computer security risk assessments and emergency response plans;

(g) the type of computer system security incidents that is required to be reported to the Commissioner's Office ; and

(h) deadlines for reporting, etc.

K. CoP

45. In view of the rapid advancement in technology, detailed operational practices may need to be updated from time to time. We **propose** that the proposed legislation should empower the Commissioner's Office to issue a CoP setting out the proposed standards based on statutory requirements, so as to provide the Commissioner's Office with greater flexibility in updating the guidelines in a timely manner taking into account the latest technology and

international standards, thereby assisting the CIOs in meeting the statutory requirements. The Commissioner's Office will also communicate with the CIOs of different sectors and include sector-specific guidelines in the CoP where necessary.

46. For example, the proposed legislation will require the CIOs to conduct computer system security audits on a regular basis, and the CoP will set out the relevant professional qualifications that an independent computer system security auditor should possess, the scope of the audit, the internationally recognised methodology and standards that can be referred to, and the details of the report and rectification plan. Other jurisdictions (e.g. the EU) have similar practice of including recommended compliance standards in guidelines outside the legislation. The scope of the CoP is at **Annex III**. Similarly, designated authorities may also issue relevant guidelines for the institutions they regulate.

47. The CoP is not a piece of subsidiary legislation and failure to comply with the provisions of the CoP by a CIO does not constitute an offence. However, where a suspected breach of the statutory obligations is detected, compliance with the recommended standards in the CoP may be a strong evidence supporting that there has been no breach of the statutory obligations. Nonetheless, as long as the objectives of the statutory obligations are met, it is open for CIOs to fulfill the statutory obligations by ways other than those set out in the CoP.

L. Summary of the proposals

48. The proposals set out in items B to K above are summarised at **Annex IV** for ease of reference.

VIEWS OF STAKEHOLDERS

49. Since 2023, we have organised more than 15 consultation sessions for over 110 stakeholders (including organisations that may be designated as CIOs, cybersecurity service providers and audit companies, sector regulators, etc.) to solicit their views on the preliminary proposed framework of the legislation. The stakeholders unanimously agreed that it is the responsibility of all sectors of

the community to safeguard the security of computer systems and supported the legislation in principle. The majority of the representatives of the infrastructure operators also indicated that their organisations have already implemented certain security measures for their computer systems. The major concerns of the stakeholders and our responses are as follows:

(a) Compliance costs - There have been comments that some sectors already have similar computer security requirements in place. Duplication of efforts in fulfilling requirements imposed by different authorities will further increase compliance costs. As such, we **propose** to designate authorities to oversee compliance by CIOs in respect of organisational and preventive obligations (see paragraph 26 above);

(b) Difficulties in hiring competent computer security personnel as supervisor - There are comments that due to the shortage of relevant talents, it may be difficult to hire a qualified supervisor for the computer system security management unit. In this regard, we have appropriately revised the relevant requirements, which CIOs only need to establish a computer system management unit with professional knowledge (see paragraph 24I(c) above). They may also choose to hire relevant personnel from third-party service providers as needed. Yet, services must be supervised by a dedicated supervisor of the CIO. Apart from that, we **propose** that the requirements concerning the supervisor of the computer system security management unit be incorporated into the CoP only as a recommended standard, so as to provide CIOs with greater flexibility in hiring a suitable candidate;

(c) Time frame for reporting incidents - Taking into account comments that it takes time for CIOs to confirm an incident upon its occurrence, we **propose** to define more clearly the time requirement for reporting a computer system security incident by specifying in the proposed legislation that the time frame for reporting[2] shall be reckoned as from the time when a CIO becomes aware of [3] a security incident in relation

---

[2] Serious incidents: Within 2 hours upon becoming aware of such incidents; other incidents: within 24 hours upon becoming aware of these incident.

[3] "Become aware of" means having a reasonable degree of certainty that a cybersecurity event has caused harm to the confidentially, integrity or availability of the CCSs or has compromised their operations. A short period of investigation in order to establish whether or not a cybersecurity incident has occurred may not be regarded as being "aware".

to a CCS (see paragraph 24III(k) above), ensuring that the CIOs have time to conduct a preliminary investigation into whether the incident is indeed a computer system security incident; and

(d) Criminal liability - Some CIOs are concerned about personal criminal liability for breaching the statutory requirements. The legislative intent was not to punish CIOs, the offences and penalties under the proposed legislation will only be applicable to organisations, where heads or staff will not be penalised at the individual level. All offences will be dealt with by financial penalty only. Yet, if the relevant violations involve breach of some existing criminal legislation, such as making false statements, using false instruments or other fraud-related offences, as is the current situation, the officers involved may be held personally criminally responsible.

WAY FORWARD

50. After consulting the Legislative Council (LegCo) Panel on Security on 2 July, we will issue a letter specifically to consult relevant sectors again on the legislative proposals set out in this paper. The consultation period will last for one month. Meanwhile, the SB has started the drafting of the proposed bill with the Department of Justice, the OGCIO and the HKPF. We will consider and adopt the views received in this consultation exercise and plan to introduce the proposed bill into the LegCo for consideration by the end of 2024.

51. Upon the passage of the proposed legislation, the Government aims to set up the Commissioner's Office within one year, after which to bring the proposed legislation into force within half a year's time. By that time, the Commissioner's Office will review the situations of operators in different CI sectors, including their level of readiness and the impact of its services on society, etc., to designate CIOs and CCSs in a progressive and phased manner.

PROTECTING THE PHYSICAL SECURITY OF INFRASTRUCTURES

52. The key of this legislation is to protect the security of the computer systems of CIs. Regarding the physical security of CIs, the Critical

Infrastructure Security Co-ordination Centre of the HKPF is committed to continuously strengthening the protection and resilience of CIs through public-private partnership, risk management, on-site security inspections, etc.

53. In addition, attacks against CIs may, depending on the intention of attackers and the circumstances of offences, constitute offences under existing legislations (e.g. criminal damage (section 60 of the Crimes Ordinance), arson (section 60(3) of the Crimes Ordinance), etc.).

ADVICE SOUGHT

54. Members are invited to comment on the Government's proposed legislative framework for enhancing the protection of computer systems of CIs.

Security Bureau
Office of the Government Chief Information Officer
Hong Kong Police Force
June 2024

Annex I

List of Obligations, Proposed Offences and Penalties of Operators of Critical Infrastructure

A. Obligations of Operators of Critical Infrastructure ("CIOs") and related offences

Obligations of operators		Offences	Penalties
I.	**Organisational**		
(a)	To **provide** to the Commissioner's Office **and maintain address and office in Hong Kong** - The address shall be provided within 30 days of its designation as CIO - Any changes shall be reported within 30 days	Failure to provide address/report changes to the Commissioner's Office within the prescribed time frame without reasonable excuse.	Maximum fine of $500,000 Continuing offence: $50,000/ day
(b)	To report **changes in ownership and operatorship** of their CIs to the Commissioner's Office - Ownership: any changes shall be reported within 30 days - Operatorship: any changes shall be reported at least three months before the date of change	Failure to report the changes to the Commissioner's Office within the prescribed time frame without reasonable excuse.	Maximum fine of $5,000,000 Continuing offence: $100,000/ day

Obligations of operators		Offences	Penalties
(c)	To set up a **computer system security management unit** (in-house or outsourced) with professional knowledge **and be supervised by a dedicated supervisor of the CIO** to ensure that there is a dedicated unit to handle matters relating to computer system security and to follow up on the directions given by the Commissioner's Office (Note: The Code of Practice ("CoP") will set out recommendations on, among other things, the composition of the unit, and the experience and qualifications of its supervisor.)	The Commissioner's Office may issue written direction to a CIO for failure to meet relevant standards. Non-compliance with written directions without reasonable excuse is an offence.	Maximum fine of $5,000,000 Continuing offence: $100,000/day
II. Preventive			
(d)	To **inform** the Commissioner's Office of the **material changes to their critical computer systems ("CCSs")**, including: - The material changes to its design, configuration, security or operation, etc. (Note: The CoP will set out examples of material changes for reference.)	Failure to inform the Commissioner's Office, without reasonable excuse, of a change within 30 days after the change is made.	Maximum fine of $500,000 Continuing offence: $50,000/day

Obligations of operators		Offences	Penalties
(e)	**To formulate and implement a computer system security management plan** - Shall be submitted to the Commissioner's Office within three months of a CIO's designation / within one month of the change. (Note: The CoP will set out the required scope for the computer system security management plan (see **Annex III** for details)).	Failure to submit the plan within the prescribed time frame without reasonable excuse.	Maximum fine of $500,000 Continuing offence: $50,000/day
		The Commissioner's Office may issue written direction to a CIO for failure to meet relevant standards. Non-compliance with written directions without reasonable excuse is an offence.	Maximum fine of $5,000,000 Continuing offence: $100,000/day
(f)	To conduct **computer system security risk assessment** - The assessment shall be conducted at least once every year - The assessment report shall be submitted to the Commissioner's Office within 30 days of the completion of the assessment. - Vulnerability assessment and penetration test should be included. (Note: The CoP will set out the internationally recognised	Failure to submit the report within the prescribed time frame without reasonable excuse.	Maximum fine of $500,000 Continuing offence: $50,000/day
		The Commissioner's Office may issue written direction to a CIO for failure to meet relevant standards. Non-compliance with written directions without reasonable excuse is an offence.	Maximum fine of $5,000,000 Continuing offence: $100,000/day

Obligations of operators		Offences	Penalties
	methodologies and standards that can be referred to.)		
(g)	To conduct **independent computer system security audit** - An audit shall be conducted at least once every two years. - The audit report shall be submitted to the Commissioner's Office within 30 days of the completion of the security audit. - An additional audit shall be conducted as directed by the Commissioner's Office when the audit report is incomplete or non-compliant. (Note: The CoP will set out the recommended professional qualifications that the auditor should possess, the scope of the security audit, internationally recognised methodologies and standards that can be referred to and the details of the report and rectification plan.)	Failure to submit the report within the prescribed time frame without reasonable excuse.	Maximum fine of $500,000 Continuing offence: $50,000/day
		The Commissioner's Office may issue written direction to a CIO for failure to meet relevant standards. Non-compliance with written directions without reasonable excuse is an offence.	Maximum fine of $5,000,000 Continuing offence: $100,000/day

