File reference: SBCR 1/3231/2022 Pt. 5

LEGISLATIVE COUNCIL BRIEF

PROTECTION OF CRITICAL INFRASTRUCTURES (COMPUTER SYSTEMS) BILL

INTRODUCTION

At the meeting of the Executive Council on 3 December 2024, the Council **ADVISED** and the Chief Executive **ORDERED** that the Protection of Critical
A Infrastructures (Computer Systems) Bill ("the Bill"), at **Annex A**, should be introduced into the Legislative Council ("LegCo").

JUSTIFICATIONS

2. Critical infrastructures ("CIs") refer to infrastructures that are necessary for or of great importance to the maintenance of normal functioning of society and the normal life of the people. Nowadays, the operation of CIs has become more dependent on the Internet, computer systems, telecommunications infrastructures and smart devices, etc. Their computer systems are also increasingly vulnerable to attacks with serious consequences. In the event that the operation of CIs is disrupted as a result of attacks on their computer systems, there may even be rippling effects affecting the entire society, seriously jeopardising the public interest including the economy, people's livelihood and public safety.

3. In this regard, laws and regulations protecting the security of computer systems of CIs have become increasingly common in other jurisdictions[1], all explicitly requiring operators of critical infrastructures to implement measures to protect their computer systems, enhance their capabilities to respond to attacks, and report to the regulatory

[1] Similar legislation has been enacted in the Mainland China, Macao Special Administrative Region ("Macao SAR"), Australia, the European Union ("EU"), Singapore, the United Kingdom ("UK") and the United States ("US"), etc. A relevant bill is also under deliberation by the Parliament of Canada.

authority in the event of security incidents on computer systems. The Bill is drafted with reference to the legislation in other jurisdictions with modifications with regard to Hong Kong's local situation.

THE PROPOSED LEGISLATIVE REGIME

A. Purpose and Principles

4. The Bill aims to impose statutory requirements to ensure that operators of CIs that have been designated under the Bill ("CIOs") have put in place appropriate measures to protect their computer systems and minimize the chance of essential services being disrupted or compromised due to cyberattacks, thereby maintaining the normal functioning of the Hong Kong society and the normal life of the people. This is conducive to enhancing the overall computer-system security in Hong Kong. It also provides for the powers of a Commissioner (to be appointed under the Bill (see Part E)) and designated authorities ("DAs") (see Part G) for the implementation of the new legislative regime, which seeks to:

(a) set out a regulatory model that is suitable for Hong Kong with reference to legislative approaches of other jurisdictions;

(b) regulate CIOs that are necessary for (i) the continuous provision of essential services or (ii) maintaining important societal and economic activities in Hong Kong, most of which are large organizations, and hence small and medium enterprises and the general public will not be subject to the regulation of the Bill;

(c) require CIOs to bear the responsibility for protecting the security of their computer systems that are essential to the core functions[2] of the CIs (see paragraph 14 below), which in no way targets personal data and trade secrets; and

(d) set out statutory obligations (see paragraph 15 below) which are basic requirements, from which CIOs can build up and enhance their capabilities for securing their computer systems with regard to their own needs and

[2] "Core functions" refer to the provision of essential service or any function that is essential to the maintenance of critical societal and economic activities in Hong Kong.

characteristics.

5. By requiring CIOs to set up dedicated management units to oversee their computer-system security, and take preventive measures including drawing up computer-system security management plans, conducting risk assessment and audits, the Bill would enhance CIOs' resilience against attacks on their computer systems and better prepare them for any emergency situations. Moreover, CIOs will be required to notify the Commissioner of computer-system security incidents while taking measures to respond to the incidents and recover the system. The Commissioner may, where necessary, provide timely assistance in remedial measures to contain the problem and reduce the chance of affecting other CIs, thereby maintaining the normal functioning of the Hong Kong society and the normal life of the people.

6. While the legislative intent is not to punish CIOs in case of breaches, in order to ensure effective implementation and enforcement, relevant offences and appropriate penalties must be stipulated. After balancing the impact of the legislative regime on institutions and the need to ensure sufficient deterrent effect, penalties for non-compliance will be imposed on an organization basis. That said, if any non-compliance involves violation of existing criminal laws, such as making false statements, using false instruments or other fraud-related offences, the persons involved could be held criminally liable, and such offences will be investigated by other responsible law enforcement authorities.

B. Scope of Regulation

CIs

7. CIs are the linchpin of society and economy and are crucial to the normal functioning of society. Their computer-system security must be safeguarded. The Bill covers two major categories of CI as follows:

(a) **Category 1 - Infrastructures for continuous provision of essential services in Hong Kong**: these relate to 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 society. In this regard, the Bill sets out eight sectors, namely (1) Energy;

(2) Information Technology; (3) Banking and Financial Services; (4) Land Transport; (5) Air Transport; (6) Maritime Transport; (7) Healthcare Services; and (8) Telecommunications and Broadcasting Services. Reference has been made to other jurisdictions with relevant legislation that also sets out sectors of essential services; and

(b) **Category 2 - Infrastructures for maintaining critical societal and economic activities***:* these relate to infrastructures (e.g. major sports and performance venues, major technology parks, etc.) the damage, loss of functionality or data leakage of which may hinder or otherwise substantially affect maintenance of critical societal and economic activities in Hong Kong. Reference has been made to the legislation of the UK, Australia, the US and the EU, which also covers infrastructures with similar descriptions.

8. Having made reference to the practice of the UK, the Bill sets out the following factors which may be taken into account in ascertaining whether an infrastructure is a CI –

(a) the kind of service provided by the infrastructure;

(b) the implications if the infrastructure is damaged, loses functionality or suffers any data leakage; and

(c) any other matters the Commissioner or DA considers relevant.

Non-application to the Government

9. The Bill does not apply to the Government. Notwithstanding, Government bureaux/departments must abide strictly by the Security Regulations and the detailed Government Information Technology Security Policy and Guidelines ("Policy and Guidelines"), which are reviewed and updated regularly with reference to the latest international standards and industry best practices. The Digital Policy Office ("DPO") also regularly conducts compliance health checks on government public-facing information systems and in-depth audits for Government bureaux/departments. Moreover, violation of the Policy and Guidelines by public officers may be liable to disciplinary actions. In this regard, we consider it appropriate to continue to regulate Government bureaux/departments with the Government's established practice to ensure

compliance by an administrative approach without incorporating them into the proposed legislation.

C. Targets of Regulation

10. The Bill provides that only CIOs designated under the Bill and their computer systems that have been designated under the Bill as critical computer systems ("CCSs") will be regulated.

CIOs

11. Given that most of the CIs are operated by large organizations, with reference to the practices of the UK, Australia and the EU, the Bill adopts an "organization-based" approach, i.e., using the organization responsible for operating a CI as the unit on which the obligations in relation to protecting the security of its computer systems are imposed, so as to ensure that each organization designated as CIOs has a requisite plan to protect its CCSs.

12. If the Commissioner or DA is satisfied that an infrastructure is a CI having regard to the considerations set out in paragraph 8 above, the Commissioner or DA may designate an organization as a CIO taking into account, among others, the following factors:

(a) how **dependent** the core function of the infrastructure concerned is **on computer systems**;

(b) the **sensitivity of the digital data controlled** by the operator in respect of the infrastructure concerned;

(c) the **extent of control** of the organization has over the operation and management of the infrastructure concerned; and

(d) any information provided in relation to the infrastructure in respect of the factors set out in paragraph 8 above.

13. To prevent CIs and CIOs from becoming targets of attack, the Bill only sets out the names of the essential services sectors in Schedule 1, instead of disclosing the list of CIs and CIOs. This approach is in line with the practice of other jurisdictions (e.g. the UK and Australia).

CCSs

14. While CIOs may have many computer systems, to enable the CIOs to focus their resources to protect the most important systems, the Bill only imposes obligations with respect to computer systems that are essential to the core functions of CIOs and are accessible by the CIOs in or from Hong Kong. Such computer systems may be designated under the Bill as CCSs for the CIs concerned. This is in line with the practices of Australia, the UK and the EU. In considering whether to designate a computer system as a CCS, the Commissioner or DA may take into account, among others, the following factors:

(a) the role of the computer system in respect of the core function for a CI;

(b) the impact on such a core function if the computer system is disrupted or destroyed;

(c) how related the computer system is with any other computer systems of the CIO concerned; and

(d) how related the computer system and any other computer systems of the CIO concerned are with those of any other CIOs.

The requirements of the Bill apply to all CCSs that have been designated as such.

D. Obligations of the CIOs

15. To ensure that CIOs will put in place a sound management structure to implement the necessary measures to protect the security of their CCSs, and promptly respond to and recover the affected systems when they are attacked, with reference to the relevant legislation in Australia, the UK and the EU, the Bill imposes on CIOs three categories of statutory obligations, namely Category 1 obligations (organizational);

Category 2 obligations (preventive); and Category 3 obligations (incident reporting and response), as listed below:

Category 1 obligations (Organizational) – CIOs must:

(a) **maintain an office in Hong Kong** and notify the Commissioner or DA of the address (and report any subsequent changes);

(b) notify the Commissioner or DA of **operator changes** in relation to the CIs; and

(c) maintain a **computer-system security management unit** (in-house or outsourced) which has to be **supervised by an employee of the CIO** who possesses adequate professional knowledge.

The main purpose of Category 1 obligations is to ensure that the CIO implements a sound management structure for protecting the security of computer systems and to ensure effective communication between the CIOs and the Commissioner or DA for the smooth implementation of the regulatory regime.

Category 2 obligations (Preventive) - CIOs must:

(d) notify the Commissioner or DA of **material changes to their computer systems**, including changes to design, configuration, security, operation, etc., of their CCSs;

(e) prepare and implement a **computer-system security management plan** and submit the plan to the Commissioner or DA;

(f) conduct a **computer-system security risk assessment** at least once every year and submit a report to the Commissioner or DA; and

(g) arrange for an independent **computer-system security audit** to be carried out at least once every two years and submit a report to the Commissioner or DA.

The main purpose of Category 2 obligations is to ensure that the necessary measures are put in place to protect the security of the CCSs of the CI and to prevent attacks on the CCSs of the CI.

Category 3 obligations (Incident Reporting and Response) - CIOs must:

(h) participate in a **computer-system security drill** organized by the Commissioner;

(i) prepare and implement an **emergency response plan** and submit it to the Commissioner; and

(j) **notify** the Commissioner of the occurrence of **computer-system security incidents** (i.e. any event that involves access to the CCSs or any other act done on or through the CCS or another computer system without lawful authority, which has an actual adverse effect on the computer-system security of the CCSs[3]) in respect of CCSs. Serious incidents which have disrupted, are disrupting or will likely disrupt the core function of CIs must be reported within 12 hours after the CIO becomes aware of the incidents, while other incidents must be reported within 48 hours.

The main purposes of Category 3 obligations are to ensure that CIOs are capable of responding to incidents and recovering promptly; and**,** in the event of attacks, allow the relevant authorities to investigate the cause, take timely actions to prevent further attacks, and plug system loopholes to reduce the possible spread of the problem.

E. Commissioner's Office

16. A Commissioner's Office responsible for the implementation of the legislative regime, including the designation of CIOs and CCSs and monitoring their compliance with the statutory obligations, will be set up under the Security Bureau (SB). It will be headed by a Commissioner to be appointed by the Chief Executive. The key duties and functions of the Commissioner include –

(a) identifying CIs and designating CIOs and CCSs;

(b) issuing codes of practice (CoPs) in respect of CIO obligations;

---

[3] Examples include unauthorized access to, or control of, the computer system by means of hacking, unauthorized interception of data, denial of service (DDoS) attack, etc. In other words, other events such as mere physical attacks to CIOs (e.g. burglary into CIs) that do not affect the computer-system security of the CCS, or disruption of service due to natural disasters or technical problems, need not be reported.

(c) monitoring and supervising compliance with the provisions of the Ordinance;

(d) regulating CIOs with regard to the computer-system security of the CCSs;

(e) monitoring, investigating and responding to computer-system security threats and computer-system security incidents in respect of CCSs of CIs;

(f) coordinating the implementation of the Ordinance with DAs (see Part G below) and government bureaux/departments; and

(g) performing any other functions that are imposed or conferred on the Commissioner under the Ordinance or any other Ordinance.

F. CoPs

17. While the compliance of certain statutory obligations, such as submitting various information, plans or reports within the prescribed deadline, is relatively straightforward, the compliance of some other obligations may involve varying forms or degrees in terms of scopes, methodologies and processes. The Commissioner and DAs will be empowered to issue CoPs, including sector-specific ones, to set out recommended standards and provide practical guidance to CIOs to fulfil the Categories 1, 2 and 3 obligations[4]. The approach is similar to that of Singapore.

18. In formulating and updating the CoPs, the Commissioner and DAs would take into account the latest technology and international standards, and consult relevant stakeholders as appropriate. CoPs are not subsidiary legislation, nor would failure to comply with the provisions of CoPs in itself constitute an offence. However, the Commissioner or DA may issue written directions to require CIOs to take any action in relation to the compliance with obligations (such as revising and resubmitting a document) if there has been non-compliance or defective compliance with such obligations, which may be considered with reference to CoPs. Failure to comply with such directions would be an offence. An outline of the CoP is at **Annex B**.

B

[4] For example, the Bill will require the CIOs to submit a computer-system security audit report at least once every two years; whereas the CoP will set out the relevant professional qualifications that an independent computer-system security auditor should possess, the scope of the audit, etc.

G. DAs for Certain Sectors

19. Some of the essential service sectors to be regulated under the legislative regime are already comprehensively regulated by other specialized authorities, e.g. (1) the banking and financial services sector regulated by the Monetary Authority ("MA"), and (2) the telecommunications and broadcasting services sector regulated by the Communications Authority ("CA"). These sectors are subject to the existing regulatory regimes in relation to the provision of essential services which are mature and well-established, and some of which have in place guidelines on certain specific aspects of computer-system security.

20. Considering that the MA and CA are most familiar with the actual practices and needs of the respective sectors currently regulated by them, the Bill designates them as DAs to carry out certain statutory functions in respect of CIOs in the sectors regulated by them. Similar practice of assigning the regulation of certain CIOs to sectoral regulators is also seen in relevant laws of the UK, Australia and the US.

21. DAs will be empowered to designate CIOs and CCSs in respect of the sectors regulated by them, and monitor their compliance of Category 1 obligations (organizational) and Category 2 obligations (preventive). CIOs regulated by DAs will report to their respective DAs on these two types of obligations. DAs are also empowered to issue CoPs to set out standards applicable to CIOs regulated by DAs in relation to Categories 1 and 2 obligations with reference to prevailing and/or trade standards.

22. In order to ensure that the Commissioner will have a full grasp of the situation of incident reporting and response of all CIOs, the Commissioner will take full charge of monitoring compliance of Category 3 obligations on incident reporting and response in respect of all CIOs, including CIOs regulated by DAs. The Commissioner will coordinate contingency plans and prevent incidents from spreading to other CIs.

23. To ensure that the Commissioner has full control of the implementation and enforcement of the requirements of the Bill so as to protect the security of CCSs of all CIs in Hong Kong as a whole, the Commissioner also retains the power to issue written directions to all CIOs (including CIOs regulated by DAs) under the legislative regime.

In practice, we envisage that the Commissioner and the DAs will consult each other as needed in carrying out their respective functions under the Bill.

H. Offences and Penalties

24. Violations under the legislative regime constitute offences subject to the defences of "due diligence" in respect of non-compliance with the Categories 1, 2 and 3 obligations or written directions, and "reasonable excuse" for other offences. The obligations and requirements under the Bill which will result in offences and penalties for non-compliance will be imposed on CIOs at the organizational level only, and are not designed to target at their staff at individual level.

25. Taking into account the legislative intent and making reference to the relevant legislation of the UK and EU, the penalties under the Bill will only include fines, with maximum level ranging from HK$500,000 to HK$5 million, and additional daily fines for persistent non-compliance for certain continuing offences, the maximum of which range from HK$50,000 to HK$100,000.

I. Powers of the Commissioner and DAs

26. The Bill empowers the Commissioner and DAs[5] to exercise various powers to –

(a) obtain information for the purpose of designating CIOs and CCSs;

(b) obtain information to better understand the CCSs of the CIOs for threat assessment, incident response preparation and ascertaining compliance of obligations; and

(c) investigate offences under the legislation.

Moreover, the Commissioner will be empowered to investigate the cause of any event that has or is likely to have an actual adverse effect on CCS (e.g. a disruption or failure

[5] The powers exercisable by DAs only relate to the CIOs regulated by them and Categories 1 and 2 obligations.

of CCS) for the purpose of identifying whether a computer-system security threat or computer-system security incident has occurred, and to investigate and respond to computer-system security threats and computer-system security incidents.

