Cybersecurity Bill

Bill No. 2/2018.

Read the first time on 8 January 2018.

CYBERSECURITY ACT 2018

(No. of 2018)

ARRANGEMENT OF SECTIONS

PART 1

PRELIMINARY

Section

PART 6

GENERAL

Section

A BILL

intituled

An Act to require or authorise the taking of measures to prevent, manage and respond to cybersecurity threats and incidents, to regulate owners of critical information infrastructure, to regulate cybersecurity service providers, and for matters related thereto, and to make consequential or related amendments to certain other written laws.

Be it enacted by the President with the advice and consent of the Parliament of Singapore, as follows:

PART 1

PRELIMINARY

Short title and commencement

1. This Act is the Cybersecurity Act 2018 and comes into operation on a date that the Minister appoints by notification in the *Gazette*.

Interpretation

2.—(1) In this Act, unless the context otherwise requires —

"Assistant Commissioner" means any Assistant Commissioner of Cybersecurity appointed under section 4(1)(*b*);

"assistant licensing officer" means any assistant licensing officer appointed under section 25(2);

"business entity" means —

(*a*) a corporation as defined in section 4(1) of the Companies Act (Cap. 50);

(*b*) an unincorporated association;

(*c*) a partnership; or

(*d*) a limited liability partnership registered under the Limited Liability Partnerships Act (Cap. 163A);

"code of practice" means any code of practice issued or approved under section 11(1), and includes such a code of practice as may be amended from time to time;

"Commissioner" means the Commissioner of Cybersecurity appointed under section 4(1)(*a*);

"computer" means an electronic, magnetic, optical, electrochemical, or other data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but does not include such device as the Minister may, by notification in the *Gazette*, prescribe;

"computer program" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function;

"computer service" includes computer time, data processing and the storage or retrieval of data;

"computer system" means an arrangement of interconnected computers that is designed to perform one or more specific functions, and includes —

(*a*) an information technology system; and

(*b*) an operational technology system such as an industrial control system, a programmable logic controller, a supervisory control and data acquisition system, or a distributed control system;

"critical information infrastructure" means a computer or a computer system in respect of which a designation under section 7(1) is in effect;

"cybersecurity" means the state in which a computer or computer system is protected from unauthorised access or attack, and because of that state —

(*a*) the computer or computer system continues to be available and operational;

(*b*) the integrity of the computer or computer system is maintained; and

(*c*) the integrity and confidentiality of information stored in, processed by or transmitted through the computer or computer system is maintained;

"cybersecurity incident" means an act or activity carried out without lawful authority on or through a computer or computer system that jeopardises or adversely affects its cybersecurity or the cybersecurity of another computer or computer system;

"cybersecurity officer" means any cybersecurity officer appointed under section 4(3);

"cybersecurity program" means any computer program designed for, or purported to be designed for, ensuring or enhancing the cybersecurity of a computer or computer system;

"cybersecurity service" means a service provided by a person for reward that is intended primarily for or aimed at ensuring or safeguarding the cybersecurity of a computer or computer system belonging to another person (*A*), and includes the following:

(*a*) assessing, testing or evaluating the cybersecurity of *A*'s computer or computer system by searching for vulnerabilities in, and compromising, the cybersecurity defences of the computer or computer system;

(*b*) conducting a forensic examination of *A*'s computer or computer system;

(*c*) investigating and responding to a cybersecurity incident that has affected *A*'s computer or computer system by conducting a thorough scan and examination of the computer or computer system to identify and remove elements relating to, and identify the root cause of, the cybersecurity incident, and which involves circumventing the controls implemented in the computer or computer system;

(*d*) conducting a thorough examination of *A*'s computer or computer system to detect any cybersecurity threat or incident that may have already penetrated the cybersecurity defences of the computer or computer system, and that may have evaded detection by conventional cybersecurity solutions;

(*e*) designing, selling, importing, exporting, installing, maintaining, repairing or servicing of one or more cybersecurity solutions;

(*f*) monitoring of the cybersecurity of *A*'s computer or computer system by acquiring, identifying and scanning information that is stored in, processed by,

or transmitted through the computer or computer system for the purpose of identifying cybersecurity threats to the computer or computer system;

(*g*) maintaining control of the cybersecurity of *A*'s computer or computer system by effecting management, operational and technical controls for the purpose of protecting the computer or computer system against any unauthorised effort to adversely affect its cybersecurity;

(*h*) assessing or monitoring the compliance of an organisation with the organisation's cybersecurity policy;

(*i*) providing advice in relation to cybersecurity solutions, including —

(i) providing advice on a cybersecurity program; or

(ii) identifying and analysing cybersecurity threats and providing advice on solutions or management strategies to minimise the risk posed by cybersecurity threats;

(*j*) providing advice in relation to any practices that can enhance cybersecurity;

(*k*) providing training or instruction in relation to any cybersecurity service, including the assessment of the training, instruction or competencies of another person in relation to any such activity;

"cybersecurity service provider" means a person who provides a cybersecurity service;

"cybersecurity solution" means any computer, computer system, computer program or computer service designed for, or purported to be designed for, ensuring or enhancing the cybersecurity of another computer or computer system;

"cybersecurity threat" means an act or activity (whether known or suspected) carried out on or through a computer or

computer system, that may imminently jeopardise or affect adversely, without lawful authority, the cybersecurity of that or another computer or computer system;

"cybersecurity vulnerability" means any vulnerability in a computer or computer system that can be exploited by one or more cybersecurity threats;

"Deputy Commissioner" means the Deputy Commissioner of Cybersecurity appointed under section 4(1)(*b*);

"essential service" means any service essential to the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore, and specified in the First Schedule;

"full-time national serviceman" means a person who is liable to render full-time national service under section 12 of the Enlistment Act (Cap. 93);

"licence" means a licence granted or renewed under section 26;

"licensable cybersecurity service" means any cybersecurity service specified as a licensable cybersecurity service in the Second Schedule;

"licensee" means the holder of a licence;

"owner", in relation to a critical information infrastructure, means the legal owner of the critical information infrastructure and, where the critical information infrastructure is jointly owned by more than one person, includes every joint owner;

"standard of performance" means any standard of performance issued or approved under section 11(1), and includes such a standard of performance as may be amended from time to time.

(2) For the purposes of the definition of "cybersecurity service", a person does not provide a cybersecurity service only because the person —

(*a*) sells, or sells licences for, cybersecurity programs intended to be installed by a user without the assistance of the seller

for the protection of the cybersecurity of a user's computer; or

(*b*) provides services for the management of a computer network or computer system, that are aimed at ensuring the availability of or enhancing the performance of the computer network or computer system.

Application of Act

3.—(1) Part 3 (except section 8) applies to any critical information infrastructure located wholly or partly in Singapore.

(2) Section 8 applies to any computer or computer system located wholly or partly in Singapore.

(3) Except as provided in subsection (4), this Act binds the Government.

(4) Nothing in this Act renders the Government liable to prosecution for an offence.