Obligations of operators		Offences	Penalties
(h)	To take measures to ensure that even with the hiring of **third-party service providers, CIO's CCSs still comply with** the relevant statutory **obligations** - Including contractual terms or other measures.	The Commissioner's Office may issue written direction to a CIO for failure to meet relevant standards. Non-compliance with written directions without reasonable excuse is an offence.	Maximum fine of $5,000,000 Continuing offence: $100,000/day
III. Incident reporting and response			
(i)	To participate in **computer system security drills** - At least once every two years. - Organised by the Commissioner's Office. (Note: The CoP will set out examples on the mode and scale of the drills for reference)	Failure to participate in a cybersecurity drill at least once every two years without reasonable excuse.	Maximum fine of $5,000,000
(j)	To formulate an **emergency response plan** for responding to computer system security incidents - The plan shall be submitted within three months of a CIO's	Failure to submit the plan within the prescribed time frame without reasonable excuse.	Maximum fine of $500,000 Continuing offence: $50,000/day

Obligations of operators		Offences	Penalties
	designation to the Commissioner's Office. - Any changes shall be submitted to the Commissioner's Office within one month of the change. (Note: The CoP will set out the scope of the emergency response plan (see **Annex III** for details).	The Commissioner's Office may issue written direction to a CIO for failure to meet relevant standards. Non-compliance with written directions without reasonable excuse is an offence.	Maximum fine of $5,000,000 Continuing offence: $100,000/day
(k)	To report **computer system security incidents** in respect of CCSs to the Commissioner's Office within the prescribed time frame. - Serious computer system security incidents[1]: the initial report shall be made within two hours after becoming aware of the incident. - For other computer system security incidents, the initial report shall be made within 24 hours after	Failure to report security incidents in respect of CCSs within the prescribed time frame without reasonable excuse.	Maximum fine of $5,000,000

[1] A serious incident refers to an incident that has or is about to have a major impact on the continuity of essential services and the normal functions of critical infrastructure, or leads to a large-scale leakage of personal information and other data.

Obligations of operators		Offences	Penalties
	becoming aware of the incident. - If the initial report is made by telephone or text message, a written record shall be submitted within 48 hours after the report has been made. - A written report shall be submitted within 14 days, providing details of the incident such as the cause(s), impact and remedial measures. - The types of incidents to be reported will be prescribed in the legislation[2]. (Note: The format and a sample of the report will be set out in the CoP (see **Annex III** for details).		

[2] These include hacking to gain unauthorised control of a CCS; installation or execution of unauthorised programs of a malicious nature on a CCS; attacks targeting interconnected systems; distributed denial of service attacks; and other incidents that affect the use or operation of a CCS.

B. Powers of obtaining information and investigating of the Commissioner's Office and offences

Powers of the Commissioner's Office		Offences	Penalties
(a)	For the purpose of **ascertaining whether an organisation should be designated as a CIO**, the Commissioner's Office may, by writing, request any organisation controlling a potential critical infrastructure (CI) to submit relevant information - Including the essential services provided by the organisation, the level of dependence on technology, and the consequences and extent of impact on the services in case of disruption or damage of its information system.	Failure to comply, without reasonable excuse, with the direction issued by the Commissioner's Office to submit information.	<u>For designated CI:</u> Maximum fine of $5,000,000 Continuing offence: $100,000/day <u>For infrastructures that is yet to be designated:</u> Maximum fine of $500,000 Continuing offence: $50,000/day
(b)	For the purpose of **ascertaining whether a computer system should be designated as a CCS**, the Commissioner's Office may, by writing, request the CIO to submit relevant information - Including the number, composition, design, service targets and inter-	Failure to comply, without reasonable excuse, with the direction issued by the Commissioner's Office to submit information	Maximum fine of $5,000,000 Continuing offence: $100,000/day

Powers of the Commissioner's Office		Offences	Penalties
	connectivity of the systems.		
(c)	The Commissioner's Office may **investigate a security incident targeting CCSs** for the purpose of assessing its impact, reducing consequential harm, and preventing it from spreading - Powers include questioning, requesting information, requiring CIO to take remedial measures and entering premises for investigation with a magistrate's warrant. (Note: Key points of the powers (including conditions and authorising authority, etc.) are separately set out in **Annex IV**.)	Failure to comply, without reasonable excuse, with the direction issued by the Commissioner's Office in exercising its statutory powers to investigate security incidents targeting CCSs.	Maximum fine of $500,000
(d)	The Commissioner's Office may investigate offences under the legislation - Powers include questioning, requesting information and entering premises for investigation with a magistrate's warrant.	Failure to comply, without reasonable excuse, with the direction issued by the Commissioner's Office in exercising its statutory powers to investigate offences under the legislation.	Maximum fine of $500,000

Powers of the Commissioner's Office		Offences	Penalties
	(Note: Key points of the powers (including conditions and authorising authority, etc.) are separately set out in **Annex IV**.)		

Annex II

Investigation Powers of the Commissioner's Office

I. Power to investigate security incidents against a critical computer system ("CCS")

Situation and Threshold for Exercising power	Authorising authority	Powers	Offence of non-compliance
An incident against a CCS has occurred.	Commissioner's Office	<u>In respect of Operator of Critical Infrastructure ("CIO")</u> • Question the CIO. • Require the CIO to furnish information.	Failure to comply with any order of the Commissioner's Office in exercising its statutory powers to investigate security incidents related to CCSs is an offence, subject to a maximum fine of $500,000. (See <u>Annex I</u>, Item B(c))
• The CIO is unwilling or unable to respond to the incident on its own. • Exercise of power is necessary. • The power is appropriate for and proportionate to the incident.		<u>In respect of CIO</u> • Direct the CIO to take remedial actions. • Direct the CIO to take action to assist in investigation. • With the consent of the CIO, check the CCSs owned/ controlled by the CIO	
• The CIO is unwilling or unable to respond to the incident on its own. • Exercise of power is necessary. • The power is appropriate for and proportionate to the incident. • Exercise of power is conducive to the investigation of	Magistrate's warrant	<u>In respect of CIO</u> • Without the CIO's consent, check the CCSs owned/ controlled by the CIO <u>In respect of CCS not under the control of the CIO</u> (e.g. CCS controlled by a third-party service provider) • Enter premises	

Situation and Threshold for Exercising power	Authorising authority	Powers	Offence of non-compliance
incident. • Exercise of power is in public interest.		where a CCS not under the control of the CIO is located and check the system. • Require any person in control of the CCS to answer questions and furnish documents. • Direct any person in control of the CCS to take remedial actions. • Direct any person in control of the CCS to take action to assist in the investigation. • Connect equipment to or install program in the CCS.	

II. Power to investigate the offences under the legislation

Situation and Threshold for Exercising power	Authorising authority	Powers	Offence of non-compliance
• The Commissioner's Office suspects that an offence under the legislation has occurred.	Commissioner's Office	• Require any person whom the investigation officers believe to have relevant information in his/her custody to furnish such information and answer questions.	Failure to comply with any order of the Commissioner's Office in exercising its statutory powers to investigate an offence under the legislation is an offence, subject to a maximum fine of $500,000. (See Annex I, Item B(c))
• There are reasonable grounds to suspect that there are on the premises documents relevant to the investigation but not furnished upon request of the investigation officers; or • Upon the investigation officers' request to furnish relevant documents, such documents will be concealed, removed, tampered with or destroyed.	Magistrate's warrant	• Enter premises and take possession of any relevant documents.	

Annex III

Summary of Main Content of "Code of Practice" (CoP)

(1) Reporting of material changes to critical computer systems

1. Examples of "material changes" may include platform migration, server virtualisation, application re-design, integration or change in interdependency with external systems or other computer systems, etc.

(2) Independent computer system security audit

1. Relevant professional qualifications that an independent computer system security auditor should possess

2. Scope of the security audit

3. Internationally recognised methodology and standards that can be referred to

4. Details of the independent computer system security audit report and rectification plan

(3) Computer system security risk assessment

1. Scope of the risk assessment, including vulnerability assessment and penetration test

2. Internationally recognised methodology and standards that can be referred to

(4) Computer system security management plan

Key elements to be covered include:

1. organisation, authority, roles and responsibilities of the **computer system security management unit**;

2. appropriate professional qualifications of the **supervisor** of the computer system security management unit;

3. factors that an Operator of Critical Infrastructure ("CIO")should consider in formulating the **policies, standards and guidelines**, such as its own requirements on security, the CoP and relevant requirements set out by statutory bodies for individual sectors;

4. how risks related to the operator and its critical computer system ("CCS") can be identified, assessed, mitigated and monitored while formulating a computer system security risk management framework;

5. establish a **monitoring and detection** mechanism:

    - to define a baseline of normal behavior in the operation of the CCS and monitor anomalies against this baseline;

    - to put in place procedures and processes to respond continuously and in a timely manner to any computer system security incidents received by the monitoring system;

    - to establish mechanisms and processes to continuously collect and analyse information or intelligence relating to information security threats, including attacker methodologies, tools and technologies involved, and appropriate mitigation actions that can be taken;

    - to conduct regular review of the monitoring mechanism (at least once every two years) to ensure that it is still effective with respect to its nature and technology advancement;

6. Computer system security training: take into consideration the roles of all personnel involved in the operation of the CI, including vendors, contractors and service providers, to formulate training programmes on various computer system security approaches;

7. adopt a "Security by Design" approach to ensure that security is an integral part of the CCS across its entire life cycle;

8. implement asset management to ensure that an up-to-date inventory of CCS and other associated assets are properly owned, kept and maintained, and restricted for access on a need-to-know basis;