27. The Bill sets out specific conditions for the exercise of the above powers, which officers can exercise such powers and whether a magistrate's warrant is needed. For instance, in terms of powers to respond to computer-system security incidents, the Commissioner's authorized officer may, with the direction of the Commissioner, request a CIO to answer questions and submit information on the incident after its occurrence. If the CIO is unwilling or unable to respond to the incident, the authorized officers may, subject to certain conditions, request the CIO to assist in the investigation and take remedial measures. In case the CIO is unwilling or unable to cooperate, the authorized officers may apply for a magistrate's warrant in order to require an organization other than the CIO who appears to have control over the CCS to assist in the investigation. Further powers to enter premises on which the CCS concerned is or is likely to be located for investigation and taking remedial measures may only be exercised by the authorized officers with warrant issued by the magistrate, and such power may be exercised without a warrant exceptionally and only in the case of emergencies. A warrant will only be issued if the magistrate is satisfied that all conditions prescribed in the Bill are met.

J. Appeal Mechanism

28. The Bill provides for an independent appeal mechanism for CIOs who disagree with a designation of CIO or CCS, a written direction issued by the Commissioner or DAs, or a decision to impose a requirement in relation to a computer-system security risk assessment or audit. In this regard, the Chief Executive will be empowered to appoint an appeal panel, comprising at least 15 members, one of which being the chairperson. An appeal board will be formed by drawing from the panel to hear each appeal. Members of the appeal board should include legal professionals and information technology professionals, etc., to ensure that there is balanced and independent third-party expertise in considering an appeal. The board may decide to affirm, reverse or vary a decision.

K. Subsidiary legislation

29. Certain details relating to implementation of the Bill, including the powers of the Commissioner or the statutory obligations of the CIOs, may need to be supplemented, updated or amended from time to time in future. The Bill empowers the Secretary for Security to specify or amend by way of subsidiary legislation matters such as the sectors that are regarded as essential services sectors; the list of DAs; the essential scopes of computer-system security management plans, security audits, risk assessments and emergency response plans; the time for notifying computer-system security incidents and details of the appeal mechanism, etc.

OTHER OPTIONS

30. The proposed legislative regime cannot be implemented without introducing new legislation. We have considered the alternative of regulating computer-system security of CIs by amending existing sectoral regulations. However, this lacks comprehensive standards, as not every CI is regulated by sectoral regulators, and the existing regulations often vary widely across sectors. Moreover, the lack of bespoke legislation for protecting computer-system security of CIs falls behind the international trend, leaving Hong Kong at a competitive disadvantage.

THE BILL

31. The key provisions of the Bill are as follows–

(a) **Part 1** - sets out preliminary provisions such as the short title and provides for the commencement of the Bill;

(b) **Part 2** - sets out the appointment, functions and powers of the Commissioner and DAs, including the issue of CoPs;

(c) **Part 3** - provides for the ascertainment of CIs and the designation of CIOs and CCSs and the power to obtain information for such ascertainment and designation as well as for ascertaining the compliance of obligations etc.;

(d) **Part 4** - sets out the statutory obligations of CIOs;

(e) **Part 5** – provides for the Commissioner's powers to respond to computer-system security threats and incidents;

(f) **Part 6 -** sets out the Commissioner's and DAs' powers to investigate offences under the Bill;

(g) **Part 7 and Schedule 7 –** provide for matters relating to appeal, including appointment of appeal panel and appeal procedures;

(h) **Part 8 –** provides for miscellaneous matters, such as the preservation of secrecy, appointment of authorized officers and the Secretary for Security's power to amend the Schedules to the Bill by subsidiary legislation;

(i) **Schedule 1** – provides for the list of sectors of essential services specified for purposes of definition of CIs;

(j) **Schedule 2** – provides for the list of DAs and categories of regulated organizations;

(k) **Schedule 3** – provides for the scope of computer-system security management plans and emergency response plans;

(l) **Schedule 4** – provides for the scope of computer-system security risk assessment;

(m) **Schedule 5** – provides for the scope of computer-system security audits;

(n) **Schedule 6** – provides for time-related notification requirements for computer-system security incidents.

LEGISLATIVE TIMETABLE

32. The legislative timetable will be as follows –

Publication in the Gazette	6 December 2024
First Reading and commencement of Second Reading debate	11 December 2024
Resumption of Second Reading debate, committee stage and Third Reading	To be notified

IMPLICATIONS OF THE BILL

33. The financial and civil service, and economic implications of the Bill are at **Annex C**. The Bill does not contain any express binding effect provision and is in conformity with the Basic Law, including the provisions concerning human rights. It has no environmental, productivity, gender or family implications, and no sustainability implications other than those set out in the economic implications paragraph at Annex C.

PUBLIC CONSULTATION

34. We have been engaging stakeholders (including organizations that may be designated as CIOs, computer-system security service providers, chambers of commerce and professional bodies, etc.) since 2023. We consulted the LegCo Panel on Security ("the Panel") on 2 July 2024, followed by a one-month consultation exercise which ended on 1 August 2024. Almost all of the views received support the legislative regime or offer constructive suggestions. 52 out of 53 submissions received indicated support for the legislative proposal. We have also made timely rebuttals against some unfounded criticisms and clarified misunderstandings. We have also refined our proposal by taking into account views expressed by stakeholders (e.g. relaxing the timeframe for reporting serious computer-system security incidents from 2 hours to 12 hours after becoming aware of the incident, and from 24 hours to 48 hours after becoming aware of other incidents). A consultation report (a summary of which is at **Annex D**) was issued to the Panel for information on 2 October 2024. The Panel supported the legislative proposal in general.

35. A briefing for major chambers of commerce and all stakeholders was held on 1 November 2024 to brief them on the consultation report and consolidate their support. We have also arranged some 10 engagement sessions with selected key potential CIOs before the introduction of the Bill to gauge their views on the framework of the CoP. We also ensure stakeholders and members of the public have a clear understanding of the Bill through various promotional materials, including social media posts.

PUBLICITY

36. We will issue a press release and make available a spokesperson to answer media and public enquiries.

ENQUIRIES

37. For enquiries on this brief, please contact Ms Sandy Cheung, Principal Assistant Secretary for Security (E) at 2810 2632.

Security Bureau
4 December 2024

Protection of Critical Infrastructures (Computer Systems) Bill

Contents

Clause Page

Clause Page

Clause Page

Clause Page

A BILL

To

Protect the security of the computer systems of Hong Kong's critical infrastructures; to regulate the operators of such infrastructures; to provide for the investigation into, and response to, computer-system security threats and incidents in respect of such computer systems; and to provide for related matters.

Enacted by the Legislative Council.

Part 1

Preliminary

1. Short title and commencement

(1) This Ordinance may be cited as the Protection of Critical Infrastructures (Computer Systems) Ordinance.

(2) This Ordinance comes into operation on a day to be appointed by the Secretary for Security by notice published in the Gazette.

2. Interpretation

(1) In this Ordinance—

appeal board (上訴委員會) means an appeal board appointed under section 4(1) of Schedule 7;

appeal panel (上訴委員團) means the appeal panel mentioned in section 47(1);

authorized officer (獲授權人員), in relation to a regulating authority, means—

(a) if the authority is the Commissioner—a person appointed under section 50(1); or

(b) if the authority is a designated authority—a person appointed by the authority under section 51(1);

category 1 obligation (第 1 類責任) means an obligation imposed by Division 1 of Part 4;

category 2 obligation (第 2 類責任) means an obligation imposed by Division 2 of Part 4, and includes an obligation to comply with requirement imposed under section 24(5) or 25(4) or (6);

category 3 obligation (第 3 類責任) means an obligation imposed by Division 3 of Part 4;

CI operator (關鍵基礎設施營運者) means an organization designated under section 12;

code of practice (實務守則), except in section 55, means a code of practice issued under section 8 (including such a code of practice that is revised under section 8);

Commissioner (專員) means the Commissioner of Critical Infrastructure (Computer-system Security) appointed under section 3(1);

computer system (電腦系統)—

(a) means a set of computer hardware and software that is organized for the collection, processing, storage, transmission or disposition of information; and

(b) includes a computer;

computer-system security (電腦系統安全), in relation to a critical computer system, means the ability of the system to resist, and the state in which the system is protected from, events and acts that compromise the availability, integrity or confidentiality of—

(a) the information stored in, transmitted or processed by, or accessible via, the system; or

(b) the services offered by, or accessible via, the system;

computer-system security incident (電腦系統安全事故), in relation to a critical computer system, means an event that—

(a) involves—

(i) access, without lawful authority, to the critical computer system; or

(ii) any other act done, without lawful authority, on or through the critical computer system or another computer system; and

(b) has an actual adverse effect on the computer-system security of the critical computer system;

computer-system security management unit (電腦系統安全管理單位), in relation to a CI operator, means a unit maintained by the operator under section 21(1);

computer-system security threat (電腦系統安全威脅), in relation to a critical computer system, means an act (whether known or suspected)—

(a) that is, or is capable of being, done on or through the critical computer system or another computer system; and

(b) the doing of which is likely to have an adverse effect on the computer-system security of the critical computer system;

core function (核心功能), in relation to a critical infrastructure, means—

(a) if the infrastructure falls within paragraph (a) of the definition of ***critical infrastructure*** in this subsection—the provision of the essential service concerned; or

(b) if the infrastructure falls within paragraph (b) of that definition—any function of the infrastructure that is essential to the maintenance of critical societal or economic activities in Hong Kong;

court (法院) means—

(a) a court as defined by section 3 of the Interpretation and General Clauses Ordinance (Cap. 1); or

(b) a magistrate;

critical computer system (關鍵電腦系統) means a computer system designated under section 13;

critical infrastructure (關鍵基礎設施) means—

(a) any infrastructure that is essential to the continuous provision in Hong Kong of an essential service in a sector specified in Schedule 1; or

(b) any other infrastructure the damage, loss of functionality or data leakage of which may hinder or otherwise substantially affect the maintenance of critical societal or economic activities in Hong Kong;

designated authority (指定當局)—see section 5;

designation date (指定日), in relation to a CI operator, means the date on which the operator is designated under section 12;

document (文件) includes—

(a) any input or output, in whatever form, into or from an information system; and

(b) any document, record of information or similar material (whether produced or stored mechanically, electronically, magnetically, optically, manually or by any other means);

function (職能) includes a power and a duty;

information (資料) includes data, text, images, sound codes, computer programs, software, databases, and any combination of them;

information system (資訊系統) has the meaning given by section 2(1) of the Electronic Transactions Ordinance (Cap. 553);

organization (機構) includes a company and any other body corporate;

regulated organization (受規管機構), in relation to a designated authority, means an organization specified in column 4 of Part 2 of Schedule 2 opposite the authority;

regulating authority (規管當局) means the Commissioner or a designated authority;

specified critical infrastructure (指明關鍵基礎設施)—see subsection (3);

tribunal (審裁處) means a tribunal established by or under an Ordinance.

(2) In this Ordinance, a reference to a critical infrastructure operated by a CI operator is a reference to a critical infrastructure in relation to which the operator is designated under section 12.

(3) For the purposes of this Ordinance—

(a) if a critical infrastructure—

(i) is related to a sector specified in column 3 of Part 2 of Schedule 2 opposite a designated authority; and

(ii) is operated by a regulated organization of the authority,

the infrastructure is a specified critical infrastructure for the authority; and

(b) a critical infrastructure is otherwise a specified critical infrastructure for the Commissioner.

(4) For the purposes of this Ordinance—

(a) if a CI operator is a regulated organization of a designated authority, the operator is a CI operator regulated by the authority; or

(b) a CI operator is otherwise a CI operator regulated by the Commissioner,

and a reference to a regulating authority that regulates a CI operator is to be construed accordingly.

(5) For the purposes of this Ordinance, an act (including access to a computer system) is done without lawful authority if the person doing the act—

(a) does so in excess of the person's authority; or

(b) is otherwise not entitled to do so.

Part 2

Regulating Authorities

Division 1—Commissioner

3. Commissioner

(1) For the purposes of this Ordinance, the Chief Executive may appoint a person to be the Commissioner of Critical Infrastructure (Computer-system Security).

(2) The Commissioner is to be appointed for a term of not more than 5 years, but is eligible for reappointment.

(3) The Commissioner is to be entitled to be paid the remuneration and allowances determined by the Secretary for Security.

4. Functions of Commissioner

The functions of the Commissioner are—

(a) to identify critical infrastructures and designate CI operators and critical computer systems;

(b) to issue, revise and maintain codes of practice in respect of category 1 obligations, category 2 obligations and category 3 obligations of CI operators;

(c) to monitor and supervise compliance with the provisions of this Ordinance;

(d) to regulate CI operators with regard to the computer-system security of the critical computer systems of critical infrastructures;

(e) to monitor, investigate and respond to computer-system security threats and computer-system security incidents in

respect of the critical computer systems of critical infrastructures;

(f) to coordinate the implementation of this Ordinance with designated authorities and government departments; and

(g) to perform any other functions imposed or conferred on the Commissioner under this or any other Ordinance.

Division 2—Designated Authorities

5. Designated authorities

For the purposes of this Ordinance, an authority is a designated authority if it is specified in column 2 of Part 2 of Schedule 2.

6. Functions of designated authorities

The functions of a designated authority are—

(a) to identify critical infrastructures regulated by the authority (***subject infrastructures***) and designate CI operators and critical computer systems for such infrastructures;

(b) to issue, revise and maintain codes of practice in respect of category 1 obligations and category 2 obligations of CI operators regulated by the authority (***subject operators***);

(c) to monitor and supervise compliance with category 1 obligations and category 2 obligations;

(d) to regulate subject operators with regard to the computer-system security of the critical computer systems of subject infrastructures to the extent that such regulation relates to category 1 obligations and category 2 obligations;

(e) to facilitate the Commissioner's performance of the Commissioner's functions under this Ordinance; and

(f) to perform any other functions imposed or conferred on the authority under this Ordinance.

Division 3—General Powers of Regulating Authorities

7. Regulating authorities may give directions

(1) The Commissioner—

(a) may, in writing, direct a CI operator regulated by the Commissioner to do, or refrain from doing, an act specified in the direction in relation to the compliance with a category 1 obligation or category 2 obligation if the Commissioner is satisfied that—

(i) the operator has failed to comply with the obligation; or

(ii) the operator's compliance with the obligation is defective; and

(b) may, in writing, direct a CI operator to do, or refrain from doing, an act specified in the direction in relation to the compliance with a category 3 obligation if the Commissioner is satisfied that—

(i) the operator has failed to comply with the obligation; or

(ii) the operator's compliance with the obligation is defective.

(2) A designated authority may, in writing, direct a CI operator regulated by the authority to do, or refrain from doing, an act specified in the direction in relation to the compliance with a category 1 obligation or category 2 obligation if the authority is satisfied that—

(a) the operator has failed to comply with the obligation; or

(b) the operator's compliance with the obligation is defective.

(3) A direction given under subsection (1) or (2) must specify the time within which it has to be complied with.

(4) Without limiting subsections (1) and (2), a direction given under either of those subsections may require the CI operator concerned to revise and resubmit any document that has to be submitted under this Ordinance.

(5) A direction given under subsection (1) or (2) by a regulating authority may be revoked at any time by the authority.

(6) For the purposes of subsections (1)(a)(ii) and (b)(ii) and (2)(b), in considering whether a CI operator's compliance with an obligation is defective, the regulating authority concerned may take into account whether the operator has observed a relevant provision in a code of practice.

(7) If a direction is given by a regulating authority to a CI operator by virtue of subsection (1)(a)(ii) or (b)(ii) or (2)(b), and the operator is able to show to the satisfaction of the authority that—

(a) the operator has done, or is doing, an act in relation to the obligation concerned; and

(b) because of the act, the operator's compliance with the obligation is not defective (whether or not on the ground that a relevant provision in a code of practice is observed),

the authority may, in writing, discharge the direction.

(8) A CI operator commits an offence if the operator fails to comply with a direction given under subsection (1) or (2).

(9) A CI operator that commits an offence under subsection (8) is liable—

(a) on summary conviction—to a fine of $3,000,000 and, in the case of a continuing offence, to a further fine of $60,000 for every day during which the offence continues; or

(b) on conviction on indictment—to a fine of $5,000,000 and, in the case of a continuing offence, to a further fine of $100,000 for every day during which the offence continues.

8. Regulating authorities may issue codes of practice

(1) A regulating authority may issue a code of practice that provides practical guidance on—

(a) if the authority is the Commissioner—

(i) how a CI operator regulated by the Commissioner is to comply with category 1 obligations and category 2 obligations; and

(ii) how a CI operator is to comply with category 3 obligations; or

(b) if the authority is a designated authority—how a CI operator regulated by the authority is to comply with category 1 obligations and category 2 obligations.

(2) A code of practice may include—

(a) a standard; and

(b) a specification.

