Protection of Critical Infrastructures (Computer Systems) Bill

Contents

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.