9. implement access control and account management: only authorised users and computer resources access control system are allowed to access the CCS while enforcing the least privilege principle; conduct review periodically; revoke all user privileges and data access rights that are no longer required; and maintain logs of all accesses and attempted accesses to the CCS;

10. implement privileged access management to ensure that personnel only have access to the specific administrative capabilities needed; regular reviews on usages of privileged accounts should be conducted by an independent party;

11. implement cryptographic key management to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of the information;

12. implement password management by defining a strong password policy;

13. implement physical security to ensure that data centres and computer rooms are located in a comprehensively protected environment;

14. implement system hardening by adopting both the least functionality principle and least privilege principle; the baseline configuration of computer systems should be developed, maintained and reviewed regularly;

15. implement change management: the CIO should plan, monitor and follow up changes to production systems properly, and should back up system files and configurations adequately;

16. implement patch management by adopting a risk-based approach to promptly devise the appropriate patch management strategy for the CCS;

17. develop appropriate policies and procedures for remote connection;

18. develop management policies for portable computing devices and removable storage media;

19. implement backup and recovery policies to ensure the resilience of the system;

20. implement network security control to allow only authorised traffic to enter the network;

21. adopt application security measures such as version control mechanism and separation of environments for development, so as to maintain integrity of an application;

22. implement log management: the CIO should provide sufficient information to support the comprehensive audits of the effectiveness and compliance of security measures;

23. implement cloud computing security to ensure proper protection; the shared responsibility for information security between the cloud service provider and the organisation should be clearly defined and implemented; and

24. implement supply chain management by defining and establishing processes and procedures, through which the confidentiality and non-disclosure agreements are properly managed and reviewed.

(5) Incident response obligations

1. Computer system security drills

- The CIO shall participate in computer system security drills directed by the Commissioner's Office

- The theme and scope of the drills will be set by the Commissioner's Office

2. Appointment of 24/7 contact point

- At least two key officers accountable for the management and operation of the CI should be appointed as contact point to communicate with the Commissioner's Office on matters of computer system security

- The Commissioner's Office should be informed about any changes as soon as possible, and in any event within a period as prescribed under the legislation

3. Scope of the emergency response plan should include but not be limited to:

- structure, roles and responsibilities of the dedicated incident response team;

- threshold for initiating the incident response protocol;

- reporting procedures for ensuring compliance with the incident reporting obligations;

- procedures for mitigating the impact of an incident and preserving evidence;

- procedures for investigating the cause(s) and impact of an incident and for providing relevant information to the designated authority in assisting the investigation;

- recovery plan for the resumption of normal operation of the CI;

- the CIO's communication plan with stakeholders and the general public, including the establishment of structures and modes for communication and coordination;

- post-incident review procedures, including the recommended measures for mitigating the risks and preventing reoccurrence;

- measures to ensure that all relevant personnel are familiar with the emergency response plan;

- a review on its emergency response plan at least once every two years, or when any material changes arise in the operating environment of the CIO.

4. Requirements for reporting computer system security incidents

- Upon becoming aware of[1] a computer system security incident, the CIO shall make timely report to the Commissioner's Office.

  Initial report

  – An initial report can be made by email, telephone or text message. It should cover at least the nature of the incident, the system(s) being affected and the impact.

  – Time frame: for serious computer system security incidents[2]: the report shall be made within two hours after becoming aware of the incident; for other computer system security incidents: the report shall be made within 24 hours after becoming aware of the incident.

  – If the initial report is made by telephone or text message, the CIO shall submit a written report within 48 hours after the initial report has been made.

  Written report

  – The CIO shall submit a written report to the Commissioner's Office using the incident reporting form specified by the Commissioner's Office via a designated channel (e.g. official website) within 14 days after becoming aware of an incident, providing further details of the incident (including the cause(s), impact and remedial measures).

---

1 "Become aware of" means having a reasonable degree of certainty that a computer systems security event has caused harm to the confidentially, integrity or availability of the CCS or has compromised their operations. A short period of investigation in order to establish whether or not an incident has occurred may not be regarded as being "aware".

2 A serious incident refers to an incident that has or is about to have a significant impact on the continuity of essential services and the normal functions of CIs, or leads to a large-scale leakage of personal information and other data.

- The CIO should provide updates on the reported incident to the Commissioner's Office upon request or within the time frame specified by the Commissioner's Office.

- The CIO should also ensure that the relevant evidence is preserved and a proper investigation is conducted to identify the cause(s) of the incident, assess the impact or potential impact, and formulate security measures to prevent reoccurrence.

Note: This overview of the key elements of the Code of Practice is generally applicable to all CIOs, except for those regulated by designated authorities. Designated Authorities may issue relevant guidelines for the CIOs under their regulation.

— End —

Annex IV

Main Recommendations on the Proposed Legislation

Recommendations	
B. Scope of regulation	
1.	Only expressly designated Operators of Critical Infrastructure ("CIO") and critical computer systems ("CCS") will be regulated.
2.	Critical Infrastructure ("CI") covers two major categories as follows:: Category 1: Infrastructures for delivering essential services in Hong Kong, covering the following eight sectors: (a) Energy; (b) Information Technology; (c) Banking and Financial Services; (d) Land Transport; (e) Air Transport; (f) Maritime; (g) Healthcare Services; and (h) Communications and Broadcasting. Category 2: Other infrastructures for maintaining important societal and economic activities
C. Targets of regulation	
3.	An "organisation-based" approach will be adopted, i.e., using the organisation responsible for operating a CI as a basis in fulfilling its obligation to safeguard the security of its computer systems.
4.	In deciding whether an infrastructure is a CI that needs to be regulated under the proposed legislation, the Commissioner's Office should take into account the following factors – (a) the implications on essential services and important societal and economic activities in Hong Kong if there was damage, loss of functionality, or data leakage in such infrastructures; (b) the level of dependence on information technology of the infrastructures concerned; and (c) the importance of the data controlled by the infrastructures concerned.
5.	Only the names of the eight essential services sectors will be set out. The list of individual CIOs will not be disclosed.

Recommendations	
6.	The existing administrative regulatory approach of Government departments will continue. They need not be incorporated into the proposed legislation
7.	CCS: computer systems that are relevant to the provision of essential service or the core functions of computer systems, and those systems which, if interrupted or damaged, will seriously impact the normal functioning of the CIs.
D. Obligations of the CIOs	
8.	Statutory obligations imposed on CIOs are classified into three categories: (I) structural; (II) preventive; and (III) incident reporting and response: **(I) Organisational** (a) provide and maintain address and office in Hong Kong (and report any subsequent changes); (b) report any changes in the ownership and operatorship of their CI to the Commissioner's Office; (c) set up a computer system security management unit, supervised by a dedicated supervisor of the CIO; **(II) Preventive** (d) inform the Commissioner's Office of material changes to their CCS, including those changes to design, configuration, security, operation, etc.; (e) formulate and implement a computer system security management plan and submit the plan to the Commissioner's Office; (f) conduct a computer system security risk assessment (at least once every year) and submit the report; (g) conduct a computer system security audit (at least once every two years) and submit the report; (h) adopt measures to ensure that their CCSs still comply with the relevant statutory obligations even when third party services providers are employed; and **(III) Incident reporting and response** (i) participate in a computer system security drill organised by the Commissioner's Office (at least once every two years);

Recommendations	
	(j) formulate an emergency response plan and submit the plan; (k) notify the Commissioner's Office of the occurrence of computer system security incidents in respect of CCS within a specified time frame: – Serious computer system security incidents: report shall be made within 2 hours after becoming aware of the incident; – Other computer system security incidents: report shall be made within 24 hours after becoming aware of the incident. Upon request by the Commissioner's Office in the course of investigating an incident or offence related to obligation categories (I) to (III) above, CIOs must submit relevant information available to them, even if such information is located outside Hong Kong.
E. Commissioner's Office	
9.	A Commissioner's Office will be set up under the Security Bureau. The proposed legislation empowers the Chief Executive to appoint a Commissioner to lead the office in performing the work under the proposed legislation, including: (a) designating CIOs and CCSs; (b) establishing "Code of Practice" ("CoP") and giving advice on the measures to be adopted by CIOs; (c) monitoring computer system security threats against CCSs; (d) assisting CIOs in responding to computer system security incidents; (e) investigating and following up on non-compliance of CIOs; (f) coordinating with various government departments, e.g. the OGCIO, the Cyber Security and Technology Crime Bureau (CSTCB) of the Hong Kong Police Force (HKPF) and the Hong Kong Computer Emergency Response Team Coordination Centre, etc., in formulating policies and guidelines and handling incidents; and (g) issuing written instructions to CIOs to plug potential security loopholes.
10.	To designate certain sector regulators as designated authorities to monitor the discharging of organisational and preventive obligations by these essential services sectors. The Commissioner's Office will takes full charge of monitoring the CIOs of all the eight sectors in

Recommendations	
	compliance of the obligations of incident reporting and response (except with certain exemptions by the Commissioner's Office).
11.	At this stage, the following designations are proposed: (a) the Monetary Authority as the authority responsible for regulating some service providers in the banking and financial services sector; and (b) the Communications Authority as the authority responsible for regulating some service providers in the communications and broadcasting sector.
12.	The Commissioner's Office retains the power to issue written directions to all CIOs under the proposed legislation, irrespective of whether or not the CIO is under the supervision of a designated authority.
F. Offences and penalties	
13.	Proposed offences include— (a) CIOs' non-compliance with statutory obligations; (b) CIO's non-compliance with written directions issued by the Commissioner's Office; (c) non-compliance with requests of the Commissioner's Office under the statutory power of investigation; and (d) non-compliance with requests of the Commissioner's Office to provide relevant information relating to a CI. Commission of any of the above acts without reasonable excuse shall constitute an offence and may be prosecuted.
14.	The offences and penalties under the proposed legislation will only be applicable to organisations. Their heads or staff will not be penalised at the individual level. However, if the relevant violations touch upon existing criminal legislation, as is the current situation, the personnel involved may be held personally criminally liable.
15.	The penalties will include fines only. The level of fines will be determined by court trials, with maximum fines ranging from HK$500,000 to HK$5 million. For certain offences, additional daily fines for persistent non-compliance will be imposed.