(3) If a regulating authority issues a code of practice, the authority must—

(a) publish the code on a website of the authority; and

(b) by notice published on a website of the authority—

(i) bring the publication of the code to the attention of those it considers likely to be affected by the code;

(ii) specify the date on which the code is to take effect; and

(iii) specify the purposes for which the code is issued.

(4) A regulating authority may from time to time revise any code of practice issued by the authority.

(5) If a code of practice is revised under subsection (4), the regulating authority must—

(a) publish the code so revised on a website of the authority; and

(b) by notice published on a website of the authority—

(i) bring the revision of the code to the attention of those it considers likely to be affected by the revision;

(ii) specify the date on which the revision is to take effect; and

(iii) specify the purposes of the revision.

(6) A regulating authority may revoke (whether in whole or in part) any code of practice issued by the authority.

(7) If a code of practice is revoked (whether in whole or in part) under subsection (6), the regulating authority must, by notice published on a website of the authority—

(a) bring the revocation to the attention of those it considers likely to be affected by the revocation; and

(b) specify the date on which the revocation is to take effect.

(8) A code of practice is not subsidiary legislation.

(9) To avoid doubt, a regulating authority may under this section issue different codes of practice for different purposes under this Ordinance.

9. Use of codes of practice in legal proceedings

(1) A failure by an organization to observe a provision of a code of practice does not by itself make the organization liable to any civil or criminal proceedings.

(2) Despite subsection (1), if in any legal proceedings the court or appeal board concerned is satisfied that a code of practice (or any part of a code of practice) is relevant to determining a matter that is in issue in the proceedings—

(a) the code (or part of the code) is admissible in evidence in the proceedings; and

(b) proof that the organization contravened or did not contravene a relevant provision of the code may be relied on by a party to the proceedings as tending to establish or negate that matter.

(3) In any legal proceedings, a document purporting to be a copy of a code of practice printed from a website of a regulating authority—

(a) is admissible in evidence on production without further proof; and

(b) unless the contrary is proved, is evidence of the information contained in the document.

(4) In this section—

legal proceedings (法律程序) includes the proceedings of an appeal board.

10. Regulating authorities may specify forms etc.

(1) A regulating authority may specify—

(a) the form of a document or notification required to be provided or made for the purposes of this Ordinance; and

(b) the way in which it is to be provided or made.

(2) A regulating authority may specify—

(a) more than one form under subsection (1)(a); and

(b) more than one way under subsection (1)(b),

whether as alternatives or to provide for different circumstances.

Part 3

Critical Infrastructures, CI Operators and Critical Computer Systems

Division 1—Ascertaining Critical Infrastructures and Designating CI Operators and Critical Computer Systems

11. Ascertaining critical infrastructures

(1) For the purposes of this Ordinance, a regulating authority may ascertain whether an infrastructure is a specified critical infrastructure for the authority.

(2) A regulating authority may, in ascertaining whether an infrastructure is a specified critical infrastructure for the authority, take into account—

(a) what kind of service is provided by the infrastructure;

(b) what implications there can be if the infrastructure is damaged, loses functionality or suffers any data leakage;

(c) any information provided in respect of the infrastructure for compliance with a requirement under Division 2; and

(d) any other matters the authority considers relevant.

12. Designating CI operators

(1) For the purposes of this Ordinance, the Commissioner may, by written notice, designate an organization as a CI operator if—

(a) the organization operates a critical infrastructure; and

(b) the infrastructure is a specified critical infrastructure for the Commissioner.

(2) For the purposes of this Ordinance, a designated authority may, by written notice, designate a regulated organization of the authority as a CI operator if—

(a) the organization operates a critical infrastructure; and

(b) the infrastructure is a specified critical infrastructure for the authority.

(3) To avoid doubt—

(a) more than one CI operator may be designated in relation to a critical infrastructure; and

(b) an organization may be designated as a CI operator for more than one critical infrastructure.

(4) A designation under subsection (1) or (2)—

(a) may be revoked at any time by the regulating authority making it; and

(b) has effect until it is so revoked.

(5) In considering whether to designate an organization as a CI operator or whether to revoke such a designation, a regulating authority may take into account—

(a) how dependent the core function of the critical infrastructure concerned is on computer systems;

(b) the sensitivity of the digital data controlled by the organization in respect of the infrastructure;

(c) the extent of control that the organization has over the operation and management of the infrastructure;

(d) any information provided in respect of the infrastructure for compliance with a requirement under Division 2; and

(e) any other matters the authority considers relevant.

13. Designating critical computer systems

(1) For the purposes of this Ordinance, a regulating authority may, by written notice to a CI operator regulated by the authority, designate a computer system (whether under the control of the operator or not) that—

(a) is accessible by the operator in or from Hong Kong; and

(b) is essential to the core function of a critical infrastructure operated by the operator,

as a critical computer system for the infrastructure.

(2) A designation under subsection (1)—

(a) may be revoked at any time by the regulating authority making it; and

(b) has effect until it is so revoked.

(3) In considering whether to designate a computer system (***subject system***) as a critical computer system or whether to revoke such a designation, a regulating authority may take into account—

(a) the role of the subject system in respect of the core function of the critical infrastructure concerned;

(b) how such a core function would be impacted if the subject system is disrupted or destroyed;

(c) the extent to which the subject system is related to any other computer systems of the CI operator concerned;

(d) the extent to which the subject system and any other computer systems of the operator are related to those of other CI operators;

(e) any information provided in respect of the infrastructure for compliance with a requirement under Division 2; and

(f) any other matters the authority considers relevant.

Division 2—Requiring Information

14. Requiring information for purposes of section 11

(1) For the purposes of section 11, a regulating authority may, by written notice, require an organization that—

(a) operates, or appears to be operating, an infrastructure; or

(b) otherwise has, or appears to have, control over an infrastructure,

to provide any information the authority reasonably considers necessary for ascertaining whether the infrastructure is a specified critical infrastructure for the authority.

(2) An organization to which a notice is given under subsection (1) must provide the information concerned within the time, and in the form and way, specified in the notice.

15. Requiring information for purposes of section 12

(1) For the purposes of section 12, a regulating authority may, by written notice, require an organization that—

(a) operates, or appears to be operating, a critical infrastructure that is a specified critical infrastructure for the authority; or

(b) otherwise has, or appears to have, control over such a critical infrastructure,

to provide any information the authority reasonably considers necessary for considering whether to designate the organization as a CI operator.

(2) For the purposes of section 12, a regulating authority may, by written notice, require a CI operator regulated by the authority to provide any information the authority reasonably considers necessary for considering whether to revoke the operator's designation as a CI operator.

(3) An organization to which a notice is given under subsection (1) or (2) must provide the information concerned within the time, and in the form and way, specified in the notice.

16. Requiring information for purposes of section 13

(1) For the purposes of section 13, a regulating authority may, by written notice, require a CI operator regulated by the authority to provide any information the authority reasonably considers necessary for considering—

(a) whether to designate a computer system as a critical computer system; or

(b) whether to revoke such a designation.

(2) A CI operator to which a notice is given under subsection (1) must provide the information concerned within the time, and in the form and way, specified in the notice.

17. Requiring information for understanding critical computer systems and preparing for threats

(1) The Commissioner—

(a) may, by written notice, require a CI operator regulated by the Commissioner to provide any information the Commissioner reasonably considers necessary for—

(i) better understanding the critical computer systems of the critical infrastructure operated by the operator, so that the Commissioner is able to assess, respond to or prepare for any potential computer-system security threat and computer-system security incident in respect of the critical computer systems of the infrastructure; or

(ii) ascertaining the compliance of the operator with a category 1 obligation or category 2 obligation; and

(b) may, by written notice, require a CI operator to provide any information the Commissioner reasonably considers necessary for ascertaining the compliance of the operator with a category 3 obligation.

(2) A designated authority may, by written notice, require a CI operator regulated by the authority to provide any information the authority reasonably considers necessary for—

(a) better understanding the critical computer systems of the critical infrastructure operated by the operator, so that the authority is able to assess, respond to or prepare for any potential computer-system security threat and computer-system security incident in respect of the critical computer systems of the infrastructure; or

(b) ascertaining the compliance of the operator with a category 1 obligation or category 2 obligation.

(3) A CI operator to which a notice is given under subsection (1) or (2) must provide the information concerned within the time, and in the form and way, specified in the notice.

18. Offence relating to sections 14, 15, 16 and 17

(1) An organization commits an offence if the organization, without reasonable excuse, fails to comply with section 14(2), 15(3), 16(2) or 17(3).

(2) An organization that commits an offence under subsection (1) is liable—

(a) if the organization is a CI operator at the time of the offence—

(i) on summary conviction—to a fine of $3,000,000 and, in the case of a continuing offence, to a further fine of $60,000 for every day during which the offence continues; or

(ii) on conviction on indictment—to a fine of $5,000,000 and, in the case of a continuing offence, to a further fine of $100,000 for every day during which the offence continues; or

(b) in any other case—

(i) on summary conviction—to a fine of $300,000 and, in the case of a continuing offence, to a further fine of $30,000 for every day during which the offence continues; or

(ii) on conviction on indictment—to a fine of $500,000 and, in the case of a continuing offence, to a further fine of $50,000 for every day during which the offence continues.

Part 4

Obligations of CI Operator

Division 1—Obligations relating to Organization of CI Operators

19. Obligation to maintain office in Hong Kong

(1) For the purposes of this Ordinance, a CI operator must—

(a) subject to subsection (2), maintain in Hong Kong an office to which notices and other documents may be given or sent; and

(b) notify, in writing, the regulating authority that regulates the operator of the address of the office (***correspondence address***)—

(i) subject to subparagraph (ii), within 1 month after the operator's designation date (***specified period***); or

(ii) if the specified period is extended under subsection (2)(b)—within the period so extended.

(2) If the CI operator does not already maintain an office in Hong Kong on the operator's designation date—

(a) subsection (1)(a) only applies to the operator—

(i) subject to subparagraph (ii), after the expiry of the specified period; or

(ii) if the specified period is extended under paragraph (b)—after the expiry of the period so extended; and

(b) the regulating authority may, on application by the operator, extend the specified period if the authority is satisfied that the operator has reasonable grounds for needing such an extension.

(3) If the CI operator's correspondence address changes after the operator makes a notification under subsection (1)(b), the operator must, in writing, notify the regulating authority of the change within 1 month after the date on which the change occurs.

(4) A CI operator commits an offence if the operator fails to comply with subsection (1) or (3).

(5) A CI operator that commits an offence under subsection (4) is liable—

(a) on summary conviction—to a fine of $300,000 and, in the case of a continuing offence, to a further fine of $30,000 for every day during which the offence continues; or

(b) on conviction on indictment—to a fine of $500,000 and, in the case of a continuing offence, to a further fine of $50,000 for every day during which the offence continues.

20. Obligation to notify operator changes

(1) A CI operator must, in writing, notify the regulating authority that regulates the operator of any operator change in relation to a critical infrastructure operated by the operator as soon as practicable and in any event within 1 month after the date on which the change occurs.

(2) A CI operator commits an offence if the operator fails to comply with subsection (1).

(3) A CI operator that commits an offence under subsection (2) is liable—

(a) on summary conviction—to a fine of $3,000,000 and, in the case of a continuing offence, to a further fine of $60,000 for every day during which the offence continues; or

(b) on conviction on indictment—to a fine of $5,000,000 and, in the case of a continuing offence, to a further fine of $100,000 for every day during which the offence continues.

(4) In this section—

operator change (營運者變更), in relation to a critical infrastructure, means a change of the organization that operates the infrastructure.

21. Obligation to set up and maintain computer-system security management unit

(1) A CI operator must, subject to subsection (3), maintain a unit (however described) for—

(a) managing the computer-system security of the critical computer systems of the critical infrastructure operated by the operator; and

(b) ensuring that this Ordinance is complied with in relation to the infrastructure.

(2) For the purposes of subsection (1), the CI operator may—

(a) set up and maintain the computer-system security management unit by itself; or

(b) engage a service provider to set up and maintain the unit.

(3) If the CI operator does not already maintain a computer-system security management unit on the operator's designation date, subsection (1) only applies to the operator—

(a) subject to paragraph (b), after the expiry of 1 month after that date (***specified period***); or

(b) if the specified period is extended under subsection (5)—after the expiry of the period so extended.

(4) The CI operator must—

(a) appoint an employee of the operator who has adequate professional knowledge in relation to computer-system security (***adequate knowledge***) to supervise the computer-system security management unit; and

(b) notify, in writing, the regulating authority that regulates the operator of the appointment—

(i) subject to subparagraph (ii), within the specified period; or

(ii) if the specified period is extended under subsection (5)—within the period so extended.

(5) If, on the CI operator's designation date, the operator—

(a) does not already maintain a computer-system security management unit; or

(b) does not already have an employee who has adequate knowledge appointed to supervise such a unit,

the regulating authority may, on application by the operator, extend the specified period if the authority is satisfied that the operator has reasonable grounds for needing such an extension.

(6) If there is any change in respect of an appointment under subsection (4)(a) after it is made, the CI operator must, in writing, notify the regulating authority of the change within 1 month after the date of the change.

(7) A CI operator commits an offence if the operator fails to comply with subsection (4)(b) or (6).

(8) A CI operator that commits an offence under subsection (7) is liable—

(a) on summary conviction—to a fine of $300,000 and, in the case of a continuing offence, to a further fine of $30,000 for every day during which the offence continues; or

(b) on conviction on indictment—to a fine of $500,000 and, in the case of a continuing offence, to a further fine of $50,000 for every day during which the offence continues.

Division 2—Obligations relating to Prevention of Threats and Incidents

22. Obligation to notify material changes to certain computer systems

(1) If any of the events specified in subsection (2) occurs in respect of a critical infrastructure operated by a CI operator, the operator must notify, in the form and way specified under section 10, the regulating authority that regulates the operator of the event within 1 month after the date on which the event occurs.

(2) For the purposes of subsection (1), the events are that—

(a) a material change occurs to the design, configuration, security or operation of a critical computer system of the critical infrastructure;

(b) a critical computer system of the infrastructure is removed;

(c) a computer system (whether under the control of the CI operator or not) that—

(i) is accessible by the operator in or from Hong Kong; and

(ii) is essential to the core function of the infrastructure,

is added to the infrastructure; and

(d) a change occurs to a computer system (whether under the control of the operator or not) that—

(i) is an existing computer system of the infrastructure; and

(ii) is accessible by the operator in or from Hong Kong,

such that the system becomes essential to the core function of the infrastructure.

(3) For the purposes of subsection (2)(a), without limiting the meaning of "material", a change is a material change as described in that subsection if the change—

(a) affects—

(i) the computer-system security of the critical computer system concerned; or

(ii) the ability of the CI operator to respond to a computer-system security threat or computer-system security incident in respect of the system; or

(b) makes any information provided in respect of the system for compliance with a requirement imposed under section 16 no longer accurate in a material particular.

(4) A CI operator commits an offence if the operator fails to comply with subsection (1).

(5) A CI operator that commits an offence under subsection (4) is liable—

(a) on summary conviction—to a fine of $300,000 and, in the case of a continuing offence, to a further fine of $30,000 for every day during which the offence continues; or

(b) on conviction on indictment—to a fine of $500,000 and, in the case of a continuing offence, to a further fine of $50,000 for every day during which the offence continues.

23. Obligation to submit and implement computer-system security management plan

(1) A CI operator must submit to the regulating authority that regulates the operator a plan (however described), prepared in accordance with subsection (3), for protecting the computer-system security of the critical computer systems of the critical infrastructure operated by the operator (***computer-system security management plan***)—

(a) subject to paragraph (b), within 3 months after the operator's designation date (***submission period***); or

(b) if the submission period is extended under subsection (2)—within the period so extended.

(2) The regulating authority may, on application by the CI operator, extend the submission period if the authority is satisfied that the operator has reasonable grounds for needing such an extension.

(3) A computer-system security management plan must cover all of the matters specified in Schedule 3.

(4) If there is any revision to a computer-system security management plan after it is submitted, the CI operator must submit the revised plan to the regulating authority that regulates the operator within 1 month after the date on which the revision is made.

(5) A CI operator must implement a computer-system security management plan.

(6) In subsections (3), (4) and (5), a reference to a computer-system security management plan includes such a plan that is revised.

(7) A CI operator commits an offence if the operator fails to comply with subsection (1) or (4).

(8) A CI operator that commits an offence under subsection (7) is liable—

(a) on summary conviction—to a fine of $300,000 and, in the case of a continuing offence, to a further fine of $30,000 for every day during which the offence continues; or

(b) on conviction on indictment—to a fine of $500,000 and, in the case of a continuing offence, to a further fine of $50,000 for every day during which the offence continues.