(5) To avoid doubt, no person is immune from prosecution for any offence under this Act by reason that the person is a public officer or is engaged to provide services to the Government.

PART 2

ADMINISTRATION

Appointment of Commissioner of Cybersecurity and other officers

4.—(1) The Minister may appoint, from public officers or employees of a statutory body under the charge of the Minister —

(*a*) a Commissioner of Cybersecurity; and

(*b*) a Deputy Commissioner and one or more Assistant Commissioners of Cybersecurity, to assist the Commissioner in the discharge of the Commissioner's duties and functions.

(2) The Minister may appoint as an Assistant Commissioner under subsection (1)(*b*) in respect of a critical information infrastructure —

(*a*) a public officer of another Ministry; or

(*b*) an employee of a statutory body under the charge of another Minister,

where that other Ministry or statutory body has supervisory or regulatory responsibility over an industry or a sector to which the owner of the critical information infrastructure belongs.

(3) The Commissioner may in writing appoint such number of public officers as cybersecurity officers as the Commissioner thinks necessary for carrying this Act into effect.

(4) Subject to any general or special directions of the Minister, the Commissioner is responsible for the administration of this Act, and has and may perform such duties and functions as are imposed, and exercise such powers as are conferred, upon the Commissioner by this Act.

(5) The Deputy Commissioner has and may exercise all the powers, duties and functions of the Commissioner except those exercisable under section 7 or 9.

(6) Subject to such conditions or limitations as the Commissioner may specify, an Assistant Commissioner or a cybersecurity officer has and may exercise all the powers, duties and functions of the Commissioner as may be delegated to that Assistant Commissioner or cybersecurity officer in writing, except —

(*a*) in the case of an Assistant Commissioner, those powers, duties or functions exercisable under this subsection, or section 6, 7, 9 or 20(5); and

(*b*) in the case of a cybersecurity officer, those powers, duties or functions exercisable under this subsection, or section 6, 7, 9, 11, 12 or 20(5).

Duties and functions of Commissioner

5. The Commissioner has the following duties and functions:

(*a*) to oversee and promote the cybersecurity of computers and computer systems in Singapore;

(*b*) to advise the Government or any other public authority on national needs and policies in respect of cybersecurity matters generally;

(*c*) to monitor cybersecurity threats, whether such cybersecurity threats occur in or outside Singapore;

(*d*) to respond to cybersecurity incidents that threaten the national security, defence, economy, foreign relations, public health, public order or public safety, or any essential services, of Singapore, whether such cybersecurity incidents occur in or outside Singapore;

(*e*) to identify and designate critical information infrastructure, and to regulate owners of critical information infrastructure with regard to the cybersecurity of the critical information infrastructure;

(*f*) to establish cybersecurity codes of practice and standards of performance for implementation by owners of critical information infrastructure;

(*g*) to represent the Government on cybersecurity issues internationally;

(*h*) to cooperate with computer emergency response teams (CERTs) of other countries or territories on cybersecurity incidents;

(*i*) to develop and promote the cybersecurity services industry in Singapore;

(*j*) to license and establish standards in relation to cybersecurity service providers;

(*k*) to establish standards within Singapore in relation to cybersecurity products or services, and the recommended level of cybersecurity of computer hardware or software, including certification or accreditation schemes;

(*l*) to promote, develop, maintain and improve competencies and professional standards of persons working in the field of cybersecurity;

(*m*) to support the advancement of technology, and research and development relating to cybersecurity;

(*n*) to promote awareness of the need for and the importance of cybersecurity in Singapore;

(*o*) to perform such other functions and discharge such other duties as may be conferred on the Commissioner under any other written law.

Appointment of authorised officers

6.—(1) The Commissioner may, after consulting the Minister, in writing appoint any of the following as an authorised officer to assist the Commissioner in exercising the powers under Part 4:

(*a*) a public officer of another Ministry;

(*b*) an employee of any statutory body;

(*c*) an auxiliary police officer appointed under the Police Force Act (Cap. 235).

(2) In exercising any of the powers of enforcement under Part 4, an authorised officer must, on demand, produce to the person against whom the authorised officer is acting the authority issued to the authorised officer by the Commissioner.

(3) Every authorised officer appointed under subsection (1)(*b*) or (*c*) is deemed to be a public servant for the purpose of the Penal Code (Cap. 224).

PART 3

CRITICAL INFORMATION INFRASTRUCTURE

Designation of critical information infrastructure

7.—(1) The Commissioner may, by written notice to the owner of a computer or computer system, designate the computer or computer system as a critical information infrastructure for the purposes of this Act, if the Commissioner is satisfied that —

(*a*) the computer or computer system is necessary for the continuous delivery of an essential service, and the loss or

compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore; and

(*b*) the computer or computer system is located wholly or partly in Singapore.

(2) A notice issued under subsection (1) must —

(*a*) identify the computer or computer system that is being designated as a critical information infrastructure;

(*b*) identify the owner of the computer or computer system so designated as a critical information infrastructure;

(*c*) inform the owner of the computer or computer system, regarding the owner's duties and responsibilities under this Act that arise from the designation;

(*d*) provide the name and contact particulars of the officer assigned by the Commissioner to supervise the critical information infrastructure;

(*e*) inform the owner of the computer or computer system that any representations against the designation are to be made to the Commissioner by a specified date, being a date not earlier than 14 days after the date of the notice; and

(*f*) inform the owner of the computer or computer system that the owner may appeal to the Minister against the designation, and provide information on the applicable procedure.

(3) Any designation under subsection (1) has effect for a period of 5 years, unless it is withdrawn by the Commissioner before the expiry of the period.

(4) The person who receives a notice under subsection (1) may request the Commissioner to proceed under subsection (5) upon showing proof that —

(*a*) the person is not able to comply with the requirements in this Part for the reason that the person has neither effective control over the operations of the computer or computer

system, nor the ability or right to carry out changes to the computer or computer system; and

(*b*) another person has effective control over the operations of the computer or computer system and the ability and right to carry out changes to the computer or computer system.

(5) If the Commissioner is satisfied that the conditions mentioned in subsection (4)(*a*) and (*b*) are met, the Commissioner may amend the notice issued to the person under subsection (1), and address and send that amended notice to the person mentioned in subsection (4)(*b*).

(6) During the period when a notice amended under subsection (5) is in effect, the provisions of this Part apply to the person mentioned in subsection (4)(*b*) as if every reference to the owner of a critical information infrastructure is a reference to the person mentioned in subsection (4)(*b*).

(7) Where —

(*a*) a notice issued under this section and amended under subsection (5) is addressed and sent to the person mentioned in subsection (4)(*b*); and

(*b*) the person mentioned in subsection (4)(*b*) then ceases to have the control, ability and right mentioned in that provision,

the owner of the critical information infrastructure must notify the Commissioner of this without delay.

(8) Where a critical information infrastructure is owned by the Government and operated by a Ministry, the Permanent Secretary allocated to the Ministry who has responsibility for the critical information infrastructure is treated as the owner of the critical information infrastructure for the purposes of this Act.

(9) A notice issued under this section need not be published in the *Gazette*.