Recommendations	
G. Investigation powers of the Commissioner's Office	
16.	The Commissioner's Office will be empowered to exercise various investigation powers, including: (1) powers to respond to security incidents; and (2) powers to investigate the offences under the legislation.
I. Appeal mechanism	
17.	An appeal board will be established to allow CIOs to appeal against a designation of CIO or CCS, or a written direction issued by the Commissioner's Office.
J. Subsidiary legislation	
18.	The Secretary for Security is empowered to specify or amend by way of subsidiary legislation in respect of certain details relating to the powers of the Commissioner's Office or the statutory obligations of CIOs, for example: (a) the type of essential services sectors that may be designated as CI; (b) list of designated authorities; (c) information that may be required by the Commissioner's Office from a CIO; (d) the type of material changes to CCSs that is required to be reported to the Commissioner's Office; (e) the scopes of, and the manner for the carrying out of, computer system security management plan s and computer system security audits; (f) the scopes of the computer security risk assessments and emergency response plans; (g) the type of computer system security incidents that is required to be reported to the Commissioner's Office ; and (h) deadlines for reporting, etc.
K. Code of Practice	
19.	The Commissioner's Office will be empowered to issue a CoP, which is not subsidiary legislation in nature. It will set out the proposed standards based on statutory requirements, such as the relevant professional qualifications that an independent computer system security auditor should possess, the scope of the audit, the internationally recognised methodologies and standards that can be

Recommendations	
	referred to, and the details of the report and rectification plan. Designated authorities may also issue relevant guidelines for the institutions they regulate.

Annex II

Proposed Legislative Framework to Enhance Protection of the Computer Systems of Critical Infrastructures
Overview and Remarks of Written Submissions

A. Legislative Purpose and Principles

No.	Comments and Remarks
1	Regarding **the overall position**, we received 52 items of submissions in support of the Government's legislation for protecting Hong Kong's critical infrastructures (CIs), and positive suggestions to improve the contents of the proposed legislation. It was agreed that CI Operators (CIOs) should assume and fulfil their statutory obligations. Practical recommendations were also made from the perspectives of information security and CIOs, which enable CIOs to meet the objective of enhancing CI computer security in a smooth manner.
2	Regarding the legislative principles, it is mentioned in paragraph 11(c) of the discussion paper that the proposed legislation "will only require CIOs to bear the responsibility for securing their Critical Computer Systems (CCSs), and in no way will it involve the personal data and business information therein". There were views that the principle may contradict the requirement mentioned in paragraph 24(k), i.e. CIOs shall report "incidents that lead to a large-scale leakage of personal information and other data" (5 submissions). [**Remarks:** We thank sectoral stakeholders for their valuable views and professional suggestions, all of which will be given careful consideration. The Government will continue to maintain communication with stakeholders in various sectors to improve the legislative framework and the content of the Code of Practice (CoP) in an ongoing manner.]

B. Scope of Regulation

No.	Comments and Remarks
1	Regarding **the information technology (IT) sector**, there were views that the definition is too broad (5 submissions). Some suggested abolishing the sector (3 submissions), while some suggested expressly stating the areas not covered in the scope of regulation (2 submissions).
2	Regarding **the second category of CIs (i.e. other infrastructures for maintaining important societal and economic activities)**, there were views

No.	Comments and Remarks
	that its definition needs to be clarified further (5 submissions). Some took the view that venues are only the supporting facilities for event organisers and so they should not be defined as CIs (1 submission). There was an enquiry concerning what type of computer system within the park area will fit the definition of CCS (1 submission), while there was also a suggestion that the category be abolished (1 submission).
3	There were suggestions for expanding the scope of the legislation to include **other sectors**: (a) the scope of CIOs should be expanded to include tertiary education and research institutions (2 submissions), emergency services (1 submission), fresh water supply (1 submission), sewage and waste treatment (1 submission), food manufacturing such as slaughtering (1 submission) and public key infrastructure (1 submission); and (b) government organisations (such as Water Supplies Department) should be included (3 submissions), of which one suggested specifying whether organisations with government participation or representatives are included (1 submission).
4	Regarding **extraterritorial jurisdiction**, there were views that the proposed legislation should only be applicable to CIOs in Hong Kong (2 submissions). [**Remarks:** Drawing reference from relevant legislation of other jurisdictions (including the United States (US), Australia, Singapore and the Mainland), the Security Bureau (SB) considers it appropriate to categorise IT as one of the CI sectors. As for whether an individual organisation and its operator should fall into the IT sector, SB will, before making a decision based on the definition, maintain close communication with the potential operators to be designated. The proposed legislation does not have extraterritorial effect. The Commissioner's Office will ensure that it will only request information that is accessible by operators with offices set up in Hong Kong, and will allow them reasonable time for preparation.]

C. Targets of Regulation

No.	Comments and Remarks
1	Regarding **CIO**: (a) it was suggested that there should be clearer definitions for "CI" and "essential services", as well as conditions of designating "CIOs" (11 submissions); (b) there were enquiries as to whether data centres, cloud service providers and financial services not regulated by the Hong Kong Monetary Authority (HKMA) fit the definition of "essential services" (5 submissions); (c) there were concerns over the confidentiality of CIOs' identities or the consequences of disclosing one's identity as a CIO (5 submissions). There were also views that CIOs should be allowed to disclose their identities to one another so as to foster experience exchange (2 submissions); (d) it was suggested that CIOs should register with a recognised domain name service provider under the domain name ".hk" (1 submission); and (e) it was suggested that the English abbreviation "CIO" for Critical Infrastructure Operator should be changed to avoid confusion with Chief Information Officer (1 submission).
2	Regarding **CCS**: (a) it was suggested that the definitions of CCS and the conditions for designating CCS should be more clearly elaborated on (18 submissions); (b) there were enquiries concerning whether CCS covers operational technology (OT), which includes supervisory control and data acquisition, programmable logic controller (e.g. traffic light system), Internet-of-Things and island system, i.e. system isolated from the Internet (7 submissions); (c) it was considered that with fail-safe features or business continuity planning, normal business operation can be ensured even in case of system failure. Thus, such systems should not be designated as CCSs (1 submission); and (d) there was an enquiry concerning whether services such as Microsoft 365 and Amazon Web Services as well as computer facilities connected to a CCS from outside the territory will be designated (1 submission).
3	**Regarding how "interconnected" is defined:**

No.	Comments and Remarks
	there were enquiries as to whether "interconnected" includes interconnected systems such as security information and event management (SIEM), middleware (such as web servers and database connectors) and loading application software (such as Microsoft Active Directory and Office 365), the disruption to the services of which may affect the provision of services by the CCS (8 submissions).
4	It was suggested that the phrase "**seriously impact**" should be more clearly defined (5 submissions).
5	Regarding **conditions for designation**, nine items of enquiries or suggestions were received as follows: (a) suggesting that in considering the designation of a CIO, whether its computer system fits the relevant definition and threshold of a CCS should be considered in tandem. A CCS should not be designated only after the designation of a CIO (2 submissions); (b) suggesting that potential CIOs should be involved in deciding whether to be designated or not (1 submission); enquiring whether an operator's consent will be sought before designation (1 submission) and the mechanism of handling an operator's objection to the designation (1 submission); (c) suggesting that the principle of phased designation and hierarchical management of CIOs at various levels should be adopted (1 submission); (d) enquiring whether all the subsidiary companies will be subject to statutory obligations if the parent company is designated (1 submission), and whether the parent company of an organisation that is designated will be automatically designated and subject to statutory obligations (1 submission); and (e) enquiring whether the physical security of CIs, other than the designated computer systems, will be brought under regulation (1 submission). [**Remarks:** CIOs and CCSs will be designated on a definition basis. The Commissioner's Office will, through mutual communication and understanding with the operators and with due consideration given to other relevant factors, determine whether a designation is suitable. We have defined CCS under the proposed legislation after taking into account the situation of Hong Kong and drawing reference from the relevant legislation in other jurisdictions. We consider such definition appropriate. The Commissioner's Office will, based on the definition, only designate a computer system necessary for the

No.	Comments and Remarks
	operator's provision of essential services as a CCS after adequate communication with the operator and thorough consideration. However, as "interconnected" may not accurately reflect the factors of consideration in designating a CCS, SB will seriously consider deleting the term.]

D. Obligations of the CIOs

I. *Organisational*

No.	Comments and Remarks
1	Regarding **ownership**, some suggested cancelling the requirement on reporting changes (2 submissions). There were also enquiries about the definition of "change in ownership" (1 submission) and about whether consideration will be given to restricting an owner's nationality from the perspective of national security (1 submission).
2	Regarding **operatorship**, there were enquiries about the definition of "change in operatorship" (3 submissions) and ways to deal with changes that take place in less than three months (2 submissions).
3	Regarding **reporting**, it was suggested that reporting should only be required when the change in operatorship may bring about unfavourable consequences (2 submissions), and that the scope of reporting should be limited to known changes (1 submission).
4	Regarding **computer system security management unit**, we received the following suggestions or enquiries: (a) suggestions for stating the minimum requirements of academic qualifications and experience of eligible supervisors and personnel, and for providing a list of recognised professional qualifications (6 submissions); (b) suggestion from the IT industry that personnel of the management unit should possess higher qualifications and richer experience (4 submissions), whereas potential CIOs, having regard to talent shortage, suggested setting only a minimum standard for such requirements, or classifying qualifications of personnel as non-obligatory standards (3 submissions); (c) suggestions / enquiries about doubling of duties of the management unit by the organisation's IT staff (4 submissions); (d) enquiries about whether the duties can be outsourced to a third-party service

No.	Comments and Remarks
	provider or doubled by a relevant unit in the parent company, and whether the personnel of the unit have to be posted in Hong Kong (3 submissions); (e) enquiry about whether background checks on the unit's personnel are required (1 submission); (f) enquiry about whether a change in supervisor needs to be reported (1 submission); (g) suggestion that the post of supervisor shall be taken up by a qualified subject matter expert (1 submission); and (h) enquiry about whether Singapore's practice, i.e. compiling and maintaining a list of qualified professional IT personnel, will be adopted (1 submission). [**Remarks:** SB understands the practical difficulties that the operators may encounter in reporting the changes in ownership and will seriously consider removing such requirement. The proposed legislation will not stipulate the statutory qualification requirements of computer system security personnel to be appointed by the operators. In drawing up the CoP, SB will compile a detailed list of eligible professional qualifications to facilitate the operators' appointment of suitable personnel.]