24. Obligation to conduct computer-system security risk assessments

(1) A CI operator must—

(a) conduct, in accordance with subsection (3), an assessment in respect of the risks relating to the computer-system security of the critical computer systems of the critical infrastructure operated by the operator (***computer-system security risk assessment***)—

(i) for the first computer-system security risk assessment conducted by the operator—within 12 months after the operator's designation date (***first period***); and

(ii) for any subsequent computer-system security risk assessment—at least once every 12 months after the expiry of the first period; and

(b) submit to the regulating authority that regulates the operator a report for the assessment—

(i) subject to subparagraph (ii), within 3 months after the expiry of the period within which the assessment is required under paragraph (a) to be conducted; or

(ii) if the 3-month period mentioned in subparagraph (i) (***submission period***) is extended under subsection (2)—within the period so extended.

(2) The regulating authority may, on application by the CI operator, extend the submission period if the authority is satisfied that the operator has reasonable grounds for needing such an extension.

(3) A computer-system security risk assessment conducted for compliance with subsection (1) must cover all of the matters specified in Schedule 4 (***Schedule 4 matters***).

(4) Subsection (5) applies if a regulating authority—

(a) receives a notification from a CI operator under section 22(1); or

(b) otherwise becomes aware that any of the events specified in section 22(2) has occurred in respect of a critical infrastructure operated by a CI operator.

(5) The regulating authority may, by written notice, require the CI operator—

(a) to conduct a computer-system security risk assessment in respect of all of the critical computer systems of the critical infrastructure, or any part of such systems specified in the notice; and

(b) to submit to the authority a report for the assessment within the time specified in the notice.

(6) A notice given under subsection (5) must specify the matters that the computer-system security risk assessment required to be conducted has to cover (including any Schedule 4 matters).

(7) To avoid doubt, a computer-system security risk assessment that a CI operator is required to conduct under subsection (5) is not to be regarded as a computer-system security risk assessment for the purposes of subsection (1) unless the regulating authority specifies otherwise in the notice given under subsection (5).

(8) A CI operator commits an offence if the operator fails to comply with subsection (1) or a requirement imposed under subsection (5).

(9) A CI operator that commits an offence under subsection (8) is liable—

(a) on summary conviction—to a fine of $300,000 and, in the case of a continuing offence, to a further fine of $30,000 for every day during which the offence continues; or

(b) on conviction on indictment—to a fine of $500,000 and, in the case of a continuing offence, to a further fine of $50,000 for every day during which the offence continues.

25. Obligation to arrange to carry out computer-system security audits

(1) A CI operator must—

(a) arrange to carry out, in accordance with subsection (3), an audit in respect of the computer-system security of the critical computer systems of the critical infrastructure operated by the operator (***computer-system security audit***)—

(i) for the first computer-system security audit arranged to be carried out—within 24 months after the operator's designation date (***first period***); and

(ii) for any subsequent computer-system security audit—at least once every 24 months after the expiry of the first period; and

(b) submit to the regulating authority that regulates the operator a report for the audit—

(i) subject to subparagraph (ii), within 3 months after the expiry of the period within which the audit is required under paragraph (a) to be carried out; or

(ii) if the 3-month period mentioned in subparagraph (i) (***submission period***) is extended under subsection (2)—within the period so extended.

(2) The regulating authority may, on application by the CI operator, extend the submission period if the authority is satisfied that the operator has reasonable grounds for needing such an extension.

(3) A computer-system security audit carried out for compliance with subsection (1) must—

(a) cover the specified period; and

(b) cover all of the matters specified in Schedule 5 (***Schedule 5 matters***).

(4) If a regulating authority has reasonable grounds to believe that a CI operator regulated by the authority has not properly implemented a computer-system security management plan (including such a plan that is revised) in respect of a critical infrastructure operated by the operator to the satisfaction of the authority, the authority may, by written notice, require the operator—

(a) to arrange to carry out a computer-system security audit for ascertaining whether the plan, or any part of the plan specified in the notice, is properly implemented; and

(b) to submit to the authority a report for the audit within the time specified in the notice.

(5) Subsection (6) applies if a regulating authority—

(a) receives a notification from a CI operator under section 22(1); or

(b) otherwise becomes aware that any of the events specified in section 22(2) has occurred in respect of a critical infrastructure operated by a CI operator.

(6) The regulating authority may, by written notice, require the CI operator—

(a) to arrange to carry out a computer-system security audit in respect of all of the critical computer systems of the critical infrastructure, or any part of such systems specified in the notice; and

(b) to submit to the authority a report for the audit within the time specified in the notice.

(7) A notice given under subsection (4) or (6) must specify—

(a) the period that the computer-system security audit required to be carried out has to cover; and

(b) the matters that the audit has to cover (including any Schedule 5 matters).

(8) For the purposes of this section, a computer-system security audit is not to be regarded as carried out unless it is carried out by an independent auditor.

(9) To avoid doubt, a computer-system security audit that a CI operator is required to arrange to be carried out under subsection (4) or (6) is not to be regarded as a computer-system security audit for the purposes of subsection (1) unless the regulating authority specifies otherwise in the notice given under subsection (4) or (6).

(10) A CI operator commits an offence if the operator fails to comply with subsection (1) or a requirement imposed under subsection (4) or (6).

(11) A CI operator that commits an offence under subsection (10) is liable—

(a) on summary conviction—to a fine of $300,000 and, in the case of a continuing offence, to a further fine of $30,000 for every day during which the offence continues; or

(b) on conviction on indictment—to a fine of $500,000 and, in the case of a continuing offence, to a further fine of $50,000 for every day during which the offence continues.

(12) In this section—

specified period (指明期間)—

(a) in relation to a computer-system security audit that falls within subsection (1)(a)(i)—means the first period; or

(b) in relation to a computer-system security audit that falls within subsection (1)(a)(ii)—means the 24-month period for carrying out the audit as determined in accordance with that subsection.

Division 3—Obligations relating to Incident Reporting and Response

26. Obligation to participate in computer-system security drill

(1) The Commissioner may conduct a drill (however described) for testing the state of readiness of CI operators in responding to computer-system security incidents in respect of the critical computer systems of critical infrastructures (***computer-system security drill***).

(2) For the purposes of subsection (1), the Commissioner may, after giving reasonable notice in writing, require a CI operator to participate in a computer-system security drill.

(3) A CI operator commits an offence if the operator fails to comply with a requirement imposed under subsection (2).

(4) A CI operator that commits an offence under subsection (3) is liable—

(a) on summary conviction—to a fine of $3,000,000; or

(b) on conviction on indictment—to a fine of $5,000,000.

27. Obligation to submit and implement emergency response plan

(1) A CI operator must submit to the Commissioner a plan (however described), prepared in accordance with subsection (3), detailing the protocol for the operator's response to computer-system security incidents in respect of the critical computer systems of critical infrastructures (***emergency response plan***)—

(a) subject to paragraph (b), within 3 months after the operator's designation date (***submission period***); or

(b) if the submission period is extended under subsection (2)—within the period so extended.

(2) The Commissioner may, on application by the CI operator, extend the submission period if the Commissioner is satisfied that the operator has reasonable grounds for needing such an extension.

(3) An emergency response plan must cover all of the matters specified in Part 2 of Schedule 3.

(4) If there is any revision to an emergency response plan after it is submitted, the CI operator must submit the revised plan to the Commissioner within 1 month after the date on which the revision is made.

(5) A CI operator must implement an emergency response plan.

(6) In subsections (3), (4) and (5), a reference to an emergency response plan includes such a plan that is revised.

(7) A CI operator commits an offence if the operator fails to comply with subsection (1) or (4).

(8) A CI operator that commits an offence under subsection (7) is liable—

(a) on summary conviction—to a fine of $300,000 and, in the case of a continuing offence, to a further fine of $30,000 for every day during which the offence continues; or

(b) on conviction on indictment—to a fine of $500,000 and, in the case of a continuing offence, to a further fine of $50,000 for every day during which the offence continues.

28. Obligation to notify computer-system security incidents

(1) If a CI operator becomes aware that a computer-system security incident has occurred in respect of a critical computer system of a critical infrastructure operated by the operator, the operator must notify the Commissioner of the incident in accordance with subsection (2).

(2) The notification—

(a) must be made as soon as practicable and in any event within the specified time; and

(b) must—

(i) be made in the form and way specified under section 10 (***specified form and way***); or

(ii) despite not being made in the specified form and way, include information on the nature of the computer-system security incident and identify the critical computer system concerned.

(3) If the notification is not made in the specified form and way, the CI operator must subsequently submit a written record of the computer-system security incident concerned in the specified form and way to the Commissioner within the specified time.

(4) After a CI operator makes a notification of a computer-system security incident under subsection (1) in the specified form and way, or submits a written record of such an incident under subsection (3), the CI operator must further submit a written report of the incident in the specified form and way to the Commissioner within the specified time.

(5) A CI operator commits an offence if the operator fails to comply with subsection (1), (3) or (4).

(6) A CI operator that commits an offence under subsection (5) is liable—

(a) on summary conviction—to a fine of $3,000,000; or

(b) on conviction on indictment—to a fine of $5,000,000.

(7) In this section—

specified time (指明時限), in relation to a provision of this section specified in column 2 of Schedule 6, means the time specified in column 3 of that Schedule opposite the provision.

Part 5

Responding to Computer-system Security Threats and Computer-system Security Incidents

Division 1—Early Intervention

29. Commissioner may direct inquiries to identify computer-system security threats and computer-system security incidents

If the Commissioner reasonably suspects that an event that has an actual adverse effect, or is likely to have an adverse effect, on the computer-system security of a critical computer system of a critical infrastructure has occurred, the Commissioner may direct an authorized officer of the Commissioner to make inquiries for the purpose of identifying—

(a) what caused the event; and

(b) whether a computer-system security threat or a computer-system security incident has occurred in respect of the system.

30. Powers of authorized officers of Commissioner in making inquiries

(1) For making inquiries under section 29, an authorized officer of the Commissioner may, by written notice, require the CI operator by which the critical infrastructure concerned is operated—

(a) to produce, within the time and at the place specified in the notice, any document so specified that the officer has reasonable grounds to believe—

(i) to be relevant, or likely to be relevant, to the inquiries; and

(ii) to be in the possession, or under the control, of the operator, or otherwise accessible in or from Hong Kong by the operator;

(b) to give an explanation or further particulars in relation to the document;

(c) to send a representative to attend before the officer at the time and place specified in the notice, and to answer a question relating to any matter under investigation that is raised by the officer; and

(d) to answer in writing, within the time specified in the notice, a written question relating to any matter under investigation that is raised by the officer.

(2) If a document is produced for compliance with a requirement imposed under subsection (1), the authorized officer may for making the inquiries inspect, make copies of, take extracts from and take possession of the document.

31. Magistrate's warrants for entering premises for early intervention

(1) Subsection (2) applies if a magistrate is satisfied by information on oath laid by an authorized officer of the Commissioner that—

(a) there are reasonable grounds to suspect that there is, or is likely to be, on any premises any document that is relevant to inquiries made under section 30; and

(b) both of the conditions specified in section 32 are met in relation to the inquiries.

(2) The magistrate may issue a warrant authorizing an authorized officer of the Commissioner, and any other person whose assistance is necessary for the execution of the warrant—

(a) to enter the premises, if necessary by force, at any time within—

(i) subject to subparagraph (ii), a period of 7 days; or

(ii) if any longer period is specified in the warrant—such a period,

beginning on the date of the warrant; and

(b) to search for, inspect, make copies of, take extracts from, seize and remove any document on the premises that the officer has reasonable grounds to believe to be relevant, or likely to be relevant, to the inquiries.

32. Conditions for issuing warrants

For the purposes of section 31(1)(b), the conditions are that—

(a) there are reasonable grounds to believe that the CI operator concerned is unwilling or unable to take all reasonable steps to respond to the inquiries; and

(b) there are reasonable grounds to believe that it is in the public interest to issue the warrant, having regard to—

(i) the potential harm that could be caused by the event mentioned in section 29 to the critical infrastructure concerned;

(ii) the potential disruption that could be caused by the event to the core function of the infrastructure;

(iii) whether or not the purpose mentioned in section 29 could be effectively achieved if the warrant is not issued;

(iv) the benefits likely to accrue from doing the acts to be authorized by the warrant; and

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

Division 2—Computer-system Security Investigations

33. Interpretation

In this Division—

computer-system security investigation (電腦系統安全調查) means an investigation carried out under section 34 and includes any response made under that section;

investigated CI operator (被調查的關鍵基礎設施營運者), in relation to a computer-system security investigation, means the CI operator that is the subject of the investigation;

investigated system (被調查系統), in relation to a computer-system security investigation, means the critical computer system in respect of which the investigated threat or incident has occurred;

investigated threat or incident (被調查的威脅或事故), in relation to a computer-system security investigation, means the computer-system security threat or computer-system security incident that is the subject of the investigation.

34. Commissioner may direct investigations to be carried out in relation to computer-system security threats or computer-system security incidents

If the Commissioner reasonably suspects that a computer-system security threat or computer-system security incident has occurred in respect of a critical computer system of a critical infrastructure, the Commissioner may direct an authorized officer of the Commissioner to carry out an investigation into, and to respond to, the threat or incident for the following purposes—

(a) identifying what caused the threat or incident;

(b) assessing the impact, or potential impact, of the threat or incident;

(c) remedying any harm that has arisen from the threat or incident;

(d) preventing any, or any further, harm from arising from the threat or incident;

(e) preventing any, or any further, computer-system security incident from arising from the threat or incident.

35. Powers of authorized officers of Commissioner in investigations

(1) For carrying out a computer-system security investigation, an authorized officer of the Commissioner may, by written notice, require the investigated CI operator to do one or more of the following acts—

(a) to produce, within the time and at the place specified in the notice, any document so specified that the officer has reasonable grounds to believe—

(i) to be relevant, or likely to be relevant, to the investigation; and

(ii) to be in the possession, or under the control, of the operator, or otherwise accessible in or from Hong Kong by the operator;

(b) to give an explanation or further particulars in relation to the document;

(c) to send a representative to attend before the officer at the time and place specified in the notice, and to answer a question relating to any matter under investigation that is raised by the officer;

(d) to answer in writing, within the time specified in the notice, a written question relating to any matter under investigation that is raised by the officer.

(2) If a document is produced for compliance with a requirement imposed under subsection (1), the authorized officer may for carrying out the investigation inspect, make copies of, take extracts from and take possession of the document.

36. Additional power of authorized officer of Commissioner

(1) Without limiting section 35, for carrying out a computer-system security investigation, the Commissioner may further authorize an authorized officer of the Commissioner to exercise the power specified in subsection (2) if the Commissioner is satisfied that—

(a) there are reasonable grounds to believe that the investigated CI operator is unwilling or unable to take all reasonable steps to assist in the investigation or respond to the investigated threat or incident; and

(b) there are reasonable grounds to believe that it is in the public interest to make the further authorization, having regard to—

(i) the potential harm that could be caused by the investigated threat or incident to the critical infrastructure concerned;

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

(iii) whether or not the purposes mentioned in section 34 could be effectively achieved if the further authorization is not made;

(iv) the benefits likely to accrue from exercising the power; and

(v) the potential impact of exercising the power on the core function of the infrastructure and on the operator.

(2) For the purposes of subsection (1), the power is to, by written notice, require the investigated CI operator to do one or more of the following acts—

(a) not to use the investigated system;

(b) to preserve the state of the system;

(c) to monitor the system;

(d) to perform a scan of the system in order to—

(i) detect any vulnerabilities of the system; and

(ii) assess the impact of the investigated threat or incident or of a potential computer-system security incident in respect of the system;

(e) to carry out any remedial measures, or to cease carrying on any activities, in relation to the investigated threat or incident;

(f) to give the authorized officer all other assistance in connection with the computer-system security investigation that the operator is reasonably able to give.

37. Magistrate's warrants for imposing requirements on organizations other than investigated CI operators

(1) Subsection (2) applies if a magistrate is satisfied by information on oath laid by an authorized officer of the Commissioner that both of the conditions specified in section 39 are met in relation to a computer-system security investigation.

(2) The magistrate may issue a warrant authorizing an authorized officer of the Commissioner, and any other person whose assistance is necessary for the execution of the warrant, to require by written notice, for carrying out the computer-system security investigation, an organization having, or appearing to have, control over the investigated system (other than the investigated CI operator) to do one or more of the following acts—

(a) to produce, within the time and at the place specified in the notice, any document so specified that the officer has reasonable grounds to believe—

(i) to be relevant, or likely to be relevant, to the investigation; and

(ii) to be in the possession, or under the control, of the organization, or otherwise accessible in or from Hong Kong by the organization;

(b) to give an explanation or further particulars in relation to the document;

(c) to send a representative to attend before the officer at the time and place specified in the notice, and to answer a question relating to any matter under investigation that is raised by the officer;

(d) to answer in writing, within the time specified in the notice, a written question relating to any matter under investigation that is raised by the officer;

(e) not to use the system;

(f) to preserve the state of the system;

(g) to monitor the system;

(h) to perform a scan of the system in order to—

(i) detect any vulnerabilities of the system; and

(ii) assess the impact of the investigated threat or incident or of a potential computer-system security incident in respect of the system;

(i) to carry out any remedial measures, or to cease carrying on any activities, in relation to the threat or incident;

(j) to give the officer all other assistance in connection with the investigation that the organization is reasonably able to give.