Power to obtain information to ascertain if computer, etc., fulfils criteria of critical information infrastructure

8.—(1) This section applies where the Commissioner has reason to believe that a computer or computer system may fulfil the criteria of a critical information infrastructure.

(2) The Commissioner may, by notice given in the prescribed form and manner, require any person who appears to be exercising control over the computer or computer system, to provide to the Commissioner, within a reasonable period specified in the notice, such relevant information relating to that computer or computer system as may be required by the Commissioner for the purpose of ascertaining whether the computer or computer system fulfils the criteria of a critical information infrastructure.

(3) Without affecting the generality of subsection (2), the Commissioner may in the notice require the person who appears to be exercising control over the computer or computer system to provide —

(*a*) information relating to —

(i) the function that the computer or computer system is employed to serve; and

(ii) the person or persons who is or are, or other computer or computer systems that is or are, served by that computer or computer system;

(*b*) information relating to the design of the computer or computer system; and

(*c*) such other information as the Commissioner may require in order to ascertain whether the computer or computer system fulfils the criteria of a critical information infrastructure.

(4) Any person who, without reasonable excuse, fails to comply with a notice issued under subsection (2) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a continuing offence, to a further fine not exceeding $5,000 for

every day or part of a day during which the offence continues after conviction.

(5) Any person to whom a notice is issued under subsection (2) is not obliged to disclose any information that is subject to any right, privilege or immunity conferred, or obligation or limitation imposed, by or under any law, contract or rules of professional conduct in relation to the disclosure of such information.

Withdrawal of designation of critical information infrastructure

9. The Commissioner may, by written notice, withdraw the designation of any critical information infrastructure at any time if the Commissioner is of the opinion that the computer or computer system no longer fulfils the criteria of a critical information infrastructure.

Furnishing of information relating to critical information infrastructure

10.—(1) The Commissioner may by notice given in the prescribed form and manner, require the owner of a critical information infrastructure to furnish, within a reasonable period specified in the notice, the following:

(*a*) information on the design, configuration and security of the critical information infrastructure;

(*b*) information on the design, configuration and security of any other computer or computer system under the owner's control that is interconnected with or that communicates with the critical information infrastructure;

(*c*) information relating to the operation of the critical information infrastructure, and of any other computer or computer system under the owner's control that is interconnected with or that communicates with the critical information infrastructure;

(*d*) such other information as the Commissioner may require in order to ascertain the level of cybersecurity of the critical information infrastructure.

(2) Any owner of a critical information infrastructure who fails, without reasonable excuse, to comply with a notice mentioned in subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part of a day during which the offence continues after conviction.

(3) The owner of a critical information infrastructure to whom a notice is issued under subsection (1) is not obliged to disclose any information that is subject to any right, privilege or immunity conferred, or obligation or limitation imposed, by or under any law or rules of professional conduct in relation to the disclosure of such information, except that the performance of a contractual obligation is not an excuse for not disclosing the information.

(4) The owner of a critical information infrastructure is not treated as being in breach of any contractual obligation mentioned in subsection (3) for doing or omitting to do any act, if the act is done or omitted to be done with reasonable care and in good faith and for the purpose of complying with a notice issued under subsection (1).

(5) If a material change is made by or on behalf of the owner of a critical information infrastructure to the design, configuration, security or operation of the critical information infrastructure after any information has been furnished to the Commissioner pursuant to a notice mentioned in subsection (1), the owner of the critical information infrastructure must notify the Commissioner of the change not later than 30 days after the change is made.

(6) For the purposes of subsection (5), a change is a material change if the change affects or may affect the cybersecurity of the critical information infrastructure or the ability of the owner of the critical information infrastructure to respond to a cybersecurity threat or incident affecting the critical information infrastructure.

(7) Any owner of a critical information infrastructure who fails, without reasonable excuse, to comply with subsection (5) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $25,000 or to imprisonment for a term not exceeding 12 months or to both.

Codes of practice and standards of performance

11.—(1) The Commissioner may, from time to time —

(*a*) issue or approve one or more codes of practice or standards of performance for the regulation of the owners of critical information infrastructure with respect to measures to be taken by them to ensure the cybersecurity of the critical information infrastructure; or

(*b*) amend or revoke any code of practice or standard of performance issued or approved under paragraph (*a*).

(2) If any provision in any code of practice or standard of performance is inconsistent with this Act, such provision, to the extent of the inconsistency, does not have effect.

(3) Where a code of practice or standard of performance is issued, approved, amended or revoked by the Commissioner under subsection (1), the Commissioner must —

(*a*) publish a notice of the issue, approval, amendment or revocation (as the case may be) in such manner as will secure adequate publicity for such issue, approval, amendment or revocation;

(*b*) specify in the notice the date of the issue, approval, amendment or revocation (as the case may be); and

(*c*) ensure that, so long as the code of practice or standard of performance remains in force, copies of that code or standard, and of all amendments to that code or standard, are available free of charge to the owner of a critical information infrastructure to which that code or standard applies.

(4) None of the following has any effect until the notice relating to it is published in accordance with subsection (3):

(*a*) a code of practice or standard of performance;

(*b*) an amendment to a code of practice or standard of performance;

(*c*) a revocation of a code of practice or standard of performance.

(5) Any code of practice or standard of performance has no legislative effect.

(6) Subject to subsections (4) and (7), every owner of a critical information infrastructure must comply with the codes of practice and standards of performance that apply to the critical information infrastructure.

(7) The Commissioner may, either generally or for such time as the Commissioner may specify, waive the application to the owner of a critical information infrastructure of any code of practice or standard of performance, or any part of it.

Power of Commissioner to issue written directions

12.—(1) The Commissioner may, if the Commissioner thinks —

(*a*) it is necessary or expedient for ensuring the cybersecurity of a critical information infrastructure or a class of critical information infrastructure; or

(*b*) it is necessary or expedient for the effective administration of this Act,

issue a written direction, either of a general or specific nature, to the owner of a critical information infrastructure or a class of such owners.

(2) Without affecting the generality of subsection (1), a direction under that subsection may relate to —

(*a*) the action to be taken by the owner or owners in relation to a cybersecurity threat;

(*b*) compliance with any code of practice or standard of performance applicable to the owner;

(*c*) the appointment of an auditor approved by the Commissioner to audit the owner or owners on their compliance with this Act or any code of practice or standard of performance applicable to the owner or owners; or

(*d*) such other matters as the Commissioner may consider necessary or expedient to ensure the cybersecurity of the critical information infrastructure.

(3) A direction under subsection (1) may be revoked at any time by the Commissioner.

(4) Before giving a direction under subsection (1), the Commissioner must, unless the Commissioner considers that it is not practicable or desirable to do so, give notice to the person or persons whom the Commissioner proposes to issue the direction —

(*a*) stating that the Commissioner proposes to issue the direction and setting out its effect; and

(*b*) specifying the time within which representations or objections to the proposed direction may be made.

(5) The Commissioner must consider any representations or objections which are duly made before giving any direction.