II. *<u>Preventive</u>*

No.	Comments and Remarks
1	Regarding **reporting changes in CCSs**, the following comments or enquiries were received: (a) suggesting that the scope of "material changes" in the relevant system, technology, configuration or updated security settings to be reported should be clearly stated (9 submissions); (b) considering that the conditions and scope to be reported were unclear (2 submissions); suggesting that reporting should only be required when the material changes to the CCS may have a negative impact (4 submissions); (c) suggesting that the reporting methodology (1 submission), frequency (1 submission), and the requirements during the first, second and subsequent years of reporting (1 submission) should be stated, and that a sample report

No.	Comments and Remarks
	should be provided (1 submission); (d) suggesting that the CoP should set out the categorisation of CCSs and the communication mechanism with the Commissioner's Office (e.g. whether a new system will fall under the definition of CCS) (1 submission); (e) suggesting allowing greater flexibility in reporting and the time frames for submitting reports (2 submissions); (f) enquiring whether prior consent is required before making changes to a CCS, and whether the system needs to be recovered if consent is not granted (1 submission); (g) enquiring whether reporting on the part of the CIO is required during and upon completion of the rectification of a non-compliance incident, and whether a follow-up audit needs to be conducted (1 submission); (h) suggesting that changes to a CCS be recorded in detail, so as to ensure transparency and accountability (1 submission); and (i) expressing concern about the possible disclosure of commercial secrets if changes to CCSs are reported (1 submission).
2	Regarding **the disclosure of information**, 11 items of suggestions or enquiries were received as follows: (a) suggesting that only general information should be disclosed, while operational secrets should be excluded (2 submissions); (b) considering it inappropriate to disclose information on the design, configuration and operation of CCSs (2 submissions); (c) suggesting that unless a serious incident is involved, sensitive information (e.g. brand, software version, IP address) should be concealed in the disclosure (1 submission); (d) suggesting disclosing only minimum information on a need-to-know basis (1 submission); (e) enquiring what sensitive information relating to a CCS will be collected (1 submission); (f) suggesting that provision of information relating to national security, personal privacy and commercial secrets should be expressly exempted (2

No.	Comments and Remarks
	submissions); (g) enquiring whether there are, in the course of investigation of an incident by the Commissioner's Office, requirements on protection of the CCS and its sensitive operational information (1 submission); and (h) suggesting that stringent regulation be exercised and clear guidelines be provided for cross-boundary flow of information (1 submission).
3	As regards the **computer system security management plan**, the following comments or enquiries were received: (a) making enquiries / suggestions about adopting the standards of international standards organisations such as the International Organization for Standardization and the International Electrotechnical Commission (e.g. ISO 27001, IEC 62443) (4 submissions); (b) enquiring about the need / frequency for regular review of the plan (2 submissions) and whether the review can be covered by the parent company (1 submission); (c) suggesting providing a practical guide for the protection of CIs (1 submission); (d) suggesting that the scope of the plan should take into account such factors as risk priorities, sufficient budget allocation, phased upgrades and collaboration with manufacturers (1 submission); (e) suggesting that the following be clearly stated: the scope of the management plan (1 submission), requirement to report changes in the management plan within a specified time frame (1 submission), retention period of login records (1 submission), definition of "a baseline of normal behavior in the operation of the CCS" (1 submission), whether requirements for confidentiality and management of non-disclosure agreement will be imposed (1 submission), and whether attack surface management (i.e. real-time continuous discovery of potential attack surfaces) is covered (1 submission); (f) suggesting that legacy or isolated Internet systems should not be subject to continuous monitoring (1 submission); and (g) suggesting enhancing the baseline requirements as follows: - implement state-of-the-art cybersecurity technologies, such as advanced

No.	Comments and Remarks
	encryption and artificial intelligence (AI)-based threat detection systems (1 submission); - implement asset management to ensure an up-to-date inventory of CCSs (1 submission); - introduce intelligence-led "purple team" (both offensive and defensive teams) (1 submission); and - use a secure private cloud or hybrid cloud solution to store and manage critical data and services (1 submission).
4	As regards **risk assessment**, the following comments or enquiries were received: (a) suggesting that a risk-based approach be adopted in conducting assessment and formulating security controls, audits and tests (4 submissions). (b) suggesting setting the scope in accordance with international standards and frameworks (2 submissions), and clearly specifying the scope and criteria to cover critical areas, including the challenges of penetration test on OT (1 submission), whether third party service providers are covered (1 submission), whether only CCSs are targeted (1 submission) and whether internal and external risks are covered according to sectors (1 submission); and providing guidelines and samples (1 submission). (c) suggesting accepting assessments conducted by internal audit department of the organisation (1 submission), accepting the existing certification and reports issued by independent third parties (2 submissions), consolidating risk assessments and audits (2 submissions), aligning with the HKMA's Cyber Resilience Assessment Framework (C-RAF) and reducing the assessment frequency to once every two years (1 submission). (d) enquiring whether an organisation that conducts risk assessments more than the required frequency (i.e., once a year) needs to submit a report after each of its risk assessments (1 submission); and (e) enquiring whether vulnerability assessment and penetration test are required after material changes of the CCS have arisen. (1 submission).
5	Regarding **security audit**, 12 items of enquiries or suggestions were received: (a) suggesting specifying the qualifications of audit staff (2 submissions), which

No.	Comments and Remarks
	should be on par with the current regulatory framework (1 submission); (b) suggesting specifying the independence of audit staff (i.e. whether to accept audits conducted by the organisation's internal audit staff or by subject matter experts) (2 submissions), and accepting the audits on privileged access management conducted by an organisation's internal audit staff (2 submissions); (c) suggesting that CIOs and the industries must adopt consistent standards and qualities, e.g. the Baseline IT Security Policy, IT Security Guidelines (G3), Council of Registered Ethical Security Testers, MITRE Adversarial Tactics, Techniques and Common Knowledge framework (MITRE ATT&CK), ISO 27001 and Service Organization Control Type 2 (1 submission); (d) suggesting specifying whether risk assessment forms part of the audit (1 submission), and whether the audit focuses on testing the effectiveness of controls or identifying and assessing inherent risks (1 submission); (e) suggesting that CIOs should owe a duty to understand their unique security weaknesses rather than merely following the guidelines provided by regulatory authorities or audit staff (1 submission); (f) suggesting defining "audit completion" (there was always a time lag between the completion of audit field work and the signing and issuance of audit report) (1 submission); (g) enquiring whether the report compiled in the year of independent audit can be used for complying with the requirement for annual assessment (1 submission); (h) suggesting increasing the frequency of audits to once a year (1 submission); and (i) enquiring whether an audit can be exempted if supported by justifications (1 submission).
6	Regarding **enhancement of baseline requirements**, below enquiries or suggestions were received: (a) suggesting that forward-looking cybersecurity strategies, including risk scoring, risk priority and risk exposure analysis, be formulated (1 submission);

No.	Comments and Remarks
	(b) suggesting monitoring the risks continuously (1 submission); (c) suggesting encouraging or mandating the use of red teams (attack teams) (1 submission); (d) suggesting conducting intelligence-led cyberattack simulation test (1 submission); (e) suggesting placing importance on CIOs' resilience from incidents (1 submission); (f) suggesting considering sanctions risks (1 submission); (g) suggesting introducing AI elements (1 submission); (h) suggesting considering 24×7 brand reputation protection (1 submission); (i) suggesting encouraging CIOs and suppliers to assist in managing and reducing cyber risks (1 submission); (j) suggesting adopting the MITRE ATT&CK framework to better address known risks (1 submission); (k) suggesting considering the use of cloud backup instead of off-site tape backup (1 submission); (l) enquiring whether it is necessary to establish an all-weather security operation centre (SoC) with the adoption of an endpoint detection and response system (1 submission) to provide all-weather monitoring of cyber risk intelligence of the dark web (1 submission); and (m) enquiring whether, in respect of risk assessment, the risks identified will be graded according to their seriousness; if so, whether time frames should be set for recovery according to the grades (1 submission). [**Remarks:** The proposed legislation is not targeted at the personal data or commercial confidential information in the CIOs' computer systems. The aim of requiring operators to provide information is to ensure that the operators properly fulfil their obligations in protecting their CCSs, and to enable the Commissioner's Office to, when a CCS incident arises, effectively assess the severity of the incident to the society and the threats to other operators. In carrying out its functions under the proposed legislation.

No.	Comments and Remarks
	Therefore, the Commissioner's Office will request CIOs to provide the necessary information in accordance with the legislation. We consider independence one of the fundamental principles of audits. Thus, the auditing parties should be independent of the audited parties to avoid conflicts of interest and to ensure the impartiality and objectivity of audits. The Commissioner's Office will set out in detail the qualification requirements for audit staff in the CoP by making reference to internationally recognised standards and relevant professional qualifications.]