(3) If a document is produced for compliance with a requirement imposed under the warrant, the authorized officer may for carrying out the investigation inspect, make copies of, take extracts from and take possession of the document.

38. Magistrate's warrants for entering premises for computer-system security investigations

(1) Subsection (2) applies if a magistrate is satisfied by information on oath laid by an authorized officer of the Commissioner that—

(a) there are reasonable grounds to suspect that—

(i) there is, or is likely to be, on any premises anything that is relevant to a computer-system security investigation; or

(ii) the investigated system of a computer-system security investigation is, or is likely to be, located on certain premises; and

(b) both of the conditions specified in section 39 are met in relation to the investigation.

(2) The magistrate may issue a warrant authorizing an authorized officer of the Commissioner, and any other person whose assistance is necessary for the execution of the warrant, to do

one or more of the following acts for carrying out the computer-system security investigation—

(a) to enter the premises, if necessary by force, at any time within—

(i) subject to subparagraph (ii), a period of 7 days; or

(ii) if any longer period is specified in the warrant—such a period,

beginning on the date of the warrant;

(b) to search for, inspect, make copies of, take extracts from, seize and remove anything on the premises that the officer has reasonable grounds to believe to be relevant, or likely to be relevant, to the investigation;

(c) to, for the purposes mentioned in section 34, access and inspect, and carry out any remedial measures in relation to, the investigated system or another computer system (***accessible system***)—

(i) that is accessible via the investigated system; and

(ii) that the officer has reasonable grounds to believe to be relevant, or likely to be relevant, to the investigation;

(d) to search for, inspect, make copies of and take extracts from any information—

(i) that is stored in the investigated system or an accessible system; and

(ii) that the officer has reasonable grounds to believe to be relevant, or likely to be relevant, to the investigation;

(e) to carry out any other remedial measures in relation to the threat or incident;

(f) to require an organization having, or appearing to have, control over the investigated system to give all other assistance—

(i) that is reasonably necessary to facilitate the officer's performance of functions for the investigation; and

(ii) that the organization is reasonably able to give.

39. Conditions for issuing warrants

For the purposes of sections 37(1) and 38(1)(b), the conditions are that—

(a) there are reasonable grounds to believe that—

(i) for section 37(1)—the investigated CI operator is unwilling or unable to take all reasonable steps to assist in the computer-system security investigation or respond to the investigated threat or incident; or

(ii) for section 38(1)(b)—

(A) the investigated CI operator;

(B) the organization mentioned in section 37(2); or

(C) both the investigated CI operator and the organization mentioned in section 37(2),

as the case requires, is or are unwilling or unable to take all reasonable steps to assist in the computer-system security investigation or respond to the investigated threat or incident; and

(b) there are reasonable grounds to believe that it is in the public interest to issue the warrant, having regard to—

(i) the potential harm that could be caused by the investigated threat or incident to the critical infrastructure concerned;

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

(iii) whether or not the purposes mentioned in section 34 could be effectively achieved if the warrant is not issued;

(iv) the benefits likely to accrue from doing the acts to be authorized by the warrant; and

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

40. Power of entry in emergencies

(1) For carrying out a computer-system security investigation, the Commissioner may, if satisfied that all of the conditions specified in subsection (2) are met in relation to the investigation, authorize an authorized officer of the Commissioner to enter any premises and do one or more of the acts specified in section 38(2) (other than the act specified in section 38(2)(a)) (***specified acts***) without warrant.

(2) For the purposes of subsection (1), the conditions are that—

(a) there are reasonable grounds to suspect that—

(i) there is, or is likely to be, on the premises anything that is relevant to the computer-system security investigation; or

(ii) the investigated system is, or is likely to be, located on the premises;

(b) there are reasonable grounds to believe that—

(i) the investigated CI operator;

(ii) the organization mentioned in section 37(2); or

(iii) both the investigated CI operator and the organization mentioned in section 37(2),

as the case requires, is or are unwilling or unable to take all reasonable steps to assist in the computer-system security investigation or respond to the investigated threat or incident;

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

(d) there are reasonable grounds to believe that it is in the public interest to make the entry and do the specified acts, having regard to—

(i) the potential harm that could be caused by the investigated threat or incident to the critical infrastructure concerned;

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

(iii) whether or not the purposes mentioned in section 34 could be effectively achieved if the entry is not made and the acts are not done;

(iv) the benefits likely to accrue from making the entry and doing the acts; and

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

(3) The authorized officer entering the premises must, if requested, produce the Commissioner's authorization for inspection.

Division 3—Supplementary Provisions

41. Use of incriminating evidence in proceedings after early interventions and computer-system security investigations

(1) If a person is to give an explanation or further particulars to an authorized officer, or to answer a question posed by such an officer, for compliance with a specified requirement, the officer must ensure that the person has first been informed or reminded of the limitations imposed by subsection (2) on the admissibility in evidence of the requirement and of the explanation or particulars, or the question and answer.

(2) Despite any other provision in this Ordinance, if—

(a) a person gives an explanation or further particulars to an authorized officer, or answers a question posed by such an officer, for compliance with a specified requirement;

(b) the explanation, particulars or answer might tend to incriminate the person; and

(c) the person claims, before giving the explanation or particulars, or answering the question, that the explanation, particulars or answer might so tend,

the requirement, as well as the explanation or particulars, or the question and answer, are not admissible in evidence against the person in criminal proceedings in a court other than those specified in subsection (3).

(3) The criminal proceedings are those in which the person is charged with—

(a) an offence under section 42; or

(b) an offence under Part V of the Crimes Ordinance (Cap. 200).

(4) In this section—

section 37 or 38 warrant (第 37 或 38 條手令) means a warrant issued under section 37 or 38;

specified requirement (指明要求) means a requirement—

(a) imposed under Division 1 or 2; or

(b) imposed under a section 37 or 38 warrant.

42. Offences relating to Divisions 1 and 2 of Part 5

(1) An organization commits an offence if the organization, without reasonable excuse, fails to comply with a specified requirement.

(2) For the purposes of subsection (1), the fact that complying with a specified requirement might tend to result in self-incrimination is not an excuse not to comply with the requirement.

(3) An organization that commits an offence under subsection (1) is liable—

(a) on summary conviction—to a fine of $300,000; or

(b) on conviction on indictment—to a fine of $500,000.

(4) In this section—

section 37 or 38 warrant (第 37 或 38 條手令) means a warrant issued under section 37 or 38;

specified requirement (指明要求) means a requirement—

(a) imposed under Division 1 or 2; or

(b) imposed under a section 37 or 38 warrant.

Part 6

Investigation of Offences

43. Regulating authorities may direct offences to be investigated

(1) Subsection (2) applies if a regulating authority reasonably suspects—

(a) if the authority is the Commissioner—that an offence under this Ordinance has been, or is being, committed; or

(b) if the authority is a designated authority—that any of the following offences has been, or is being, committed—

(i) an offence under section 7 for a failure to comply with a direction given by the authority;

(ii) an offence under section 18 for a failure to comply with a requirement imposed by the authority;

(iii) an offence under Division 1 or 2 of Part 4 for a failure to comply with a category 1 obligation or category 2 obligation by a CI operator regulated by the authority.

(2) The regulating authority may direct an authorized officer of the authority to carry out an investigation into the offence and, for this purpose, to require by written notice an organization to do one or more of the following acts—

(a) to produce, within the time and at the place specified in the notice, any document so specified that the officer has reasonable grounds to believe—

(i) to be relevant, or likely to be relevant, to the investigation; and

(ii) to be in the possession, or under the control, of the organization, or otherwise accessible in or from Hong Kong by the organization;

(b) to give an explanation or further particulars in relation to the document;

(c) to send a representative to attend before the officer at the time and place specified in the notice, and to answer a question relating to any matter under investigation that is raised by the officer;

(d) to answer in writing, within the time specified in the notice, a written question relating to any matter under investigation that is raised by the officer.

(3) If a document is produced for compliance with a requirement imposed under subsection (2), the authorized officer may for carrying out the investigation inspect, make copies of, take extracts from and take possession of the document.

44. Use of incriminating evidence in proceedings after investigations

(1) If a person is to give an explanation or further particulars to an authorized officer, or to answer a question posed by such an officer, for compliance with a requirement imposed under section 43, the officer must ensure that the person has first been informed or reminded of the limitations imposed by subsection (2) on the admissibility in evidence of the requirement and of the explanation or particulars, or the question and answer.

(2) Despite any other provision in this Ordinance, if—

(a) a person gives an explanation or further particulars to an authorized officer, or answers a question posed by such an officer, for compliance with a requirement imposed under section 43;

(b) the explanation, particulars or answer might tend to incriminate the person; and

(c) the person claims, before giving the explanation or particulars, or answering the question, that the explanation, particulars or answer might so tend,

the requirement, as well as the explanation or particulars, or the question and answer, are not admissible in evidence against the person in criminal proceedings in a court other than those specified in subsection (3).

(3) The criminal proceedings are those in which the person is charged with—

(a) an offence under section 45; or

(b) an offence under Part V of the Crimes Ordinance (Cap. 200).

45. Offence relating to section 43

(1) An organization commits an offence if the organization, without reasonable excuse, fails to comply with a requirement imposed under section 43.

(2) For the purposes of subsection (1), the fact that complying with a requirement imposed under section 43 might tend to result in self-incrimination is not an excuse not to comply with the requirement.

(3) An organization that commits an offence under subsection (1) is liable—

(a) on summary conviction—to a fine of $300,000; or

(b) on conviction on indictment—to a fine of $500,000.

46. Magistrate's warrants for entering premises or accessing electronic devices for investigations into offences

(1) Subsection (2) applies if a magistrate is satisfied by information on oath laid by an authorized officer of a regulating authority that there are reasonable grounds to suspect that there is, or is likely to be, anything—

(a) that—

(i) is located on any premises; or

(ii) is stored in, or accessible via, any electronic device; and

(b) that is or contains, or is likely to be or to contain, evidence of an offence being investigated under this Part (***investigated offence***).

(2) The magistrate may issue a warrant authorizing an authorized officer of the regulating authority, and any other person whose assistance is necessary for the execution of the warrant, to do one or more of the following acts for carrying out the investigation—

(a) in relation to premises—

(i) to enter the premises, if necessary by force;

(ii) to search for, inspect, seize and remove anything on the premises that the officer has reasonable grounds to believe is or contains, or is likely to be or to contain, evidence of the investigated offence;

(b) in relation to an electronic device—

(i) to access and inspect the device;

(ii) to search for, inspect, make copies of and take extracts from any information—

(A) that is stored in, or accessible via, the device; and

(B) that the officer has reasonable grounds to believe is or contains, or is likely to be or to contain, evidence of the investigated offence.

(3) The acts specified in subsection (2) may only be done at any time within—

(a) subject to paragraph (b), a period of 7 days; or

(b) if any longer period is specified in the warrant—such a period,

beginning on the date of the warrant concerned.

Part 7

Appeals

47. Appeal panel

(1) For handling appeals under this Part, there is to be an appeal panel.

(2) Part 2 of Schedule 7 has effect with respect to the appeal panel.

48. Appeals against decisions

(1) An organization aggrieved by any of the following decisions made in relation to the organization may lodge an appeal against the decision—

(a) a decision to give a direction under section 7;

(b) a decision to make a designation under section 12;

(c) a decision to make a designation under section 13;

(d) a decision to impose a requirement under section 24(5);

(e) a decision to impose a requirement under section 25(4) or (6).

(2) Part 3 of Schedule 7 has effect with respect to the appeal.

(3) Subject to subsections (4) and (5), the lodging of an appeal under subsection (1) against a decision does not by itself operate as a stay of execution of the decision.

(4) An organization that lodges an appeal under subsection (1) against a decision may, at any time before the appeal is determined by the appeal board appointed for the appeal, apply to the board for a stay of execution of the decision.

(5) The appeal board must, as soon as reasonably practicable after receiving an application under subsection (4), determine the application.

(6) The appeal board may by order grant the stay subject to any condition as to costs, payment of money into the board or other matters that the board considers appropriate.

49. Decisions of appeal board

(1) An appeal board appointed for an appeal may—

(a) confirm, vary or reverse any decision to which the appeal relates; or

(b) give any direction in relation to the decision as the board considers appropriate.

(2) The appeal board must give reasons in writing for its decision.

(3) The appeal board must serve a copy of its decision and of the reasons for its decision on the parties to the appeal.

(4) The appeal board's decision takes effect—

(a) subject to paragraph (b), immediately after the decision is made; or

(b) if the board orders that its decision is not to come into operation until a specified date—on that date.

(5) A document purporting to be a copy of a decision or order of the appeal board and to be certified by the chairperson of the board to be a true copy of the decision or order is admissible in any proceedings as evidence of the decision or order.

(6) The decision of the appeal board is final.

Part 8

Miscellaneous

50. Appointment of authorized officers by Commissioner

(1) The Commissioner may, in writing, appoint a public officer to perform any function conferred or imposed by this Ordinance on an authorized officer of the Commissioner.

(2) The Commissioner must provide the appointed authorized officer with a copy of the appointment.

(3) The Commissioner may perform a function mentioned in subsection (1) as if the Commissioner were an authorized officer appointed under that subsection.

51. Appointment of authorized officers by designated authority

(1) A designated authority may, in writing, appoint—

(a) a public officer;

(b) a person employed—

(i) by the authority; or

(ii) otherwise in connection with the authority's performance of a function under this Ordinance; or

(c) with the consent of the Secretary for Security, any other person or class of persons,

to perform any function conferred or imposed by this Ordinance on an authorized officer of the authority.

(2) The designated authority must provide the appointed authorized officer with a copy of the appointment.

(3) A designated authority may perform a function mentioned in subsection (1) as if the authority were an authorized officer appointed under that subsection.

52. Delegation of functions by Commissioner and designated authorities

(1) The Commissioner may, in writing, delegate to a public officer any of the Commissioner's functions under this Ordinance.

(2) A designated authority may, in writing, delegate to—

(a) a public officer; or

(b) a person employed—

(i) by the authority; or

(ii) otherwise in connection with the authority's performance of a function under this Ordinance,

any of the authority's functions under this Ordinance.

(3) However, the power to delegate conferred by subsection (1) or (2) may not be delegated.

53. Performance of functions

(1) When performing a function under this Ordinance, a specified officer—

(a) may be assisted by any person whom the officer reasonably requires; and

(b) must produce evidence of the officer's appointment or delegation (as the case requires), and the relevant warrant (if any), for inspection by a person who is affected by the performance of the function and requires to see them.

(2) In this section—

specified officer (指明人員) means—

(a) an authorized officer; or

(b) a person to whom any function is delegated under section 52.

54. Commissioner may perform functions in respect of critical infrastructures and CI operators regulated by designated authorities if necessary

(1) Any function that may be performed under a provision of this Ordinance by a designated authority in respect of a critical infrastructure that is a specified critical infrastructure for the authority, or a CI operator regulated by the authority, may be performed by the Commissioner as if the Commissioner were the designated authority.

(2) However, the Commissioner must not perform the function unless the Commissioner is satisfied that—

(a) it is necessary to do so for the timely protection of the critical computer systems of the critical infrastructure concerned; or

(b) it is otherwise necessary in the public interest to do so.

55. Commissioner may exempt CI operators

(1) The Commissioner may, by written notice (***exemption notice***), exempt a CI operator from a category 1 obligation, category 2 obligation or category 3 obligation (***subject obligation***) if the Commissioner is satisfied that it is in the public interest to so exempt the operator.

(2) An exemption notice is not subsidiary legislation.

(3) In considering whether it is in the public interest to exempt a CI operator under subsection (1), the Commissioner may take into account—

(a) whether the operator has done, or is doing, an act that can achieve the same purpose as the compliance with the subject obligation; and

(b) whether—

(i) the operator is subject to an obligation (***alternative obligation***) that—

(A) is imposed by or under another Ordinance, or any code of practice, direction or requirement (however described); and

(B) corresponds substantially to the subject obligation; and

(ii) the operator's compliance with the alternative obligation achieves the same purpose as the compliance with the subject obligation.

(4) An exemption under subsection (1)—

(a) is in force for a period the Commissioner considers appropriate and specifies in the exemption notice; and

(b) is subject to any condition the Commissioner considers appropriate.