(6) Any person who, without reasonable excuse, fails to comply with a direction under subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part of a day during which the offence continues after conviction.

Change in ownership of critical information infrastructure

13.—(1) Where there is any change in the beneficial or legal ownership (including any share in such ownership) of a critical information infrastructure, the relevant person must inform the Commissioner of the change in ownership not later than 7 days after the date of that change in ownership.

(2) Any person who, without reasonable excuse, fails to comply with subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 2 years or to both.

(3) In subsection (1), the relevant person is —

(*a*) in the case of a transfer of the whole of the legal ownership of the critical information infrastructure to another person — the person who was the owner of the critical information infrastructure before the change in ownership; or

(*b*) in any other case, an owner of the critical information infrastructure.

Duty to report cybersecurity incident in respect of critical information infrastructure, etc.

14.—(1) The owner of a critical information infrastructure must notify the Commissioner of the occurrence of any of the following in the prescribed form and manner, within the prescribed period after becoming aware of such occurrence:

(*a*) a prescribed cybersecurity incident in respect of the critical information infrastructure;

(*b*) a prescribed cybersecurity incident in respect of any computer or computer system under the owner's control that is interconnected with or that communicates with the critical information infrastructure;

(*c*) any other type of cybersecurity incident in respect of the critical information infrastructure that the Commissioner has specified by written direction to the owner.

(2) The owner of a critical information infrastructure must establish such mechanisms and processes for the purposes of detecting cybersecurity threats and incidents in respect of the critical information infrastructure, as set out in any applicable code of practice.

(3) Any owner of a critical information infrastructure who, without reasonable excuse, fails to comply with subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 2 years or to both.

Cybersecurity audits and risk assessments of critical information infrastructure

15.—(1) The owner of a critical information infrastructure must —

(*a*) at least once every 2 years (or at such higher frequency as may be directed by the Commissioner in any particular case), starting from the date of the notice issued under section 7, cause an audit of the compliance of the critical information infrastructure with this Act and the applicable codes of practice and standards of performance, to be carried out by an auditor approved or appointed by the Commissioner; and

(*b*) at least once a year, starting from the date of the notice issued under section 7, conduct a cybersecurity risk assessment of the critical information infrastructure in the prescribed form and manner.

(2) The owner of the critical information infrastructure must, not later than 30 days after the completion of the audit mentioned in subsection (1)(*a*) or the cybersecurity risk assessment mentioned in subsection (1)(*b*), furnish a copy of the report of the audit or assessment to the Commissioner.

(3) Where it appears to the Commissioner from the report of an audit furnished under subsection (2), that any aspect of the audit was not carried out satisfactorily, the Commissioner may direct the owner of the critical information infrastructure to cause the auditor to carry out that aspect of the audit again.

(4) Where it appears to the Commissioner —

(*a*) that the owner of a critical information infrastructure has not complied with a provision of this Act, or an applicable code of practice or standard of performance; or

(*b*) that any information provided by the owner of a critical information infrastructure under section 10 is false, misleading, inaccurate or incomplete,

the Commissioner may by order require an audit in respect of the critical information infrastructure to be carried out by an auditor

appointed by the Commissioner, for the purpose of ascertaining the owner's compliance with this Act or an applicable code of practice or standard of performance, or the accuracy or completeness of the information, as the case may be, and the cost of such audit must be borne by the owner.

(5) Where it appears to the Commissioner, from the report of a cybersecurity risk assessment furnished under subsection (2), that the assessment was not carried out satisfactorily, the Commissioner may either —

(*a*) direct the owner of the critical information infrastructure to carry out further steps to evaluate the level of cybersecurity of the critical information infrastructure; or

(*b*) appoint a cybersecurity service provider to conduct another cybersecurity risk assessment of the critical information infrastructure, and the cost of such assessment must be borne by the owner.

(6) Where the owner of a critical information infrastructure has notified the Commissioner under section 10(5) of a material change made to the design, configuration, security or operation of the critical information infrastructure, or the Commissioner otherwise becomes aware of such material change having been made, the Commissioner may by written notice direct the owner to carry out another audit or cybersecurity risk assessment in addition to the audit or cybersecurity risk assessment mentioned in subsection (1).

(7) Any owner of a critical information infrastructure who —

(*a*) fails, without reasonable excuse, to comply with subsection (1);

(*b*) fails to comply with the Commissioner's direction under subsection (3), (5)(*a*) or (6); or

(*c*) obstructs or prevents an audit mentioned in subsection (4) or a cybersecurity risk assessment mentioned in subsection (5)(*b*) from being carried out,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding

2 years or to both and, in the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part of a day during which the offence continues after conviction.

(8) Any owner of a critical information infrastructure who, without reasonable excuse, fails to comply with subsection (2) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $25,000 or to imprisonment for a term not exceeding 12 months or to both and, in the case of a continuing offence, to a further fine not exceeding $2,500 for every day or part of a day during which the offence continues after conviction.

Cybersecurity exercises

16.—(1) The Commissioner may conduct cybersecurity exercises for the purpose of testing the state of readiness of owners of different critical information infrastructure in responding to significant cybersecurity incidents.

(2) An owner of a critical information infrastructure must participate in a cybersecurity exercise if directed in writing to do so by the Commissioner.

(3) Any person who, without reasonable excuse, fails to comply with a direction under subsection (2) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000.

Appeal to Minister

17.—(1) The owner of a critical information infrastructure who is aggrieved by —

(*a*) the decision of the Commissioner to issue the notice under section 7(1) designating the critical information infrastructure as such;

(*b*) a written direction of the Commissioner under section 12 or 16(2); or

(*c*) any provision in any code of practice or standard of performance issued or approved by the Commissioner that applies to the owner, or any amendment made to it,

may appeal to the Minister against the decision, direction, provision or amendment in the manner prescribed.

(2) An appeal under subsection (1) must be made within 30 days after the date of the notice or direction, or the issue, approval or amendment (as the case may be) of the code of practice or standard of performance, as the case may be, or such longer period as the Minister allows in a particular case (whether allowed before or after the end of the 30 days).

(3) Any person who makes an appeal to the Minister under subsection (1) must, within the period specified in subsection (2) —

(*a*) state as concisely as possible the circumstances under which the appeal arises, and the issues and grounds for the appeal; and

(*b*) submit to the Minister all relevant facts, evidence and arguments for the appeal.

(4) Where an appeal has been made to the Minister under subsection (1), the Minister may require —

(*a*) any party to the appeal; and

(*b*) any person who is not a party to the appeal but appears to the Minister to have information that is relevant to the matters appealed against,

to provide the Minister with all such information as the Minister may require, whether for the purpose of deciding if an Appeals Advisory Panel should be established or for determining the appeal, and any person so required must provide the information in such manner and within such period as may be specified by the Minister.

(5) The Minister may dismiss an appeal of an appellant who fails to comply with subsection (3) or (4).

(6) Unless otherwise provided by this Act or allowed by the Minister, where an appeal is lodged under this section, the decision,

direction or other thing appealed against must be complied with until the determination of the appeal.