III. *<u>Incident Reporting and Response</u>*

No.	Comments and Remarks
1	As regards **security drills**, 12 items of enquiries or suggestions were received: (a) making suggestions or enquiries about setting minimum requirements or scales to minimise the need for service disruption, for example, accepting regular drills conducted by CIOs if the scales of such drills are similar to the required scale (4 submissions), allowing drills conducted by CIOs or designated authorities (2 submissions) and exempting OT systems from conducting mobile scanning or penetration test (2 submissions); (b) suggesting that a risk-based approach be adopted in conducting drills (2 submissions); (c) enquiring whether the drill is based on a white-box test (test performed with full knowledge of the system's internal implementation and design) or a black-box test (a test performed based on actual cyberattacks, without prior knowledge of the system's internal implementation) (1 submission); and (d) enquiring whether simulated scenario tests based on the threat profile of the CIO will be conducted above the baseline (1 submission).
2	**As regards the definition of "serious incident"**, it was suggested in 11 items of submissions that the definition of "serious incidents" should be more clearly elaborated on, or an assessment matrix should be provided for reference.

No.	Comments and Remarks
3	As regards the definition of **"other incidents required to be reported"**, the following suggestions or enquires were received: (a) suggesting further refining the definition of "other incidents required to be reported", for example making clear whether the following incidents needs to be reported: incidents caused by system errors, human errors, power outages, etc., which are not cyberattack-related; data leakage incidents that do not involve disruption of essential services; and incidents considered by the CIO to be at a manageable risk level (17 submissions); (b) suggesting that data leakage incidents that do not affect system security and the provision of essential services need not be reported (1 submission); (c) enquiring about the circumstances under which CIOs are required to report data leakage, e.g. the quantity of data and whether the leakage is from CCSs (1 submission); and (d) enquiring about the circumstances when the source of data leakage is non-CCS (while the data is from the CCS) (1 submission).
4	As regards the definition of **"become aware of"/"short period of investigation"**, the following comments were received: there was a need to further refine the definition of "become aware of" and "short period of investigation", so as to prevent over-reporting due to failure to ascertain the cause of an incident within the statutory time frame (8 submissions).
5	As regards the **emergency response plan**, 2 items of enquiries were received: (a) whether digital forensics and investigation need to be conducted by the CIO's subject matter experts (1 submission); and (b) the assistance to be provided by the Commissioner's Office in case of an incident, which may be included in the emergency response plan (1 submission).
6	As regards the time frame for **incident reporting**, the following comments or enquiries were received: (a) considering that the time frame of reporting a serious incident within 2 hours after becoming aware of it is too tight (8 submissions), and suggesting extending it to 24 hours (1 submission); (b) considering that the time frame of reporting other incidents within 24 hours

No.	Comments and Remarks
	after becoming aware of them is too tight (2 submissions), and suggesting extending it to 72 hours (3 submissions); (c) considering that the time frame for incident reporting does not align with the criteria set by the HKMA (1 submission) and the Communications Authority (CA) (1 submission); (d) suggesting specifying the circumstances under which the time frame for reporting can be extended (2 submissions), and setting another time frame for reporting incidents relating to OT systems; (e) suggesting that the time frame for reporting incidents that involve third party service providers (especially those located outside Hong Kong) should be waived (1 submission); and (f) enquiring whether reporting is not required if the cause of the incident is not identified (1 submission).
7	As regards the **recipients of reports**, 7 items of enquiries or comments were received: (a) enquiring whether CIOs need to report to other relevant organisations (e.g. the Police, the HKMA, the CA, etc.) besides the Commissioner's Office (3 submissions); (b) suggesting establishing a clear reporting mechanism to increase the response speed (2 submissions); and (c) suggesting establishing a coordination mechanism to streamline the procedures and avoid duplicated reporting (2 submissions).
8	Regarding **information to be reported**, 6 items of enquiries or comments were received: (a) suggesting drawing up clear guidelines or samples (5 submissions), listing the minimum requirements for the details to be reported for various types of incidents (1 submission); (b) suggesting that the vulnerabilities found in the system should be reported (1 submission); and (c) enquiring whether security vulnerabilities should be reported and disclosed to the Commissioner's Office and potentially affected users; if yes, whether the Commissioner's Office will implement a coordinated vulnerability

No.	Comments and Remarks
	disclosure and support plan, so as to assist CIOs and facilitate the disclosure and post-incident mitigation procedures (1 submission). [**Remarks:** SB understands the actual difficulties that operators may encounter in incident reporting and has made reference to the relevant requirements in the United Kingdom, the European Union and the US. SB will seriously consider relaxing the time frame for reporting serious computer system security incidents from 2 hours to 12 hours after being aware of the incident, and from 24 hours to 48 hours after being aware of other incidents. Meanwhile, to ensure effective and early response to incidents, we have made reference to the practices in Singapore and Australia, and propose that when a CCS necessary for an operator's provision of essential services has been or is likely to be disrupted, or its services interrupted, the Commissioner's Office should be empowered to proactively investigate the cause directly with the operator, so as to ascertain whether it is caused by an attack. In the proposed legislation, a computer system security incident refers to an act or activity carried out without lawful authority on or through a computer or computer system that jeopardises or adversely affects its cybersecurity or the cybersecurity of another computer or computer system. The CoP will elaborate on the coverage of "incidents required to be reported" and give examples. It is proposed under the proposed legislation that operators will be required to participate in a computer system security drill organised by the Commissioner's Office at least once every two years. This requirement is set after making reference to the practices in different jurisdictions, including Singapore, as well as the international standards. We consider such requirements and arrangements for the computer system security drills appropriate.]

E. The Commissioner's Office

No.	Comments and Remarks
1	Regarding **written instructions**, the following enquiries or suggestion were received: (a) enquiries were made concerning the circumstances under which the Commissioner's Office will issue written instructions (1 submission), the contents of written instructions (1 submission), CIOs' responsibilities upon

No.	Comments and Remarks
	receipt of the written instructions (1 submission) and the expected response time (1 submission); and (b) it was suggested that issuing temporary urgent written instructions (e.g. requesting prompt remedial action for the latest vulnerabilities identified) should be avoided (1 submission).
2	Regarding **confidentiality of the data**, the following suggestions or enquiries were received: (a) enquiring about the measures to be taken by the Commissioner's Office to ensure security in the collection, storage and destruction of the data received (5 submissions); (b) enquiring about the duty of confidentiality of the Commissioner's Office (2 submissions); (c) suggesting that except with CIOs' consent, the Commissioner's Office must not share the data collected from CIOs with other government departments (1 submission); and (d) suggesting making a confidentiality agreement and developing communication guidelines (1 submission).
3	Regarding **gathering intelligence relating to cybersecurity risks**, the following suggestions were received: (a) making suggestions / enquiries concerning whether the Commissioner's Office will proactively and continuously gather intelligence relating to cybersecurity risks, collate intelligence reported by CIOs and share such intelligence with CIOs, thereby enhancing the overall capability to guard against cybersecurity risks (4 submissions); (b) suggesting collaborating with stakeholders to establish an SoC or a Network Operation Center to enhance network security standard (1 submission); and (c) considering that the traditional SIEM system or the SoC lack incident response or intelligence hunting capabilities (1 submission), and that CIOs need to adopt a proactive and intelligence-hunting approach when carrying out incident response investigation (1 submission).
4	Regarding **the division of work with the Police**, we received enquiries about: (a) the division of work between the Commissioner's Office and the Police in conducting investigation (1 submission);

No.	Comments and Remarks
	(b) whether CIOs need to report the incident to the Police and/or other organisations (e.g. the PCPD Office and the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT)) at the same time (2 submissions); and (c) the circumstances under which the Police will enter CIOs' premises for security inspections (1 submission).
5	Regarding **the division of work with the PCPD Office**, the following suggestions or enquiries were received: (a) enquiring whether an incident involving personal data leakage needs to be reported to the PCPD Office in parallel (2 submissions); (b) suggesting that the affected data subjects should be notified if the incident involves personal data leakage (1 submission); (c) suggesting better co-ordination with the PCPD Office (1 submission) to avoid confusion arising from duplication in reporting or investigation (2 submissions); and (d) suggesting that the division of work should be aligned with future amendments that may be made in the Personal Data (Privacy) Ordinance (1 submission).
6	Regarding **multilateral collaboration**, it was suggested that the Commissioner's Office should consider signing a bilateral agreement with the Mainland to ensure compliance and co-operation on cybersecurity in cross-boundary services (1 submission).
7	Regarding matters on **compatibility with extraterritorial legislation**, two items of enquiries or suggestions were received: (a) enquiring how the Commissioner's Office will deal with cases where a multinational supplier's compliance with this legislation leads to conflicts with certain extraterritorial legislation or international standards (1 submission); and (b) suggesting that consistency with the Mainland's cybersecurity standards and international best practices be maintained (1 submission). [**Remarks:** The proposed legislation is not targeted at the personal data or the commercial confidential information in the CIOs' computer systems. The Commissioner's Office will handle the data in accordance with

No.	Comments and Remarks
	the relevant legislation and internal guidelines, and will establish an internal confidential system to ensure security in the transmission and storage of data. The purposes for reporting an incident to the Commissioner's Office and to the PCPD Office are different, and so are the details of the reports. While the Commissioner's Office is responsible for identifying the reasons for data leakage and plugging the loopholes as soon as possible, the PCPD Office focuses on the protection of personal data. Hence, where an incident involves cyberattack on a computer system resulting in leakage of personal data, the operator does need to report it to both the Commissioner's Office and the PCPD Office, but "duplication" of efforts does not exist, ass the purposes of submission of reports and the follow-up actions taken will be different.