(5) The Commissioner may, by written notice (***revocation notice***), revoke an exemption under subsection (1) if the Commissioner is satisfied that—

(a) a condition of the exemption has been contravened; or

(b) it is no longer in the public interest to exempt the CI operator concerned under that subsection.

(6) A revocation notice is not subsidiary legislation.

(7) If an exemption is revoked under subsection (5)—

(a) the Commissioner must specify in the revocation notice—

(i) the date on which the revocation is to take effect (***revocation date***); and

(ii) (if applicable) how and by when the CI operator is to comply with the obligation covered by the exemption; and

(b) the provision imposing the obligation is to apply, on and after the revocation date, to the operator with necessary modifications having regard to the revocation notice.

(8) The Commissioner may, by written notice, require a CI operator to provide any information the Commissioner reasonably considers necessary for considering whether to exempt the operator under subsection (1) or whether to revoke such an exemption under subsection (5).

(9) A CI operator to whom a notice is given under subsection (8) must provide the information concerned within the time, and in the form and way, specified in the notice.

56. Designated authorities may prosecute offences

(1) A designated authority may prosecute any of the following offences in the name of the authority—

(a) an offence under section 7 for a failure to comply with a direction given by the authority;

(b) an offence under section 18 for a failure to comply with a requirement imposed by the authority;

(c) an offence under Division 1 or 2 of Part 4 for a failure to comply with a category 1 obligation or category 2 obligation by a CI operator regulated by the authority;

(d) an offence under section 45 for a failure to comply with a requirement imposed by an authorized officer of the authority;

(e) an offence of conspiracy to commit an offence mentioned in paragraph (a), (b), (c) or (d).

(2) Any offence prosecuted under subsection (1) must be tried before a magistrate as an offence that is triable summarily.

(3) For prosecuting an offence mentioned in subsection (1) only, an authorized officer of the designated authority concerned, even if the officer is not qualified to practise as a barrister or to act as a solicitor under the Legal Practitioners Ordinance (Cap. 159)—

(a) may appear and plead before a magistrate in any case of which the officer has charge; and

(b) has, in relation to the prosecution, all the other rights of a person qualified to practise as a barrister or to act as a solicitor under that Ordinance.

(4) This section does not derogate from the powers of the Secretary for Justice in respect of the prosecution of criminal offences.

57. Preservation of secrecy

(1) Except in the performance of any function under this Ordinance or for carrying into effect the provisions of this Ordinance, a specified person—

(a) must not suffer or permit any person to have access to any matter relating to the affairs of any person that comes to the specified person's knowledge in connection with the performance of any function under this Ordinance; and

(b) must not communicate any such matter to any person other than the person to whom such matter relates.

(2) Despite subsection (1), a specified person may—

(a) disclose information that has already been made available to the public;

(b) disclose information for the purposes of any criminal proceedings in Hong Kong or an investigation conducted with a view to bringing any such proceedings;

(c) disclose information for seeking advice from, or giving advice by, any counsel, solicitor or other professional adviser, acting or proposing to act in a professional capacity in connection with any matter arising under this Ordinance;

(d) disclose information in connection with any judicial or other proceedings to which the specified person is a party; and

(e) disclose information in accordance with an order of a court or tribunal, or in accordance with a law or a requirement made under a law.

(3) Despite subsection (1), a regulating authority may—

(a) subject to subsection (4), disclose information to—

(i) the Chief Executive;

(ii) the Chief Secretary for Administration;

(iii) the Financial Secretary;

(iv) the Secretary for Justice;

(v) the Secretary for Security;

(vi) the Commissioner of Police of Hong Kong;

(vii) the Commissioner of the Independent Commission Against Corruption;

(viii) the Privacy Commissioner for Personal Data established under section 5(1) of the Personal Data (Privacy) Ordinance (Cap. 486);

(ix) a tribunal; or

(x) a public officer authorized under subsection (9);

(b) disclose information with the consent of—

(i) the person from whom the information was obtained or received; and

(ii) if the information does not relate to such person—the person to whom it relates; and

(c) disclose information in summary form that is so framed as to prevent particulars relating to any person from being ascertained from it.

(4) A regulating authority must not disclose information under subsection (3)(a) unless the authority is of the opinion that—

(a) the disclosure will enable or assist the recipient of the information to perform the recipient's functions; and

(b) it is not contrary to the public interest for the information to be so disclosed.

(5) Subject to subsection (6), if information is disclosed under subsection (1), (2) or (3) (other than subsection (2)(a) or (3)(c))—

(a) the person to whom the information is so disclosed; or

(b) any other person obtaining or receiving the information from that person,

must not disclose the information to any other person.

(6) Subsection (5) does not prohibit the person referred to in subsection (5)(a) or (b) from disclosing the information to any other person if—

(a) the regulating authority disclosing the information consents to the disclosure;

(b) the information has already been made available to the public;

(c) the disclosure is for the purpose of seeking advice from, or giving advice by, any counsel, solicitor or other professional adviser, acting or proposing to act in a professional capacity in connection with any matter arising under this Ordinance;

(d) the disclosure is in connection with any judicial or other proceedings to which the person so referred to is a party; or

(e) the disclosure is in accordance with an order of a court or tribunal, or in accordance with a law or a requirement made under a law.

(7) A regulating authority may attach any condition that it considers appropriate to—

(a) a disclosure of information made by it under subsection (3); or

(b) a consent granted by it under subsection (6)(a).

(8) Subsection (1) does not affect section 13(3) of The Ombudsman Ordinance (Cap. 397) or section 44(8) of the Personal Data (Privacy) Ordinance (Cap. 486).

(9) The Secretary for Security may authorize any public officer as a person to whom information may be disclosed under subsection (3)(a)(x).

(10) In this section—

related person (有關連人士), in relation to a regulating authority, means—

(a) a person employed—

(i) by the authority; or

(ii) otherwise in connection with the authority's performance of a function under this Ordinance; or

(b) a person appointed—

(i) as a consultant, agent or adviser of the authority for this Ordinance; or

(ii) otherwise in connection with the authority's performance of a function under this Ordinance;

specified person (指明人士) means a person who is or has been—

(a) a regulating authority;

(b) an authorized officer;

(c) a person to whom any function is delegated under section 52(1) or (2);

(d) a member of—

(i) a regulating authority;

(ii) the appeal panel; or

(iii) a council, board, committee or other body of a regulating authority established or vested with any responsibility for, or otherwise in connection with the authority's performance of a function under, this Ordinance;

(e) a related person of a regulating authority; or

(f) a person employed by or assisting a related person of a regulating authority.

58. Offences relating to section 57

(1) A person who contravenes section 57(1) commits an offence.

(2) A person commits an offence if—

(a) the person discloses any information in contravention of section 57(5); and

(b) at the time of the disclosure—

(i) the person knew, or ought to have known, that the information was previously disclosed to the person or any other person under section 57(1), (2) or (3) (other than section 57(2)(a) or (3)(c)); and

(ii) the person had no reasonable grounds to believe that section 57(5) did not apply to the person by virtue of section 57(6).

(3) A person who commits an offence under subsection (1) or (2) is liable—

(a) on summary conviction—to a fine at level 6 and to imprisonment for 6 months; or

(b) on conviction on indictment—to a fine of $1,000,000 and to imprisonment for 2 years.

59. Protection of informers

(1) Any information on the identity of a relevant person is not admissible in evidence in—

(a) any proceedings under Part 7;

(b) any civil or criminal proceedings before a court; or

(c) any proceedings before a tribunal.

(2) In such proceedings, a witness is not obliged—

(a) to disclose the name or address of a relevant person who is not a witness in those proceedings; or

(b) to state any matter that would lead, or would tend to lead, to discovery of the name or address of a relevant person who is not a witness in those proceedings.

(3) If a book, document or paper that is in evidence, or liable to inspection, in such proceedings contains an entry—

(a) in which a relevant person is named or described; or

(b) that might lead to discovery of a relevant person,

the appeal board, court or tribunal (as the case requires) must cause all such passages to be concealed from view, or to be obliterated, so far as may be necessary to protect the relevant person from discovery.

(4) In such proceedings, the appeal board, court or tribunal (as the case requires) may, despite subsection (1), (2) or (3), permit inquiry, and require full disclosure, concerning a relevant person if—

(a) it is of the opinion that justice cannot be fully done between the parties to the proceedings without disclosure of the name of the relevant person; or

(b) in the case of a relevant person falling within paragraph (a) of the definition of ***relevant person*** in subsection (5), it is satisfied that the relevant person made a material statement that the relevant person—

(i) knew or believed to be false; or

(ii) did not believe to be true.

(5) In this section—

relevant person (有關人士) means—

(a) an informer who has given information to an authorized officer with respect to an investigation under Part 5 or 6; or

(b) a person who has assisted a regulating authority or authorized officer with respect to such an investigation.

60. Immunity

(1) A person who complies with a direction or requirement imposed by or under this Ordinance does not incur any civil liability, whether arising in contract, tort, defamation, equity or otherwise, by reason only of the compliance.

(2) A person does not incur any civil liability (whether arising in contract, tort, defamation, equity or otherwise) in respect of an act done, or omitted to be done, by the person in good faith in the performance, or purported performance, of any function under this Ordinance.

(3) Subsection (2) does not affect the liability of the Government for the act or omission.

61. Legal professional privilege

(1) Subject to subsection (2), this Ordinance does not affect any claims, rights or entitlements that would, apart from this Ordinance, arise on the ground of legal professional privilege.

(2) Subsection (1) does not affect any requirement imposed under this Ordinance to disclose the name and address of a client of a legal practitioner (whether or not the legal practitioner is qualified in Hong Kong to practise as counsel or to act as a solicitor).

62. Production of information in information systems

(1) If—

(a) a person may require the production of any document under this Ordinance; and

(b) any information or matter contained in the document is recorded otherwise than in a legible form but is capable of being reproduced in a legible form,

the person may also require the production of a reproduction of the recording of the information or matter, or the relevant part of the recording, in a legible form.

(2) If—

(a) a person may require the production of any document under this Ordinance; and

(b) any information or matter contained in the document is recorded in an information system,

the person may also require the production of a reproduction of the recording of the information or matter, or the relevant part

of the recording, in a form that enables the information or matter to be reproduced in a legible form.

63. Lien claimed on documents

If a person claims a lien on any document in the person's possession that is required to be produced under this Ordinance—

(a) the lien does not affect the requirement to produce the document;

(b) no fee is payable for or in respect of the production; and

(c) the production does not affect the lien.

64. Disposal of certain property

If a regulating authority or authorized officer comes into possession of any property under this Ordinance, section 102 of the Criminal Procedure Ordinance (Cap. 221) applies as if—

(a) the authority or officer were the police within the meaning of that section; and

(b) the property were property that had come into the possession of the police in connection with an offence.

65. Due diligence

(1) In any legal proceedings for an offence under section 7 or Part 4, the defendant is entitled to be acquitted if—

(a) sufficient evidence is adduced to raise an issue that—

(i) the commission of the offence was due to a cause beyond the defendant's control; and

(ii) the defendant took all reasonable precautions and exercised all due diligence to avoid the commission of the offence by the defendant; and

(b) the contrary is not proved by the prosecution beyond reasonable doubt.

(2) If the defence under subsection (1) involves an allegation that the offence was due to—

(a) the act or omission of another person; or

(b) reliance on information given by another person,

the defendant is not, without the leave of the court, entitled to rely on the defence unless the defendant has issued a notice in accordance with subsection (3).

(3) A notice issued for the purposes of subsection (2) must—

(a) identify or assist in the identification of the person who committed the act or omission or gave the information; and

(b) be issued to the person bringing the legal proceedings at least 7 working days before the hearing of the proceedings.

(4) If the defence under subsection (1) involves an allegation that the offence was due to an act or omission of another person, the defence is not established unless sufficient evidence is adduced to raise an issue that the defendant has taken all reasonable steps to secure the cooperation of that other person in complying with the provision concerned, having regard in particular to the steps which the defendant took, and those which might reasonably have been taken by the defendant, for the purpose of securing the cooperation of that other person.

(5) If the defence under subsection (1) involves an allegation that the offence was due to reliance on information given by another person, the defence is not established unless sufficient evidence is adduced to raise an issue that it was reasonable in all the circumstances for the defendant to rely on the information, having regard in particular to—

(a) the steps which the defendant took, and those which might reasonably have been taken by the defendant, for the purpose of verifying the information; and

(b) whether the defendant had any reason not to believe the information.

66. Reasonable excuse

(1) This section applies if a provision of this Ordinance that creates an offence makes a reference to a reasonable excuse for a contravention to which the provision relates.

(2) The reference to a reasonable excuse is to be construed as providing for a defence to a charge in respect of the contravention to which the provision relates.

(3) A defendant is to be taken to have established that the defendant had a reasonable excuse for the contravention if—

(a) sufficient evidence is adduced to raise an issue that the defendant had such a reasonable excuse; and

(b) the contrary is not proved by the prosecution beyond reasonable doubt.

67. Service of notice etc.

(1) Subject to the other provisions of this Ordinance, a notice or other document required to be given or sent (however described) (collectively ***served***) under or for the purposes of this Ordinance is, in the absence of evidence to the contrary, so served if—

(a) for service on a regulating authority—

(i) it is delivered by hand or sent by post to the address of an office specified by the authority for the purpose;

(ii) it is sent by facsimile transmission to a facsimile number specified by the authority for the purpose; or

(iii) it is sent in the form of an electronic record to an address in an information system specified by the authority for the purpose; or

(b) for service on an organization—

(i) it is delivered by hand or sent by post to—

(A) the address provided by the organization under section 19;

(B) the address of the organization's registered office within the meaning of the Companies Ordinance (Cap. 622); or

(C) (if neither of the addresses mentioned in sub-subparagraphs (A) and (B) is available) the organization's last known address;

(ii) it is sent by facsimile transmission to a facsimile number specified by the organization for the purpose; or

(iii) it is sent in the form of an electronic record to an address in an information system specified by the organization for the purpose.

(2) In this section—

address (地址) includes a number, or any sequence or combination of letters, characters, numbers or symbols of any language, used for sending or receiving a document in electronic form;

electronic record (電子紀錄) has the meaning given by section 2(1) of the Electronic Transactions Ordinance (Cap. 553).

68. Certificates of designation

(1) In any legal proceedings concerning a CI operator or critical computer system, a certificate—

(a) purporting to be signed by, or on behalf of, a regulating authority; and

(b) stating that—

(i) the organization specified in the certificate is a CI operator designated by the authority under section 12; or

(ii) the computer system specified in the certificate is a critical computer system designated by the authority under section 13,

must be admitted in the proceedings on its production without further proof.

(2) Until the contrary is proved, the court or appeal board concerned must presume that the certificate is signed by, or on behalf of, the regulating authority concerned.

(3) Until the contrary is proved, the certificate is evidence of the facts stated in it.

(4) In this section—

legal proceedings (法律程序) includes the proceedings of an appeal board.

69. Secretary for Security may make regulations

(1) The Secretary for Security may make regulations for the better carrying out of the provisions of this Ordinance.

(2) Regulations made under this section may prescribe offences for the contravention of the regulations, punishable by a fine.

(3) For an offence punishable on summary conviction, the maximum fine that may be prescribed under subsection (2) for

an offence is $3,000,000 and, in the case of a continuing offence, a further fine not exceeding $60,000 may be prescribed for every day during which the offence continues.

(4) For an offence punishable on conviction on indictment, the maximum fine that may be prescribed under subsection (2) for an offence is $5,000,000 and, in the case of a continuing offence, a further fine not exceeding $100,000 may be prescribed for every day during which the offence continues.

70. Amendment of Schedules

(1) The Secretary for Security may by notice published in the Gazette amend any of the Schedules.

(2) A notice under subsection (1) may contain incidental, consequential, supplemental, transitional or savings provisions that are necessary or expedient in consequence of the notice.

Schedule 1

[ss. 2 & 70]

Sectors Specified for Definition of *Critical Infrastructure*

1. Energy
2. Information technology
3. Banking and financial services
4. Air transport
5. Land transport
6. Maritime transport
7. Healthcare services
8. Telecommunications and broadcasting services

Schedule 2

[ss. 2, 5 & 70]

Designated Authorities and Regulated Organizations

Part 1

Interpretation

1. In this Schedule—

authorized institution (認可機構) has the meaning given by section 2(1) of the Banking Ordinance (Cap. 155);

Cap. 106 (《第 106 章》) means the Telecommunications Ordinance (Cap. 106);

Cap. 106V (《第 106V 章》) means the Telecommunications (Carrier Licences) Regulation (Cap. 106 sub. leg. V);

Cap. 584 (《第 584 章》) means the Payment Systems and Stored Value Facilities Ordinance (Cap. 584);

Communications Authority (通訊事務管理局) means the Communications Authority established by section 3 of the Communications Authority Ordinance (Cap. 616);

designated system (指定系統) has the meaning given by section 2 of Cap. 584;

domestic free television programme service licensee (本地免費電視節目服務持牌人) means a holder of a licence granted under section 8(1) of the Broadcasting Ordinance (Cap. 562) (whether in reliance on section 10(1) of that Ordinance or not), or such a licence extended or renewed under section 11(1) of that

Ordinance, to provide a domestic free television programme service (as defined by section 2(1) of that Ordinance);

Monetary Authority (金融管理專員) means the Monetary Authority appointed under section 5A of the Exchange Fund Ordinance (Cap. 66);

settlement institution (交收機構) has the meaning given by section 2 of Cap. 584;

space station carrier licence (空間電台傳送者牌照) has the meaning given by section 2(1) of Cap. 106V;

system operator (系統營運者) has the meaning given by section 2 of Cap. 584;

unified carrier licence (綜合傳送者牌照) has the meaning given by section 2(1) of Cap. 106V.