(7) The Minister may determine an appeal under this section —

(*a*) by confirming, varying or reversing a decision, notice, direction, provision of a code of practice or standard of performance, or an amendment to such code or standard; or

(*b*) by directing the Commissioner to reconsider the Commissioner's decision, notice, direction, or provision of a code of practice or standard of performance, as the case may be.

(8) Before determining an appeal under subsection (7), the Minister may consult any Appeals Advisory Panel established for the purpose of advising the Minister in respect of the appeal but, in making such determination, is not bound by the advice of the Panel.

(9) The decision of the Minister in any appeal is final.

(10) The Minister may make regulations in respect of the manner in which an appeal may be made to, and the procedure to be adopted in the hearing of any appeal by, the Minister under this section.

Appeals Advisory Panel

18.—(1) Where the Minister considers that an appeal lodged under section 17(1) involves issues the resolution or understanding of which require particular technical skills or specialised knowledge, the Minister may establish an Appeals Advisory Panel to provide advice to the Minister in respect of the appeal.

(2) For the purposes of establishing an Appeals Advisory Panel, the Minister may do all or any of the following:

(*a*) determine, and from time to time vary, the terms of reference of the Appeals Advisory Panel;

(*b*) appoint persons possessing particular technical skills or specialised knowledge to be the chairperson and other members of an Appeals Advisory Panel;

(*c*) at any time remove the chairperson or other member of an Appeals Advisory Panel from such office;

(*d*) determine any other matters which the Minister considers incidental to or expedient for the proper and efficient conduct of business by the Appeals Advisory Panel.

(3) An Appeals Advisory Panel may regulate its proceedings in such manner as it considers appropriate, subject to the following:

(*a*) the quorum for a meeting of the Appeals Advisory Panel is a majority of its members;

(*b*) a decision supported by a majority of the votes cast at a meeting of the Appeals Advisory Panel at which a quorum is present is the decision of that Panel.

(4) The remuneration and allowances, if any, of a member of an Appeals Advisory Panel is to be determined by the Minister.

(5) An Appeals Advisory Panel is independent in the performance of its functions.

PART 4

RESPONSES TO CYBERSECURITY THREATS AND INCIDENTS

Powers to investigate and prevent cybersecurity incidents, etc.

19.—(1) Where information regarding a cybersecurity threat or incident has been received by the Commissioner, the Commissioner may exercise, or may authorise the Deputy Commissioner, an Assistant Commissioner, a cybersecurity officer or an authorised officer to exercise, such of the powers mentioned in subsection (2) as are necessary to investigate the cybersecurity threat or incident, for the purpose of —

(*a*) assessing the impact or potential impact of the cybersecurity threat or incident;

(*b*) preventing any or further harm arising from the cybersecurity incident; or

(*c*) preventing a further cybersecurity incident from arising from that cybersecurity threat or incident.

(2) The powers mentioned in subsection (1) are the following:

(*a*) require, by written notice, any person to attend at such reasonable time and at such place as may be specified by the incident response officer, to answer any question or to provide a signed statement in writing concerning the cybersecurity threat or incident;

(*b*) require, by written notice, any person to produce to the incident response officer any physical or electronic record, or document, or a copy of the record or document, that is in the possession of that person, or to provide the incident response officer with any information, which the incident response officer considers to be related to any matter relevant to the investigation;

(*c*) without giving any fee or reward, inspect, copy or take extracts from such record or document or copy of the record or document mentioned in paragraph (*b*);

(*d*) examine orally any person who appears to be acquainted with the facts and circumstances relating to the cybersecurity threat or incident, and reduce to writing any statement made by the person so examined.

(3) The incident response officer must specify in the notice mentioned in subsection (2)(*b*) —

(*a*) the time and place at which any record, document or copy is to be produced or any information is to be provided; and

(*b*) the manner and form in which it is to be produced or provided.

(4) A statement made by a person examined under this section must —

(*a*) be reduced to writing;

(*b*) be read over to the person;

(*c*) if the person does not understand English, be interpreted for the person in a language that he or she understands; and

(*d*) after correction (if necessary), be signed by that person.

(5) If any person fails to comply with a written notice under subsection (2)(*a*), the incident response officer may report such failure to a Magistrate who may then issue an order for the person to attend before the Commissioner, at a time and place specified in the order, to answer any question or provide a signed statement in writing concerning the cybersecurity threat or incident.

(6) Any person examined under this section or to whom a notice under subsection (2) or an order under subsection (5) is issued is not obliged to disclose any information that is subject to any right, privilege or immunity conferred, or obligation or limitation imposed, by or under any law or rules of professional conduct in relation to the disclosure of such information, except that the performance of a contractual obligation is not an excuse for not disclosing the information.

(7) The person examined under this section or to whom a notice under subsection (2) or an order under subsection (5) is issued, is not treated as being in breach of any contractual obligation mentioned in subsection (6) for doing or omitting to do any act, if the act is done or omitted to be done with reasonable care and in good faith and for the purpose of answering any question asked during the examination or complying with the notice or order.

(8) Any person who —

(*a*) wilfully misstates or without reasonable excuse refuses to give any information, provide any statement or produce any record, document or copy required of the person by an incident response officer under subsection (2); or

(*b*) fails, without reasonable excuse, to comply with an order issued by a Magistrate under subsection (5),

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 6 months or to both.

(9) In this section and sections 20, 21 and 22, "incident response officer" means the Commissioner, the Deputy Commissioner or any Assistant Commissioner, cybersecurity officer or authorised officer

exercising the powers under this section or section 20, as the case may be.

Powers to investigate and prevent serious cybersecurity incidents, etc.

20.—(1) Where the Commissioner receives information regarding a cybersecurity threat or incident which satisfies the severity threshold in subsection (3), the Commissioner may exercise, or may authorise the Deputy Commissioner, an Assistant Commissioner, a cybersecurity officer or an authorised officer to exercise, such of the powers mentioned in subsection (2) as are necessary to investigate the cybersecurity threat or incident, for the purpose of —

(*a*) assessing the impact or potential impact of the cybersecurity threat or incident;

(*b*) eliminating the cybersecurity threat or otherwise preventing any or further harm arising from the cybersecurity incident; or

(*c*) preventing a further cybersecurity incident.

(2) The powers mentioned in subsection (1) are the following:

(*a*) any power mentioned in section 19(2)(*a*), (*b*), (*c*) or (*d*);

(*b*) direct, by written notice, any person to carry out such remedial measures, or to cease carrying on such activities, as may be specified to the person, in relation to a computer or computer system that the incident response officer has reasonable cause to suspect is or was affected by the cybersecurity incident, in order to minimise cybersecurity vulnerabilities in the computer or computer system;

Examples

Examples of remedial measures include —

(*a*) the removal of malicious software from the computer;

(*b*) the installation of software updates to address cybersecurity vulnerabilities;

(*c*) temporarily disconnecting infected computers from a computer network until paragraph (*a*) or (*b*) is carried out; and

(*d*) the redirection of malicious data traffic towards a designated computer or computer system.