F. Designated Authorities for Individual Sectors

No.	Comments and Remarks
1	Regarding designated authorities, the following suggestions or enquiries were received: (a) suggesting that each sector should have its own designated authority (1 submission); and (b) enquiring about the time of announcement of designated authorities (1 submission).
2	Regarding the definition of **some service providers**, it was suggested that there should be clarifications on whether the HKMA will only regulate banking entities within its sector but not other non-banking entities within the banking and financial services sector (1 submission).
3	Regarding matters on regulation of **individual sectors**, the following suggestions or enquiries were received: (a) making enquiries about / suggestions for designating the Securities and Futures Commission, the Insurance Authority and the Mandatory Provident Fund Schemes Authority as the designated authorities of the **banking and financial services sector**, and the considerations for their designation/non-

No.	Comments and Remarks
	designation (1 submission); and (b) whether operators currently not regulated by the HKMA will be under its regulation after the legislation comes into effect (1 submission).
4	In respect of **coordination of the needs of individual sectors**, the following enquiries or comments were received: (a) suggesting establishing the CoP and conducting risk assessments according to the needs of the sectors, rather than setting requirements across the board (6 submissions); (b) enquiring whether a non-HKMA regulated organisation can be regulated by the HKMA if its parent company is under the HKMA's regulation (1 submission); (c) suggesting that the existing regulatory mechanism should be followed, so as to simplify the requirements and avoid reporting to multiple regulators at the same time (2 submissions); (d) suggesting considering maximum compatibility, so as to avoid duplicated or inconsistent requirements (3 submissions); (e) suggesting including only the broad principles and leaving the details to be worked out by the industry regulators (1 submission); and (f) enquiring how to strike a balance to ensure that sectors that currently have relatively loose requirements on computer system security will not become targets of malicious actors (1 submission).
5	Regarding the **aviation industry**, it was suggested that the Civil Aviation Department should be the designated authority (1 submission). [**Remarks:** CIOs of designated sectors will discharge their organisational and preventive statutory obligations as stipulated in the proposed legislation by complying with the guidelines issued by the designated authorities of the sectors. In addition to the baseline requirements that are applicable to all sectors, standards and methodology that are applicable to relevant operators will be formulated and set out in the CoP through close communication with various sectors and risk assessment, thereby assisting them in meeting the statutory requirements.]

G. Offences and Penalties

No.	Views and Remarks
1	Regarding **penalties**, the following suggestions or enquiries were received: (a) suggesting that the emphasis should be put on strengthening CIOs' cyber resilience and recovery capability rather than punishing them (2 submissions), and that mere formalistic compliance by the CIOs should be avoided (1 submission); (b) suggesting clearly stating the circumstances under which personal criminal liabilities will be involved (2 submissions), clarifying whether company directors or the management will be held personally criminally liable for negligence (1 submission), stating the circumstances under which personal criminal liabilities will not be involved (1 submission), and imposing restrictions on personal criminal liabilities (2 submissions); (c) making enquiries / suggestions about the following: clearly setting out circumstances and examples under which "reasonable excuse" could be given (3 submissions), safe harbour provisions in cases of non-compliance of third parties or due diligence (3 submissions), and exemption of criminal liabilities for self-reporting of non-compliance (2 submissions); (d) suggesting that the following should be clearly specified: the criteria for imposing the penalties (6 submissions), whether the maximum fines will be one-off or accumulative (2 submissions), whether the level of fines will be determined according to the structure or financial capability of the company (2 submissions), whether there will be aggravating or extenuating factors (1 submission), and the offences that will incur daily penalties (1 submission); (e) enquiring whether a parent company will be affected if its subsidiary company commits an offence (1 submission); (f) enquiring about the difference with penalties imposed by the designated authorities (1 submission) and whether this will lead to double penalties (1 submission); and (g) considering that the fines are too lenient (1 submission) and suggesting that the level of fines should be determined based on the scale and financial capability of the company (1 submission); suggesting that the penalties should be extended to upper stream of the supply chain (1 submission); considering that the penalties are excessive (1 submission); suggesting that daily fines should be cancelled (1 submission) and the penalties for mild non-compliance should be reduced (1 submission).

No.	Views and Remarks
2	Regarding **liabilities on third-party services**, the following enquiries or suggestions were received: (a) considering that it is difficult for CIOs to exercise control over third-party service providers, whether located in or outside Hong Kong, to ensure their compliance with the agreement and legislation (8 submissions); (b) suggesting that the liabilities to be borne by third-party service providers should be stated in the legislation (4 submissions), CIOs should be empowered to supervise third-party service providers (2 submissions), or third-party services should be covered under the scope of risk assessment (1 submission); (c) suggesting exempting CIOs' liabilities for non-compliance of third-party service providers (2 submissions); (d) suggesting that CIOs should be allowed to disclose their identities as CIOs to third-party service providers on a need-to-know basis (3 submissions); and (e) suggesting drawing up clear guidelines regarding management of third-party services (6 submissions), covering: - the measures to be implemented (1 submission); - acceptable international standards or frameworks (1 submission); - the applicability to outsourced personnel (1 submission); - actions to take if the requirements are incompatible with overseas laws (1 submission); - the way to handle cases where a CIO also has the identity of a third-party service provider (1 submission); and - a responsibility assignment matrix from the CIO to the third-party service providers, under which the "responsible, accountable, consulted and informed" parties are defined (1 submission).
3	Regarding **commencement date** of the legislation, the following suggestions were received: (a) suggesting that a grace period be set for the industries to assess system risks, devise incident response plans, hire talents, discuss contract terms with third-party service providers (during the contract period or upon contract completion), etc. (14 submissions); and that the grace period be at least 12 months (1 submission); (b) suggesting that the legislation be implemented in a phased manner on a risk-

No.	Views and Remarks
	based approach, first covering essential service, i.e. Category 1 services, so as to allow CIOs to give priority to more critical computer systems (7 submissions); and (c) suggesting expressly announcing the timetable (1 submission).
4	Regarding **review on the legislation and policies**, the following suggestions or comments were received: (a) suggesting establishing a steering committee, advisory committee, project team, working group or platform to facilitate communication and experience sharing between the Commissioner's Office and the industries, with a view to formulating better policies and improving the CoP (5 submissions); (b) enquiring whether a mechanism would be in place to listen to or solicit views from individual CIOs (2 submissions); and (c) suggesting maintaining dialogues with CIOs, cybersecurity experts and heads of compliance of the industries, and drawing reference from international standards, so as to collect constant feedback and dispel doubts (2 submissions). [**Remarks:** The legislative intent is not to punish the CIOs. The purpose of the offences and penalties is to ensure that the legislation can be effectively implemented and enforced. The offences and penalties under the proposed legislation have taken into account the situation of Hong Kong and relevant legislation in other jurisdictions. Therefore, we consider the penalties currently proposed are appropriate. The Commissioner's Office will make positive efforts to assist the operators in improving their scale and capability of preventing security incidents so as to avoid breaching the law. Under the proposed legislation, CIOs would be allowed to engage third-party service providers, but the operators still need to fulfil the relevant statutory obligations under the legislation. SB will draw reference from the experience of other jurisdictions, in order to include more guidelines on "due diligence" performance and "reasonable endeavor" in the CoP, which will serve as reference for CIOs when they draw up and enforce contracts with third-party service providers. The Government aims to set up the Commissioner's Office within one year upon the passage of the proposed legislation, after which to bring the proposed legislation into force within half a year's time. In the meantime, SB and the Commissioner's Office will maintain

No.	Views and Remarks
	close communication with potential operators to be designated, and will designate CIOs and CCSs in a phased manner having regard to the risk and level of readiness of organisations, while developing relevant content of the CoP. As for statutory obligations under the proposed legislation such as risk assessment, independent audit and submission of relevant reports, the time frames will be calculated from the time of designation. Therefore, potential organisations to be designated as CIOs should have ample preparation time.]

H. Investigation Powers of the Commissioner's Office

No.	Comments and Remarks
1	Regarding the term **"premises"**, there were views that the definition of "relevant premises" in the English version is unclear (Remarks: the term in the Chinese version is "premises") (3 submissions).
2	Regarding the definition of **"relevant information"**, there were views that the meaning of the term is too broad (2 submissions).
3	Regarding **powers** of the Commissioner's Office, the following comments and suggestions were received: (a) suggesting that the Commissioner's Office should only be granted the minimum investigation powers, which must be authorised by law and against which appeals and reviews can be made (2 submissions); (b) enquiring about the objective threshold or conditions for granting the investigation powers (2 submissions); (c) suggesting that unless with adequate legal authorisation, the power to connect to or install programmes in CCSs should be removed (2 submissions); (d) enquiring whether the Commissioner's Office has the power to conduct on-site checks (including random checks) (2 submissions); (e) enquiring about the types of information required during investigation (1 submission); (f) enquiring how to handle information involving legal professional privilege (1 submission) and whether there is a right to obtain legal privilege (1 submission);

No.	Comments and Remarks
	(g) suggesting that guidelines should be given for recording and retaining digital forensic evidence (1 submission); (h) suggesting that the Commissioner's Office may authorise the issuance of warrants or the remote control of critical computer facilities in emergencies (1 submission); (i) enquiring how to conduct cross-boundary investigation (1 submission), such as on third-party cloud service providers outside Hong Kong (1 submission); and (j) enquiring whether there are guidelines for CIOs to follow if they need to collect evidence from and share information with overseas parties (1 submission).
4	In respect of the **rights and responsibilities of CIOs**, the following enquiries or suggestions were received: (a) enquiring whether the investigated parties have the right to appoint a legal representative (1 submission); (b) enquiring about the standards and procedures for entering the data centre (the crimes committed by the clients may not be known to the data centre) (1 submission); (c) enquiring about the duties and functions of the staff of the Commissioner's Office, and whether the positions of subject matter experts or advisory members will be taken up by a third party (1 submission); and (d) suggesting that the recovery work be carried out by the party most familiar with the CCS, i.e. the CIO (1 submission). [**Remarks:** The proposed legislation stipulates that only when a CIO is unwilling or unable to respond to a serious incident on its own would the Commissioner's Office consider applying to a Magistrate for a warrant to connect equipment to or install programmes in CCSs in view of necessity, appropriateness, proportionality and public interest, so as to respond to the incident. Relevant regulators in other jurisdictions (such as Australia and Singapore) also have similar powers.]