Part 2

Specifications of Designated Authorities and Regulated Organizations

Column 1	Column 2	Column 3	Column 4
Item	Designated authority	Sector	Regulated organization
1.	Monetary Authority	Banking and financial services	(a) An authorized institution (b) A licensee as defined by section 2 of Cap. 584

Column 1 Item	Column 2 Designated authority	Column 3 Sector	Column 4 Regulated organization
			(c) A settlement institution of a designated system
			(d) A system operator of a designated system
2.	Communications Authority	Telecommunications and broadcasting services	(a) A holder of a unified carrier licence
			(b) A holder of a space station carrier licence
			(c) A domestic free television programme service licensee
			(d) A licensee as defined by section 13A(1) of Cap. 106

Schedule 3

[ss. 23, 27 & 70]

Computer-system Security Management Plans and Emergency Response Plans

Part 1

General Matters

1. The organization of the computer-system security management unit of the CI operator concerned, including details of the roles and responsibilities of personnel engaged for managing risks relating to the computer-system security of the critical computer systems concerned (including reporting lines and accountabilities).

2. The process of identifying computer systems that are essential to the core function of the critical infrastructure concerned.

3. The policies and guidelines for—
   (a) identifying, assessing, monitoring, responding to and mitigating—
      (i) risks relating to the computer-system security of critical computer systems concerned;
      (ii) vulnerabilities of the systems; and
      (iii) computer-system security threats and computer-system security incidents in respect of the systems;
   (b) detecting computer-system security threats and computer-system security incidents in respect of the systems;

(c) controlling access to, and preventing any act done without lawful authority on, the systems;

(d) ensuring that any changes to the systems are overseen, managed and controlled;

(e) ensuring that all components of the systems are secured, managed and controlled to protect the information stored in, transmitted or processed by, or accessible via, them;

(f) adopting principles that prioritize and integrate security measures throughout the entire development life cycle of the systems;

(g) ensuring the availability of the systems during disruption;

(h) managing contracts and other communications with suppliers of computer-related services and products adopted for the systems in order to ensure that—

(i) the CI operator concerned complies with category 1 obligations, category 2 obligations and category 3 obligations; and

(ii) measures for computer-system security as required by the operator are properly implemented; and

(i) reviewing any computer-system security management plan submitted under section 23.

4. The provision of training to personnel performing obligations relating to the computer-system security of the critical computer systems concerned.

Part 2

Matters relating to Emergency Response

1. The structure, roles and responsibilities of a team responsible for responding to computer-system security incidents.

2. The threshold for initiating the protocol mentioned in section 27(1).

3. The procedures for reporting computer-system security incidents.

4. The procedures for investigating the cause and assessing the impact of computer-system security incidents.

5. A recovery plan for resuming the provision of essential services by, or the normal operation of, the critical infrastructure concerned.

6. A plan for communicating with stakeholders and the general public in respect of computer-system security incidents.

7. The recommended post-incident measures for mitigating the risks of, and preventing, the recurrence of computer-system security incidents.

8. The policies and guidelines for reviewing any emergency response plan submitted under section 27.

Schedule 4

[ss. 24 & 70]

Matters Specified for Computer-system Security Risk Assessments

Part 1

Interpretation

1. In this Schedule—

penetration test (滲透測試), in relation to a computer system, means a test that—

(a) simulates an attack on the system by electronic means; and

(b) aims at identifying the vulnerabilities of the system through the simulated attack;

vulnerability assessment (保安漏洞評估), in relation to a computer system, means an assessment that—

(a) systematically examines the system for known vulnerabilities; and

(b) aims at identifying the vulnerabilities of the system for preventing any exploitation of them.

Part 2

Matters Specified for Computer-system Security Risk Assessments

1. Vulnerability assessment of the critical computer systems concerned.

2. Penetration test of the critical computer systems concerned.

3. Identification and prioritization of risks relating to the computer-system security of the critical computer systems concerned (including any weakness relating to security control) (***identified risks***).

4. Determination of—

(a) the extent of the likely impact on the computer-system security of the critical computer systems concerned that may result from the identified risks; and

(b) the level of risks that the systems can tolerate.

5. Identification of the treatment and monitoring required to deal with the identified risks.

Schedule 5

[ss. 25 & 70]

Matters Specified for Computer-system Security Audits

1. Verification of whether the existing protection measures in respect of the critical computer systems concerned have been performed properly, including—
   (a) whether computer-system security management plans (within the meaning of section 23(1)) are implemented; and
   (b) if so, whether the implementation is done by observing a relevant provision in a code of practice or done in another way.

2. An opinion on the condition of the computer-system security of the critical computer systems concerned based on the verification mentioned in item 1 of this Schedule.

Schedule 6

[ss. 28 & 70]

Specified Time for Notifications under Section 28

Column 1 Item	Column 2 Provision	Column 3 Time
1.	Section 28(2)(a)	(a) If the computer-system security incident concerned has disrupted, is disrupting or is likely to disrupt the core function of the critical infrastructure concerned—12 hours after the CI operator concerned becomes aware of the incident. (b) In any other case—48 hours after the operator becomes aware of the incident.
2.	Section 28(3)	48 hours after the notification concerned is made under section 28(1).
3.	Section 28(4)	14 days after the date on which the CI operator concerned becomes aware of the computer-system security incident concerned.

Schedule 7

[ss. 2, 47, 48 & 70]

Appeals

Part 1

Preliminary

1. Interpretation

In this Schedule—

appeal (上訴) means an appeal under section 48;

IT professional (資訊科技專業人士) means a person who has professional or academic qualifications, or practical experience, in information technology or computer science;

legal professional (法律專業人士) means a solicitor or counsel;

legal representative (法律代表), in relation to a party to an appeal, means the legal professional who represents the party at the appeal.

Part 2

Appeal Panel

2. Appeal panel

(1) The Chief Executive must appoint at least 15 individuals whom the Chief Executive considers to be suitable for appointment under this subsection as members of the appeal panel.

(2) The Chief Executive must not appoint to the appeal panel—

(a) a public officer; or

(b) a person employed—

(i) by a regulating authority; or

(ii) otherwise in connection with the authority's performance of a function under this or any other Ordinance.

(3) The Chief Executive is to appoint one of the members of the appeal panel as chairperson.

(4) In appointing the members of the appeal panel, the Chief Executive must ensure that—

(a) the chairperson is—

(i) a former Justice of Appeal of the Court of Appeal;

(ii) a former judge, a former recorder or a former deputy judge of the Court of First Instance; or

(iii) a person eligible for appointment under section 9 of the High Court Ordinance (Cap. 4);

(b) at least 2 of the members are IT professionals;

(c) at least 2 of the members are legal professionals; and

(d) at least 2 of the members are neither IT professionals nor legal professionals.

(5) Each member of the appeal panel is to be appointed for a period of not more than 2 years, but is eligible for reappointment.

Part 3

Conduct of Appeal

Division 1—General

3. Beginning appeal

(1) For lodging an appeal against a decision, a person must lodge with the chairperson of the appeal panel a notice setting out the grounds of appeal.

(2) The notice—

(a) must be in the form specified by the chairperson of the appeal panel; and

(b) must be lodged within 1 month after the date on which the person receives notice of the decision.

(3) The chairperson of the appeal panel may in a particular case extend the period specified in subsection (2)(b) if the chairperson considers it appropriate to do so.

4. Appointment of appeal board

(1) As soon as practicable after a notice has been lodged under section 3(1) of this Schedule, the chairperson of the appeal panel must appoint from the panel an appeal board to handle the appeal.

(2) The appeal board is to consist of the following members—

(a) a chairperson;

(b) at least 2 ordinary members.

(3) In appointing the members of the appeal board, the chairperson of the appeal panel must ensure that—

(a) the chairperson of the board is a legal professional;

(b) at least one of the ordinary members is an IT professional;

(c) at least one of the ordinary members is neither an IT professional nor a legal professional; and

(d) the members do not have a disclosable interest in the decision appealed against.

(4) For the purposes of subsection (3)(d), a person has a disclosable interest in a decision if—

(a) the person has, in relation to the decision—

(i) a pecuniary interest (whether direct or indirect); or

(ii) a personal interest greater than that which the person has as a member of the public; and

(b) the pecuniary interest or personal interest could conflict or could reasonably be perceived to conflict with the proper performance of the person's functions under this Ordinance.

5. General procedures for handling appeals

(1) An appeal board appointed for an appeal may—

(a) determine the appeal on the basis of written submissions only (without an oral hearing); or

(b) conduct an oral hearing for determining the appeal.

(2) In considering an appeal, every question before an appeal board is to be decided by a majority of votes of the members voting on the question.

(3) Subject to subsection (4), each member of the appeal board has 1 vote.

(4) If there is an equality of votes in respect of any question to be decided, the chairperson of the appeal board has a casting vote in addition to his or her original vote.

(5) Subject to the other provisions in this Schedule, the procedures for the conduct of any hearing for an appeal, and otherwise for handling an appeal, are to be decided by the appeal board.

Division 2—Hearing

6. Application

This Division applies if an appeal board conducts a hearing for determining an appeal.

7. Presiding of and quorum for hearing

(1) The hearing is to be presided over by the chairperson of the appeal board.

(2) The quorum for the hearing is 3 members of the appeal board or one half of the members of the board, whichever is the greater.

(3) For determining the quorum, if the number of members of the appeal board is an odd number, the number is to be regarded as having been increased by 1.

8. Date, time and place of hearing

The chairperson of the appeal board must—

(a) fix the date, time and place for the hearing so that the hearing may begin as soon as practicable; and

(b) serve on the parties to the appeal a notice of the date, time and place of the hearing.

9. Proceedings of appeal board

(1) The appeal board has the following powers when hearing the appeal—

(a) power to take evidence on oath;

(b) power to examine witnesses;

(c) power to receive and consider any material, whether by way of oral evidence, written statements, documents or otherwise, and whether or not the material would be admissible in civil or criminal proceedings;

(d) power to determine the way in which any material mentioned in paragraph (c) is received;

(e) power to award to a person the expenses that, in the board's opinion, the person has reasonably incurred in attending the hearing;

(f) power to make any order that may be necessary for or ancillary to the conduct of the hearing or the carrying out of its functions.

(2) If it appears to the appeal board that the regulating authority concerned has reversed the decision appealed against, the board may determine the appeal in favour of the appellant.

(3) The regulating authority may participate in the hearing through an authorized officer of the authority or a legal representative, or both.

(4) The appellant may participate in the hearing through one or more of the following persons—

(a) a director of the appellant;

(b) a legal representative;

(c) with the consent of the appeal board—any other person.

(5) The appeal board may make an order as to the payment of the costs and expenses incurred in relation to the hearing, whether by the board, any party to the appeal, or any person attending the hearing as a witness.

10. Hearing generally private

(1) Subject to subsection (2), the hearing is to be conducted in private.

(2) After consulting the parties to the appeal, the appeal board may, by order, direct that the hearing, or any part of the hearing, be held in public.

(3) For the purposes of subsection (2), the appeal board must have regard to—

(a) the views or private interests of the parties to the appeal, including any claims as to privilege; and

(b) the public interest.

11. Failure of appellant to send representative to attend hearing

(1) If at the time fixed for the hearing, the appellant fails to send any representative to attend the hearing, the appeal board may—

(a) if it is satisfied that the failure was due to a reasonable ground—postpone or adjourn the hearing for a period it considers appropriate; or

(b) if it is satisfied that the failure was not due to any reasonable ground—

(i) proceed to hear the appeal; or

(ii) by order, dismiss the appeal.

(2) If an appeal is dismissed under subsection (1)(b)(ii)—

(a) the appellant may, within 28 days after the date on which the order for dismissal is made, apply to the appeal board for a review of the order by written notice lodged with the chairperson of the board; and

(b) the board may, if it is satisfied that the failure was due to a reasonable ground, set aside the order for dismissal.

(3) A notice under subsection (2)(a) must be in the form specified by the chairperson of the appeal panel.

(4) The appellant must, as soon as practicable after a notice is lodged under subsection (2)(a), serve a copy of the notice on the other parties to the appeal.

(5) If the appeal board sets aside an order for dismissal under subsection (2)(b), the chairperson of the board must—

(a) fix a new date, time and place for a new hearing of the appeal so that the new hearing may begin as soon as practicable; and

(b) serve, at least 14 days before the date so fixed, on the parties to the appeal a notice of the date, time and place of the new hearing.

12. Privileges and immunities

(1) The appeal board, when hearing the appeal, has the same privileges and immunities as it would have if the appeal were legal proceedings in a court.

(2) A party, legal representative, witness or any other person who appears before the appeal board at the hearing has the same privileges and immunities as the person would have if the appeal were legal proceedings in a court.

Explanatory Memorandum

The main purposes of this Bill are—

(a) to protect the security of the computer systems of Hong Kong's critical infrastructures;

(b) to regulate the operators of such infrastructures; and

(c) to provide for the investigation into, and response to, computer-system security threats and incidents in respect of such computer systems.

2. The Bill contains 8 Parts and 7 Schedules.

Part 1—Preliminary

3. Clause 1 sets out the short title and provides for commencement.

4. Clause 2 contains the definitions for the interpretation of the Bill. The main definitions include ***CI operator***, ***code of practice***, ***computer-system security***, ***computer-system security incident***, ***computer-system security management unit***, ***computer-system security threat***, ***critical computer system***, ***critical infrastructure***, ***designated authority***, ***regulated organization***, ***regulating authority*** and ***specified critical infrastructure***. The clause also explains—

(a) what a reference to a critical infrastructure operated by a CI operator means;

(b) what a reference to a CI operator regulated by a regulating authority means; and

(c) what a reference to doing an act without lawful authority means.

5. Schedule 1 specifies various sectors for the purposes of the definition of ***critical infrastructure*** in clause 2.

Part 2—Regulating Authorities

6. Clause 3 provides for the appointment of the Commissioner of Critical Infrastructure (Computer-system Security) (***Commissioner***).

7. Clause 4 sets out the functions of the Commissioner.

8. Clause 5, together with Schedule 2, provides for the specification of designated authorities.

9. Clause 6 sets out the functions of designated authorities.

10. Clause 7 empowers a regulating authority to give written directions to CI operators regulated by the authority.

11. Clause 8 empowers a regulating authority to issue codes of practice.

12. Clause 9 provides for the use of codes of practice in legal proceedings.

13. Clause 10 empowers a regulating authority to specify forms etc. for the purposes of the Bill.

Part 3—Critical Infrastructures, CI Operators and Critical Computer Systems

Division 1—Ascertaining Critical Infrastructures and Designating CI Operators and Critical Computer Systems

14. Clause 11 provides for the ascertainment of critical infrastructures.

15. Clauses 12 and 13 provide for the designation of CI operators and critical computer systems respectively.

Division 2—Requiring Information

16. Clauses 14 to 17 empower a regulating authority to require information for—

(a) ascertaining critical infrastructures;

(b) designating CI operators;

(c) designating critical computer systems; and

(d) better understanding critical computer systems or ascertaining CI operators' compliance with obligations under Part 4.

17. Clause 18 provides for an offence for failure to provide information as required under clauses 14 to 17.

Part 4—Obligations of CI Operators

Division 1—Obligations relating to Organization of CI Operators

18. Clause 19 imposes an obligation on CI operators to maintain an office in Hong Kong.

19. Clause 20 imposes an obligation on CI operators to notify the regulating authority that regulates the operator of any change of the operator of a critical infrastructure.

20. Clause 21 imposes an obligation on CI operators to maintain a computer-system security management unit.

Division 2—Obligations relating to Prevention of Threats and Incidents

21. Clause 22 imposes an obligation on CI operators to notify the regulating authority that regulates the operator of any material change to critical computer systems etc.

22. Clause 23 imposes an obligation on CI operators to submit and implement computer-system security management plans. Matters that must be covered by such plans are set out in Schedule 3.