(*c*) require the owner of a computer or computer system to take any action to assist with the investigation, including but not limited to —

(i) preserving the state of the computer or computer system by not using it;

(ii) monitoring the computer or computer system for a specified period of time;

(iii) performing a scan of the computer or computer system to detect cybersecurity vulnerabilities and to assess the manner and extent that the computer or computer system is affected by the cybersecurity incident; and

(iv) allowing the incident response officer to connect any equipment to the computer or computer system, or install on the computer or computer system any computer program, as is necessary for the purpose of the investigation;

(*d*) after giving reasonable notice to the owner or occupier of any premises, enter those premises if the incident response officer reasonably suspects that there is within the premises a computer or computer system that is or was affected by the cybersecurity incident;

(*e*) access, inspect and check the operation of a computer or computer system that the incident response officer has reasonable cause to suspect is or was affected by the cybersecurity incident, or use or cause to be used any such computer or computer system to search any data contained in or available to such computer or computer system;

(*f*) perform a scan of a computer or computer system to detect cybersecurity vulnerabilities in the computer or computer system;

(*g*) take a copy of, or extracts from, any electronic record or computer program contained in a computer that the incident response officer has reasonable cause to suspect is or was affected by the cybersecurity incident;

(*h*) subject to subsection (5), with the consent of the owner, take possession of any computer or other equipment for the purpose of carrying out further examination or analysis.

(3) A cybersecurity threat or incident satisfies the severity threshold mentioned in subsection (1) if —

(*a*) it creates a risk of significant harm being caused to a critical information infrastructure;

(*b*) it creates a risk of disruption to the provision of an essential service;

(*c*) it creates a threat to the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore; or

(*d*) the cybersecurity threat or incident is of a severe nature, in terms of the severity of the harm that may be caused to persons in Singapore or the number of computers or value of the information put at risk, whether or not the computers or computer systems put at risk are themselves critical information infrastructure.

(4) An incident response officer exercising the power mentioned in subsection (2)(*e*) may require any assistance the incident response officer needs to gain such access from —

(*a*) any person whom the incident response officer reasonably suspects uses or has used the computer or computer system; or

(*b*) any person having charge of, or who is otherwise concerned with the operation of, such computer or computer system.

(5) Where the owner of the computer or other equipment does not consent to the exercise of the power mentioned in subsection (2)(*h*), the power may be exercised if the Commissioner is satisfied that —

(*a*) the exercise of the power is necessary for the purposes of the investigation;

(*b*) there is no less disruptive method of achieving the purpose of the investigation; and

(*c*) after consultation with the owner, and having regard to the importance of the computer or other equipment to the business or operational needs of the owner, the benefit from the exercise of the power outweighs the detriment caused to the owner,

and the Commissioner has issued to the incident response officer a written authorisation to exercise the power.

(6) The incident response officer must, immediately after the completion of the further examination or analysis on the computer or other equipment which was taken into possession in exercise of the power mentioned in subsection (2)(*h*), return the computer or other equipment to the owner.

(7) Any person who —

(*a*) in relation to an investigation under this section, wilfully misstates or without reasonable excuse refuses to give any information, provide any statement or produce any record, document or copy required of the person by the incident response officer under section 19(2);

(*b*) in relation to an investigation under this section, fails, without reasonable excuse, to comply with an order issued by a Magistrate under section 19(5);

(*c*) fails, without reasonable excuse, to comply with a direction or requirement of an incident response officer under subsection (2)(*b*) or (*c*); or

(*d*) fails, without reasonable excuse, to comply with a lawful demand of an incident response officer made in the discharge of the incident response officer's duties under this section,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $25,000 or to imprisonment for a term not exceeding 2 years or to both.

Production of identification card by incident response officer

21. Every incident response officer, when exercising any of the powers under this Part, must declare the incident response officer's office and must, on demand, produce to any person affected by the exercise of that power such identification card as the Commissioner may direct to be carried by the incident response officer when exercising such power.

Appointment of cybersecurity technical experts

22.—(1) The Commissioner may in writing appoint any of the following as a cybersecurity technical expert for a specified period to assist any incident response officer in the course of an investigation under section 19 or 20:

(*a*) a public officer or an employee of a statutory body;

(*b*) an individual (who is not a public officer or an employee of a statutory body) with suitable qualifications or experience to properly perform the role of a cybersecurity technical expert;

(*c*) a full-time national serviceman enlisted in any force constituted under the Singapore Armed Forces Act (Cap. 295) or in the Special Constabulary constituted under section 66 of the Police Force Act (Cap. 235).

(2) The role of a cybersecurity technical expert is to provide such advice of a technical nature, as the incident response officer may require in the course of an investigation under section 19 or 20.

(3) The Commissioner may, for any reason that appears to the Commissioner to be sufficient, at any time revoke an individual's appointment as a cybersecurity technical expert.

(4) The Commissioner must issue to each cybersecurity technical expert an identification card, which must be carried at all times by the cybersecurity technical expert when performing the role of a cybersecurity technical expert.

(5) A cybersecurity technical expert whose appointment as such ceases must return any identification card issued to the cybersecurity technical expert under subsection (4) to the Commissioner.

Emergency cybersecurity measures and requirements

23.—(1) The Minister may, if satisfied that it is necessary for the purposes of preventing, detecting or countering any serious and imminent threat to —

(*a*) the provision of any essential service; or

(*b*) the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore,

by a certificate under the Minister's hand, authorise or direct any person or organisation specified in the certificate (called in this section the specified person) to take such measures or comply with such requirements as may be necessary to prevent, detect or counter any threat to a computer or computer system or any class of computers or computer systems.

(2) The measures and requirements mentioned in subsection (1) may include, without limitation —

(*a*) the exercise by the specified person of the powers in sections 39(1)(*a*) and (*b*) and (2)(*a*) and (*b*) and 40(2)(*a*), (*b*) and (*c*) of the Criminal Procedure Code (Cap. 68);

(*b*) requiring or authorising the specified person to direct another person to provide any information that is necessary to identify, detect or counter any such threat, including —

(i) information relating to the design, configuration or operation of any computer, computer program or computer system; and

(ii) information relating to the cybersecurity of any computer, computer program or computer system;

(*c*) providing to the Minister or the Commissioner any information (including real-time information) obtained from any computer controlled or operated by the specified person, or obtained by the specified person from another person pursuant to a measure or requirement under paragraph (*b*), that is necessary to identify, detect or counter any such threat, including —

(i) information relating to the design, configuration or operation of any computer, computer program or computer system; and

(ii) information relating to the cybersecurity of any computer, computer program or computer system; and

(*d*) providing to the Minister or the Commissioner a report of a breach or an attempted breach of cybersecurity of a description specified in the certificate under subsection (1), relating to any computer controlled or operated by the specified person.

(3) Any measure or requirement mentioned in subsection (1), and any direction given by a specified person for the purpose of taking any such measure or complying with any such requirement —

(*a*) does not confer any right to the production of, or of access to, information subject to legal privilege; and

(*b*) subject to paragraph (*a*), has effect despite any obligation or limitation imposed or right, privilege or immunity conferred by or under any law, contract or rules of professional conduct, including any restriction on the disclosure of information imposed by law, contract or rules of professional conduct.