I. Appeal Mechanism

No.	Comments and Remarks
1	Regarding appeal mechanism, the following suggestions or enquiries were received: (a) enquiring about the method for forming the appeal board (3 submissions), including whether the board members possess the relevant expertise of the sector (1 submission), and ways to fulfil confidentiality and maintain independence of the board (1 submission); (b) enquiring whether there are guidelines for conducting appeals (1 submission), whether there are performance pledges (1 submission), whether the board's decisions are final and the means for seeking further review (2 submissions); (c) enquiring whether charges are involved for making appeals (1 submission); (d) enquiring whether, during the appeal process, CIOs need to comply with the directions of the Commissioner's Office (1 submission); (e) suggesting that as regards compatibility, the PCPD Office's existing mechanism for handling appeals (pursuant to the Administrative Appeals Board Ordinance (Cap.442)) be adopted (1 submission); and (f) enquiring how CIOs can file an appeal against a court warrant or the investigation powers of the Commissioner's Office (2 submissions). [**Remarks:** Drawing reference from the arrangements of various existing statutory appeal boards, SB proposed that under the proposed legislation, the appeal board will be a team comprising of about 15 experts from the industry, cybersecurity and legal profession (including one chairperson of the board) appointed by the CE. The board members should be independent of the Commissioner's Office. Each appeal hearing will be conducted by three board members. The three board members must make a declaration about the absence of conflict of interest (e.g. industry competitors) and sign a non-disclosure agreement on the content of the hearing.]

J. Subsidiary Legislation

No.	Comments and Remarks
1	Regarding subsidiary legislation, the following suggestions and comments were received: (a) suggesting that the time and mechanism should be clarified as regards expanding the scopes of sectors by way of subsidiary legislation (1 submission); and (b) expressing concerns that the subsidiary legislation will be used to bypass the legislative process (2 submissions). [**Remarks:** The enactment and amendment of a subsidiary legislation are subject to an established set of highly stringent procedures to ensure fairness, openness, impartiality and transparency, and such procedures are monitored by the LegCo.]

K. CoP

No.	Comments and Remarks
1	As regards the **monitoring and detection mechanism** under the **computer system security management plan**, we received a suggestion for specifying whether "separation" refers to separation of the development environment from the testing environment or from the production environment, or both (1 submission).
2	As regards the **computer system security training** under the **computer system security management plan**, the following enquiries or suggestions were received: (a) suggesting that the scope, depth and methodology of training as well as the types of personnel to be trained (e.g. operators, maintenance personnel, suppliers, contractors and service providers) should be clearly stated (2 submissions), and it should be made clear whether training for contractors and service providers (which is not a common practice in the industry) should be provided (1 submission); (b) enquiring whether training has to be tailored to the functions of the personnel to be trained (1 submission); and whether both theoretical and practical training are to be covered (1 submission); (c) suggesting that cybersecurity training should be made mandatory (1 submission) and CIOs should be required to allocate more resources to

No.	Comments and Remarks
	training (1 submission); (d) suggesting that the Commissioner's Office should assist or support CIOs in devising cybersecurity training (1 submission); (e) enquiring whether there are sufficient cybersecurity auditors and talents for safeguarding cybersecurity other than the red team (offensive team) locally (1 submission); (f) training courses that are provided by the Hong Kong Internet Registration Corporation Limited (HKIRC) cannot be found (1 submission); and enquiring whether staff training support other than training provided by the HKIRC is available (1 submission); (g) enquiring whether the Government has plans for increasing the supply of cybersecurity talents (1 submission); and (h) suggesting that more training should be provided for small and medium enterprises (1 submission).
3	Regarding the appointment of **24/7 contact point** under **incident response obligations**, there were enquiries about whether it is necessary for the contact point to be working in Hong Kong and whether such positions can be taken up by personnel in the representative office (2 submissions); it was suggested that the SoC can serve as the contact point (1 submission); and there was an enquiry as to whether the position can be doubled by the computer system security management unit (1 submission).
4	As regards the **timetable for completing the CoP**, the following enquiries or comments were received: (a) enquiring when the CoP will be issued (3 submissions) and implemented (1 submission), and suggesting that the CoP be issued as soon as possible (1 submission); and (b) suggesting that CIOs should be given sufficient time to prepare for the detailed arrangements after the issuance of the CoP (1 submission).
5	Regarding **contents development**, the following enquiries or comments were received: (a) suggesting that sectoral experts' participation should be invited and industries should be widely consulted (5 submissions) in drawing up the contents, or the contents should be drawn up by professional organisations

No.	Comments and Remarks
	(1 submission); (b) making suggestions / enquiries about whether contents will be developed in accordance with international standards such as ISO, SOC2 or the framework of the National Institute of Standards and Technology (4 submissions); (c) enquiring about the overall direction (1 submission); suggesting that the details should cover, for example, the requirements, methodologies and standards in respect of asset identification and management, risk assessment, risk detection, security audits, penetration test, design, configuration, operation, implementation, incident response and investigation, evidence preservation, incident impact assessment and incident recovery, and guidelines should be provided (7 submissions); (d) suggesting providing pragmatic guidelines for tackling issues relating to supply chain (1 submission), including implementation of encryption key management (1 submission); (e) suggesting that flexibility should be allowed in handling the "security by design" requirement, which has been advocated only in recent years (1 submission); (f) suggesting maintaining technological neutrality in the contents (1 submission); (g) suggesting that, as far as access control is concerned, CIOs should only need to maintain logs of accesses and attempted accesses to the systems within a reasonable period of time instead of maintaining all logs (1 submission); (h) suggesting that a working group should be formed to further study the uniqueness of the third party service environment, with a view to improving the contents of the CoP (1 submission); (i) suggesting that emphasis should be put on the principles, and there is no need to specify and restrict cybersecurity products (1 submission); (j) raising two enquiries and suggestions regarding the enhancement of baseline requirements: - whether more detailed requirements similar to C-RAF and NIST are needed for access control, account management and privileged access management in order to mandate the implementation of best practices; - as regards baseline maintenance, whether hardening checks are required; - whether patch management will be extended to cover threat and

No.	Comments and Remarks
	vulnerability management; - whether implementation of vulnerability hunting or vulnerability disclosure programmes will be recommended; - as regards patch management, whether there are clear guidelines for prompt updates; - how to define "adequately" in the context of backup and recovery, and whether a fallback venue is required; - how to perform security test sooner (also known as "shift left") and adopt the "development, security, operations" approach to achieve design security; and (k) suggesting maintaining dialogues with the industries in order to formulate new requirements and improve the CoP having regard to technological development (2 submissions). [**Remarks:** In formulating the CoP, the Commissioner's Office will take into full account the views of industry stakeholders. Practicable requirements will be imposed based on the prevailing international standards or characteristics of the industries, having regard to the uniqueness of the sectors. The Commissioner's Office will also review and improve the content of the CoP in an ongoing manner. In formulating the CoP, the Commissioner's Office will set out in detail the requirements and scope of the computer system security training and provide relevant information on training for reference.]

L. Other Comments and Suggestions

No.	Comments and Remarks
1	Regarding **financial support**, the following enquiries or suggestions were received: (a) suggesting that subsidies and grants be provided for the industries (6 submissions); (b) suggesting that consideration be given to setting up a network security fund or funding scheme (2 submissions); (c) suggesting encouraging the use of Technology Voucher Programme (TVP) (1 submission) and enhancing the TVP (1 submission); and (d) enquiring whether the incident reports will be recognised by the

No.	Comments and Remarks
	Commissioner's Office and for which cyber insurance claims can be made (1 submission).
2	Regarding **resources for the industries**, four items of enquiries or suggestions were received: (a) requesting that resources, guidelines and support (1 submission), such as cybersecurity experts, technical support and funding for security enhancement, be provided for CIOs (1 submission); (b) requesting that a list of approved service providers and guidelines for choosing service providers (and whether insurance is required) be provided (1 submission); and (c) enquiring whether CIOs will be accorded priority in receiving supply of energy, fresh water and fuel (1 submission).
3	In respect of **enhancing the overall cybersecurity ecosystem of Hong Kong**, we received the following suggestions: (a) providing incentives, e.g. tax reduction, public recognition, encouraging the input of resources and demonstration of commitment for sectors to exceed baseline requirements (2 submissions); (b) encouraging CIOs to share useful cyber threat intelligence, which the Commissioner's Office can promptly disseminate to other CIOs to avoid similar attacks (2 submissions); (c) providing resources and support for CIOs, instead of focusing on penalties (1 submission); (d) the Commissioner's Office take the lead in establishing a cybersecurity ecosystem (1 submission); (e) large-scale attacks operations be coordinated by central authorities (1 submission); (f) considering introducing mandatory certification in cybersecurity (1 submission); (g) establishing a critical third-party service framework to enhance the cyber resilience capabilities of third-party service providers (1 submission); (h) encouraging using the services of a diversified network of providers

No.	Comments and Remarks
	(1 submission); (i) studying the impact of AI on cybersecurity (1 submission); (j) putting in place an encryption key management mechanism to maintain the digital sovereignty of entities in Hong Kong (1 submission); and (k) earmarking provisions for enhancing the public awareness of cybersecurity (1 submission). [**Remarks:** Most operators have already established certain standards for computer system security. Individual regulatory authorities have also drawn up guidelines for the security measures of the computer systems in the industry. We therefore expect that the relevant requirements under the proposed legislation will not have much impact on major operators. At present, the Government's TVP assists eligible operators to enhance cybersecurity standard. The HKIRC provides cybersecurity-related training services for corporate staff, and the HKCERT also provides technical advice on cybersecurity for enterprises. We welcome suggestions for safeguarding and strengthening the cybersecurity ecosystem in Hong Kong. Upon its establishment, the Commissioner's Office will collaborate with the Digital Policy Office, the Police and industry stakeholders to jointly promote IT security through public education, and will continue to enhance the IT security awareness of CIOs and provide them with technical support.]

Security Bureau
October 2024