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 takes 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) 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.