(4) A specified person who, without reasonable excuse, fails to take any measure or comply with any requirement directed by the Minister under subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both.

(5) Any person who, without reasonable excuse —

(*a*) obstructs a specified person in the taking of any measure or in complying with any requirement under subsection (1); or

(*b*) fails to comply with any direction given by a specified person for the purpose of the specified person taking any such measure or complying with any such requirement,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both.

(6) No civil or criminal liability is incurred by —

(*a*) a specified person for doing or omitting to do any act if the specified person had done or omitted to do the act in good faith and for the purpose of or as a result of taking any measure or complying with any requirement under subsection (1); or

(*b*) a person for doing or omitting to do any act if the person had done or omitted to do the act in good faith and for the purpose of or as a result of complying with a direction given by a specified person for the purpose of taking any such measure or complying with any such requirement.

(7) The following persons are not considered to be in breach of any restriction upon the disclosure of information imposed by law, contract or rules of professional conduct:

(*a*) a specified person who, in good faith, obtains any information for the purpose of taking any measure under subsection (1) or complying with any requirement under that subsection, or who discloses any information to the Minister or the Commissioner, in compliance with any requirement under that subsection;

(*b*) a person who, in good faith, obtains any information, or discloses any information to a specified person, in compliance with a direction given by the specified person for the purpose of taking any measure under subsection (1) or complying with any requirement under that subsection.

(8) The following persons, namely:

(*a*) a specified person to whom a person has provided information in compliance with a direction given by the specified person for the purpose of taking any measure under subsection (1) or complying with any requirement under that subsection;

(*b*) a person to whom a specified person provides information in compliance with any requirement under subsection (1),

must not use or disclose the information, except —

(i) with the written permission of the person from whom the information was obtained or, where the information is the confidential information of a third person, with the written permission of the third person;

(ii) for the purpose of preventing, detecting or countering a threat to a computer, computer system or class of computers or computer systems;

(iii) to disclose to any police officer or other law enforcement authority any information which discloses the commission of an offence under this Act or any other written law; or

(iv) in compliance with a requirement of a court or the provisions of this Act or any other written law.

(9) Any person who contravenes subsection (8) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 12 months or to both.

(10) Where an offence is disclosed in the course of or pursuant to the exercise of any power under this section —

(*a*) no information for that offence may be admitted in evidence in any civil or criminal proceedings; and

(*b*) no witness in any civil or criminal proceedings is obliged —

(i) to disclose the name, address or other particulars of any informer who has given information with respect to that offence; or

(ii) to answer any question if the answer would lead, or would tend to lead, to the discovery of the name, address or other particulars of the informer.

(11) If any book, document, data or computer output which is admitted in evidence or liable to inspection in any civil or criminal proceedings contains any entry in which any informer is named or described or which may lead to the informer's discovery, the court must cause those entries to be concealed from view or to be obliterated so far as may be necessary to protect the informer from discovery.

PART 5

CYBERSECURITY SERVICE PROVIDERS

No person to provide licensable cybersecurity service without licence

24.—(1) Except under and in accordance with a cybersecurity service provider's licence granted or renewed under section 26, no person —

(*a*) may engage in the business of providing any licensable cybersecurity service to other persons; or

(*b*) being a person who is in the business of providing a licensable cybersecurity service, may advertise, or in any way hold out, that the person provides, or is willing to provide, the licensable cybersecurity service.

(2) Any person who contravenes subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 2 years or to both.

(3) Subsection (1) does not apply to the provision of a cybersecurity service by a company to its related company.

(4) In this section, "related company" has the same meaning given to it by section 6 of the Companies Act (Cap. 50).

Licensing officer and assistant licensing officers

25.—(1) For the purposes of this Part, the Commissioner is the licensing officer and the officer responsible for the administration of this Part.

(2) The licensing officer may appoint such number of assistant licensing officers as are necessary to assist the licensing officer in carrying out the licensing officer's functions and duties under this Part.

(3) Only public officers may be appointed as assistant licensing officers.

(4) The functions and duties conferred on the licensing officer by this Part may be performed by any assistant licensing officer and such performance is subject to the direction and control of the licensing officer.

(5) The Minister may from time to time give to the licensing officer such directions, not inconsistent with the provisions of this Part, as the Minister may consider necessary for carrying out the provisions of this Part, and the licensing officer must comply with any direction so given.

Grant and renewal of licence

26.—(1) An application for the grant or renewal of a licence must be —

(*a*) made to the licensing officer in such form or manner as may be prescribed;

(*b*) accompanied by the prescribed fee, if any; and

(*c*) in the case of an application for the renewal of a licence, made not later than one month or such other period before

the expiry of the licence (called in this section the renewal period) as may be prescribed.

(2) An applicant for the grant or renewal of a licence must, at the request of the licensing officer, provide such further information or evidence that the licensing officer may require to decide the application.

(3) Upon receipt of an application under subsection (1), the licensing officer may —

(*a*) grant or renew the licence applied for; or

(*b*) refuse the application.

(4) Subject to the provisions of this Act, an applicant of an application under subsection (1) is eligible for the grant or renewal of the licence if, and only if —

(*a*) the applicant has paid the prescribed fee (if any); and

(*b*) the applicant satisfies such other requirements as may be prescribed for such grant or renewal.

(5) Without prejudice to subsection (4), the licensing officer may refuse to grant a licence to a person or renew the licence of a person if, in the opinion of the licensing officer —

(*a*) where the person is an individual, the individual is not a fit and proper person to hold or to continue to hold the licence;

(*b*) where the person is a business entity, the business entity is not a fit and proper person to hold or to continue to hold the licence; or

(*c*) it is not in the public interest to grant or renew the licence, or the grant or renewal of the licence may pose a threat to national security.

(6) Where a person submits an application for the renewal of the person's licence before the start of the renewal period, the licence continues in force until the date on which the licence is renewed or the application for its renewal is refused, as the case may be.

(7) Any person who, in making an application for the grant or renewal of a licence —

(*a*) makes any statement or furnishes any particulars, information or document which the person knows to be false or does not believe to be true; or

(*b*) furnishes any information which the person knows or has reason to believe is misleading in a material particular,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 12 months or to both.