23. Clause 24 imposes an obligation on CI operators to conduct computer-system security risk assessments regularly. Matters that must be covered by such assessments are set out in Schedule 4.

24. Clause 25 imposes an obligation on CI operators to arrange to carry out computer-system security audits regularly. Matters that must be covered by such audits are set out in Schedule 5.

Division 3—Obligations relating to Incident Reporting and Response

25. Clause 26 imposes an obligation on CI operators to participate in computer-system security drills conducted by the Commissioner if so required by the Commissioner.

26. Clause 27 imposes an obligation on CI operators to submit and implement emergency response plans. Matters that must be covered by such plans are set out in Part 2 of Schedule 3.

27. Clause 28 imposes an obligation on CI operators to notify the Commissioner of computer-system security incidents. Schedule 6 specifies the time within which such notifications have to be made.

Part 5—Responding to Computer-system Security Threats and Computer-system Security Incidents

28. Clauses 29 to 32 provide for the early intervention of events that have an actual adverse effect, or are likely to have an adverse effect, on the computer-system security of critical computer systems.

29. Clauses 33 to 40 provide for the investigation into, and response to, computer-system security threats and computer-system security incidents.

30. Clause 41 provides for the use of incriminating evidence in proceedings after early interventions and investigations.

31. Clause 42 provides for an offence for failing to comply with requirements imposed for early interventions and investigations.

Part 6—Investigation of Offences

32. Clauses 43 and 46 provide for the investigation of offences under the Bill.

33. Clause 44 provides for the use of incriminating evidence in proceedings after investigations.

34. Clause 45 provides for an offence for failing to comply with a requirement made for investigations.

Part 7—Appeals

35. Clause 47 provides for the establishment of an appeal panel, with details set out in Part 2 of Schedule 7.

36. Clause 48 provides that an organization aggrieved by certain decisions made in relation to it may lodge an appeal. The procedures for such appeals are set out in Part 3 of Schedule 7.

37. Clause 49 provides for the decisions for such appeals.

Part 8—Miscellaneous

38. Clauses 50 and 51 respectively empower the Commissioner and designated authorities to appoint authorized officers.

39. Clauses 52 and 53 provide for the delegation of functions by the Commissioner and designated authorities.

40. Clause 54 provides that the Commissioner may perform functions in respect of critical infrastructures and CI operators regulated by designated authorities if necessary.

41. Clause 55 provides that the Commissioner may exempt CI operators from any obligations under Part 4.

42. Clause 56 provides that designated authorities may prosecute offences.

43. Clauses 57 and 58 provide for the preservation of secrecy.

44. Clause 59 provides for the protection of informers.

45. Clause 60 provides for the immunity of persons who comply with a direction or requirement imposed by or under the Bill.

46. Clause 61 provides that the Bill does not affect legal professional privilege.

47. Clause 62 provides for the production of information contained in information systems.

48. Clause 63 provides that a lien on any document does not affect any requirement to produce the document.

49. Clause 64 provides for the disposal of property that comes into the possession of a regulating authority or authorized officer under the Bill.

50. Clauses 65 and 66 provide for the defences of due diligence and reasonable excuse for certain offences under the Bill.

51. Clause 67 provides for how notices etc. are to be served.

52. Clause 68 provides for the use of certificates of designation in legal proceedings.

53. Clause 69 empowers the Secretary for Security to make regulations for the better carrying out of the provisions of the Bill.

54. Clause 70 empowers the Secretary for Security to amend any of the Schedules to the Bill by notice published in the Gazette.

Annex B

PROPOSED OUTLINE OF CODE OF PRACTICE ("COP")

Note:

1. This proposed outline of CoP is for illustrative purpose only. The exact contents of the CoP will be formulated by the Commissioner after commencement of the Bill, in consultation with relevant stakeholders as appropriate. While a CoP is generally applicable to all Critical Infrastructure Operators ("CIOs"), the Commissioner may develop sector-specific CoPs having regard to the circumstances and needs of individual sectors.

2. Designated Authorities may issue relevant CoPs for the CIOs regulated by them.

(1) Reporting of material changes to computer systems (clause 22 of the Bill)

1. Examples of "material changes", such as (which may be circumstances-dependent) platform migration, server virtualisation, application re-design, integration or change in interdependency with external systems or other computer systems, etc.

(2) Computer-system security management plan (clause 23 of the Bill)

Key elements to be covered include:

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

2. suggested professional qualifications of the **head** of the computer-system security management unit;

3. factors that a CIO should consider in formulating the **policies, standards and guidelines**, such as its own requirements on security, the regulatory requirements prescribed by other regulatory bodies for individual sectors;

4. how risks related to a CIO and its CCSs can be identified, assessed, mitigated and monitored while formulating a computer-system security risk management framework;

5. considering the national security risk and sanctions risk in procurement;

6. devising measures to be taken (whether by contract or other means) when engaging a service provider to ensure that due diligence and reasonable endeavour have been exercised by CIOs to perform relevant obligations notwithstanding the engagement of a service provider

7. establishing 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;

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

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

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

11. implementing access control and account management: only authorized 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;

12. implementing privileged access management to ensure that only authorized personnel have access to the specific administrative capabilities needed;

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

14. implementing password management in accordance with a strong password policy;

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

16. implementing 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;

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

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

19. developing appropriate policies and procedures for remote connection;

20. developing management policies for portable computing devices and removable storage media;

21. implementing backup and recovery policies to ensure the resilience of the system;

22. implementing network security control to allow only authorized traffic to enter the network;

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

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

25. implementing cloud computing security to ensure proper protection; the shared responsibility for information security between the cloud service provider and the organization should be clearly defined and implemented; and

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

(3) Computer-system security risk assessment (clause 24 of the Bill)

1. Matters to be covered for compliance with vulnerability assessment and penetration test

2. Internationally recognized methodology and standards for reference

(4) Computer-system security audit (clause 25 of the Bill)

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

2. Scope of security audit;

3. Internationally recognized methodologies and standards for reference;

4. Details to be included in the computer-system security audit report and rectification plan to address non-compliances identified in the audit exercise.

(5) Incident response obligations

1. Computer-system security drills (clause 26 of the Bill)

- Possible themes and scopes of the drills which may be set by the Commissioner

2. Scope of the emergency response plan (clause 27 and Schedule 3 of the Bill)

- Number of contact points for communication with the Commissioner on matters of computer-system security;
- detailed timeframes (subject to those prescribed in the legislation) for reporting changes of contact points and other revisions to emergency response plan to the Commissioner;
- 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 Commissioner 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; and
- 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.

3. Requirements for reporting computer-system security incidents (clause 28 and Schedule 6 of the Bill)

- Scope and examples of reportable incidents
- Suggested protocol for handling incidents, in particular those involving personal data leakage
- Manners of reporting to the Commissioner to comply with reporting requirements upon becoming aware of a computer-system security incident.

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[1]: the report shall be made within 12 hours after becoming aware of the incident; for other computer-system security incidents: the report shall be made within 48 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 using the incident reporting form specified by the Commissioner 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).

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

- 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.

—

[1] A serious incident refers to a computer-system security incident that has disrupted, is disrupting or will be likely disrupt the core function of the critical infrastructure concerned. For example, if the incident has or is about to have a significant impact on the continuity of essential services of the critical infrastructure, it may be regarded as a serious incident.

Annex C

IMPLICATIONS OF THE BILL

Financial and Civil Service Implications

The legislative proposal will have civil service and financial implications. Subject to the passage of the Bill, a new Commissioner's Office will be set up under the Security Bureau ("SB") to oversee the implementation of the legislative regime.

2. We plan to create three permanent directorate posts and eight permanent non-directorate posts, for the establishment of the Commissioner's Office and the implementation of the legislative regime; and to arrange secondment of officers from the Hong Kong Police Force and the Digital Policy Office respectively to support the Commissioner's Office in areas requiring their expertise, such as incident response. For the creation of the three permanent directorate posts, we plan to seek the approval from the Finance Committee of the Legislative Council in mid-2025. SB plans to be responsible for the operating expenses of Commissioner's Office, including but not limited to accommodation, information technology infrastructure set-up, secretarial support of the Appeal Panel to be set up, etc.

3. While the Bill does not apply to the Government, bureaux and departments ("B/Ds") are required to comply with the detailed Government Information Technology Security Policy and Guidelines, which have been in place since the early 2000s. Any relevant resources implications have been and will continue to be absorbed by individual B/Ds.

Economic implications

4. The legislative proposal should enhance computer-system security of Hong Kong's critical infrastructures, and assure that economic activities enabled by these infrastructures are less susceptible to disruptions due to threats of cyberattacks. This will help ensure Hong Kong's economic security which is essential to its overall long-term economic development. The legislative regime will also increase the demand for professionals in the computer field, and help nurture, attract and retain talent for the industry. At present, "cyber security specialist" is a profession covered in the Talent List, which could facilitate Mainland and overseas talents to come to Hong Kong under the relevant talent admission schemes. In the longer term, we expect that the legislative regime would raise the awareness of the need to train the local workforce so as to acquire the requisite specialist skills, and to upkeep their skills through continuous training to cope with ever-changing demands.

Annex D

SUMMARY OF VIEWS RECEIVED DURING CONSULTATION

We have been engaging stakeholders and LegCo since 2023. A summary of major views received thus far and our responses is set out below.

I. Scope of Regulation

(a) **Inclusion of "Information Technology" ("IT") sector:** We have received views that since IT is involved in the operation of critical infrastructures ("CIs") in different sectors, there should be clearer criteria to define whether individual operators fall into the "IT" sector. Given the society's heavy reliance on IT infrastructure, we consider it an important sector that should be listed as one of the sectors to be regulated. This is also in line with the practice in the United States, Australia, Singapore and the Mainland China. In any event, we will maintain communication with the potential operators to be designated before making a designation.

(b) **No extra-territorial effect:** The proposed legislation empowers the Commissioner to, in the course of investigating an incident or offence related to the statutory obligations of operators of critical infrastructures ("CIOs"), require CIOs to submit relevant information accessible to them in or from Hong Kong. There are concerns that the proposed legislation may involve law enforcement actions against computer systems located outside Hong Kong. In response, we have emphasized that the Bill does not have extra-territorial effect as it does not purport to exercise long-arm enforcement jurisdiction over places outside Hong Kong. The Commissioner will only request information that is accessible by operators in or from Hong Kong, which is entirely in line with the principle of territorial jurisdiction. The Commissioner will allow CIOs reasonable time for complying with the requirement.

II. Target of Regulation – Critical Computer Systems ("CCS")

(c) **"Interconnected systems":** In view of the concerns that the coverage of "interconnected systems" as CCS might be too extensive, after taking into account the situation of Hong Kong and drawing reference from the relevant

legislation in other jurisdictions (such as the United Kingdom ("UK")), we have modified the scope of the computer systems that may be designated as CCS to remove the concept of "interconnected systems". The Bill provides that computer systems which are essential to the core functions of the CI and are accessible by the CIO in or from Hong Kong may be designated as CCSs. The factors that may be taken into account by the Commissioner are also set out in the Bill. Stakeholders have responded positively to such revised proposal.

III. Obligations of CIOs

Category 1 Obligations (Organizational)

(d) **Removal of requirement to report changes in ownership**: In the light of comments that there might be technical difficulties in reporting changes in ownership, given CIOs are often large corporations or listed companies the "ownership" of which may often change, we have removed the requirement of reporting changes in ownership. Upon review, and drawing reference from the relevant legislation in other jurisdictions, including the UK and Macao SAR, we consider that the report of change in operatorship should be sufficient for updating designations. Stakeholders have responded positively to the revised proposal.

(e) **Hiring competent computer security personnel as supervisor:** Some stakeholders have expressed concerns about the shortage of relevant talents to be hired for setting up a computer-system security management unit. In this regard, we will incorporate the requirements concerning the qualifications of the supervisor of the computer-system security management unit into the Code of Practice ("CoP") as recommended standards, so as to provide CIOs with greater flexibility in hiring suitable candidates. Stakeholders have responded positively to such revised proposal.

Category 2 Obligations (Preventive)

(f) **Scope and standards of assessments and audits:** We have received views that there should be clearer descriptions of the scopes of assessments and audits, the standards to which reference could be made and the format of

incident reports. In developing the content of the CoP, we will make reference to the latest technology and international standards, and draw up recommended standards that conform to the statutory requirements. Stakeholders will also be consulted as appropriate to ensure that the CoPs will provide guidance which best suits their needs.

Category 3 Obligations (Incident Reporting and Response)

(g) **Incident reporting timeline:** In view of concerns that it would be difficult for CIOs to report 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 having made reference to the relevant requirements in the UK, the EU and the US, we have relaxed the time frame for reporting serious computer-system security incidents from 2 hours to 12 hours after becoming aware of the incident (other incidents relaxed from 24 hours to 48 hours).

Meanwhile, to ensure effective and early identification of and response to incidents, we have empowered the Commissioner to proactively conduct "early investigation" of any event that has or is likely to have an actual adverse effect on CCS (e.g. a disruption or failure of CCSs) to ascertain the cause of such an event. This is added with reference to the practices in Singapore and Australia. Stakeholders have responded positively to such revised proposal.

IV. Commissioner's Office

(h) **Interface with the Office of the Privacy Commissioner for Personal Data ("PCPD"):** As CIOs might have to report a computer-system security incident to both the PCPD and the Commissioner if the incident involves leakage of personal data, some have expressed concerns that there might be duplication of efforts by the CIOs. It should be noted that there is currently no statutory mechanism for mandatory notification of personal data breach incident to the PCPD, although data users are encouraged to do so. In any event, we have explained that the purposes for reporting a computer-system security incident to the Commissioner and a personal data breach incident to the PCPD are different, and so are the follow-up actions. The Commissioner is responsible

for identifying the cause of the computer-system security incident and plugging the loopholes in an incident and does not focus on personal data, whereas the PCPD focuses on ensuring all data users comply with the requirements of the Personal Data (Privacy) Ordinance (Cap. 486) on the protection of personal data.

V. Designated Authorities ("DAs")

(i) **Sectors regulated by sectoral regulators:** Potential CIOs in the Banking and Financial Services sector and those in the Telecommunications and Broadcasting sector have expressed views that their respective existing regulatory regimes should be adopted or incorporated into the proposed legislative regime, so as to reduce their compliance costs. The introduction of the mechanism of regulation under the Bill by DAs in specific sectors has been designed to address this concern. Under the proposed legislative regime, certain sectoral regulators will be designated as "DAs", responsible for monitoring compliance of Category 1 obligations (organizational) and Category 2 obligations (preventive) by CIOs regulated by the DAs. DAs may issue CoPs to provide guidance on compliance with such statutory obligations under the Bill with reference to prevailing and/or trade standards as appropriate. This approach allows the DAs to establish sets of standards and requirements that best suit the sectors' needs. Stakeholders have responded positively to such proposal.

VI. Penalties

(j) **Penalty levels:** Some have expressed views that the penalties under the legislative regime are excessive. We have emphasized that 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 fine levels are commensurate with the scale of business of CIOs and have been formulated with reference to the situation in Hong Kong and similar legislation in other jurisdictions (e.g. Macao SAR).

(k) **Third-party service providers:** Some have expressed concerns that it is difficult to ensure that third-party service providers (particularly those located

overseas) would comply with contractual agreement to deliver services in compliance with the legislation. We have emphasized that while CIOs may engage third-party service providers, CIOs still need to fulfil the relevant statutory obligations under the legislation. More guidelines on how to meet the threshold of "due diligence" in discharging their categories 1 to 3 obligations will be included in the CoP, which will serve as reference for CIOs when engaging third-party service providers or drawing up and enforcing contracts with them.

VII. Investigation powers of Commissioner

(l) **Access to computer systems of CIOs:** Some have expressed concerns about the Commissioner's power to access CCSs. The proposed legislation stipulates that only when a CIO is unwilling or unable to assist in the investigation by the Commissioner or respond to a threat or incident on its own would the Commissioner consider applying to a magistrate for a warrant to gain access to CCSs in view of public interest, so as to respond to the incident and take necessary remedial measures. A warrant will only be issued if the magistrate is satisfied that all the conditions specified in the Bill are met. The power of entry to premises may be exercised without a warrant exceptionally and only in case of emergencies. Relevant regulators in other jurisdictions (such as Australia and Singapore) also have similar powers which do not even require judicial authorization as a general rule.

(m) **Potential access to sensitive data:** The proposed legislation requires CIOs to report material changes concerning the design, configuration, security or operation of CCSs. Some have expressed views that the information reported should not involve sensitive or confidential information. In response, we have emphasized that the proposed legislation does not target the personal data or trade secrets in the CIOs' computer systems. Moreover, the Commissioner, DAs and all personnel employed or appointed in connection with the performance of functions under the Bill will be subject to statutory obligations to preserve secrecy, and unauthorized disclosure may render them liable on conviction to imprisonment.