(8) In deciding for the purposes of this section whether an individual or a business entity is a fit and proper person to hold or continue to hold a licence, the licensing officer may take into account any matter the licensing officer considers relevant, including any of the following:

(*a*) in the case of an individual —

(i) that the individual has been convicted in Singapore or elsewhere of any offence involving fraud, dishonesty or moral turpitude;

(ii) that the individual has had a judgment entered against the individual in civil proceedings that involves a finding of fraud, dishonesty or breach of fiduciary duty on the part of the individual;

(iii) that the individual is or was suffering from a mental disorder;

(iv) that the individual is an undischarged bankrupt or has entered into a composition with the creditors of the individual; or

(v) that the individual has had a licence revoked by the licensing officer previously;

(*b*) in the case of a business entity —

(i) that the business entity has been convicted in Singapore or elsewhere of any offence involving fraud, dishonesty or moral turpitude;

(ii) that the business entity has had a judgment entered against the business entity in civil proceedings that involves a finding of fraud, dishonesty or breach of fiduciary duty on the part of the business entity;

(iii) that any officer of the business entity is not a fit and proper person to be an officer of a business entity holding the licence;

(iv) that the business entity is in liquidation or is the subject of a winding up order, or there is a receiver appointed in relation to the business entity, or the business entity has entered into a composition or scheme of arrangement with the creditors of the business entity; or

(v) that the business entity has had a licence revoked by the licensing officer previously.

(9) In deciding, for the purposes of subsection (8)(*b*)(iii), whether an officer of a business entity is a fit and proper person to be an officer of a business entity holding a licence, the licensing officer may take into account any matter the licensing officer considers relevant, including any of the matters in subsection (8)(*a*)(i) to (v) with each reference to the individual substituted with a reference to the officer.

(10) In this section, "officer of a business entity" means any director or partner of the business entity or other person who is responsible for the management of the business entity.

Conditions of licence

27.—(1) The licensing officer may grant a licence to an applicant, or renew an applicant's licence, subject to such conditions as the licensing officer thinks fit to impose.

(2) For the purpose of subsection (1), the licensing officer may specify —

(*a*) conditions applicable to all licensees;

(*b*) conditions applicable to a specified class of licensees; or

(*c*) conditions applicable to a specified licensee only.

(3) The licensing officer may at any time add to, modify or revoke any condition of a licence imposed under subsection (1).

(4) Before making any modification to the conditions of a licence, the licensing officer must give notice to the licensee concerned —

(*a*) stating that the licensing officer proposes to make the modification in the manner specified in the notice; and

(*b*) specifying the time (being not less than 14 days after the date of service of the notice) within which written representations with respect to the proposed modification may be made.

(5) Upon receipt of any written representation mentioned in subsection (4)(*b*), the licensing officer must consider the representation and may —

(*a*) reject the representation; or

(*b*) withdraw or amend the proposed modification whether in accordance with the representation or otherwise,

and, in either case (except where the proposed modification is withdrawn), must issue a direction in writing to the licensee concerned requiring that effect be given within a reasonable time to the proposed modification specified in the notice or to such modification as amended.

Form and validity of licence

28.—(1) A licence must —

(*a*) be in such form as the licensing officer may determine; and

(*b*) contain the conditions subject to which it is granted.

(2) A licence is in force for such period (not exceeding 5 years) as the licensing officer may specify in the licence, starting from the date of its issue.

(3) A licence that is renewed continues in force for such period (not exceeding 5 years) as the licensing officer may specify in writing to the licensee, starting from the date immediately following that on which (but for its renewal) the licence would have expired.

Duty to keep records

29.—(1) A licensee must —

(*a*) in relation to each occasion on which the licensee is engaged to provide its cybersecurity service, keep a record of the following information:

(i) the name and address of the person engaging the licensee for the service;

(ii) the name of the person providing the service on behalf of the licensee;

(iii) the date on which the service is provided;

(iv) details of the type of service provided;

(v) such other particulars as may be prescribed; and

(*b*) retain every such record for a period of not less than 3 years after the date of the occasion to which the record relates.

(2) Every licensee must furnish to the licensing officer such records at such time, in such format and through such medium (whether electronic or otherwise) as the licensing officer may require.

(3) If a licensee —

(*a*) knowingly makes a record that —

(i) is false or misleading; or

(ii) omits any matter or thing without which the record is misleading; and

(*b*) furnishes the record to the licensing officer following a requirement under subsection (2),

the licensee shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 12 months or to both.

(4) Subsection (3) does not apply if the record is not false or misleading in a material particular.

Revocation or suspension of licence

30.—(1) Subject to subsection (4), the licensing officer may by order revoke any licence if the licensing officer is satisfied that —

(*a*) the licensee has failed to comply with any condition to which the licence is subject;

(*b*) the licence had been obtained by fraud or misrepresentation;

(*c*) a circumstance existed at the time the licence was granted or renewed that the licensing officer was unaware of, which would have required or permitted the licensing officer to refuse to grant or renew the licensee's licence if the licensing officer had been aware of the circumstance at that time;

(*d*) the licensee has ceased to carry on in Singapore the business for which the licensee is licensed;

(*e*) the licensee has been declared bankrupt or has gone into compulsory or voluntary liquidation other than for the purpose of amalgamation or reconstruction;

(*f*) the licensee has been convicted of an offence under this Act, or an offence involving fraud, dishonesty or moral turpitude;

(*g*) the licensee is no longer a fit and proper person to continue to hold the licence; or

(*h*) it is undesirable in the public interest for the licensee to continue to carry on the business of a licensee.

(2) Subject to subsection (4), the licensing officer may, in any case in which the licensing officer considers that no cause of sufficient gravity for revoking any licence exists, by order —

(*a*) suspend the licence for a period not exceeding 6 months;

(*b*) censure the licensee concerned; or

(*c*) impose such other conditions as the licensing officer considers appropriate.

(3) The licensing officer must give the licensee written notice of —

(*a*) the licensing officer's intention to exercise any power under subsection (1) or (2); and

(*b*) the date on which the licensing officer intends to exercise the power.

(4) The licensing officer must not, during a period of 14 days after the licensing officer informs the licensee of such intention, exercise any power under subsection (1) or (2) unless the licensee concerned is given an opportunity to be heard, whether in person or by a representative and whether in writing or otherwise.

(5) Where the licensing officer has by order revoked a licence under subsection (1) or made any order under subsection (2) in respect of a licensee, the licensing officer must serve on the licensee concerned a notice of the order.

(6) An order under subsection (1) or (2) by the licensing officer revoking or suspending a licence —

(*a*) takes effect immediately upon service of the notice of the order under subsection (5), in a case where the licensing officer states in the order that it is undesirable in the public interest for the licensee to continue to carry on the licensee's business as a licensee; and

(*b*) in any other case, takes effect at the end of 14 days after the service of the notice of the order on the licensee under subsection (5).

(7) In any proceedings under this section consequent upon the conviction of a licensee for a criminal offence, the licensing officer must accept the licensee's conviction as final and conclusive.

(8) In deciding for the purposes of this section whether a licensee is a fit and proper person to continue to hold a licence, the licensing officer may take into account any matter the licensing officer considers relevant, including any matter mentioned in section 26(8).

Unlicensed cybersecurity service provider not to recover fees, etc.

31. Any person who provides any licensable cybersecurity service is not entitled to bring any proceeding in any court to recover any commission, fee, gain or reward for the service provided unless, at the time of providing the service, the person is the holder of a valid cybersecurity service provider's licence.

Financial penalty

32.—(1) This section applies where a licensee —

(*a*) contravenes a provision of this Part, which contravention is not an offence; or

(*b*) fails to comply with any condition imposed by the licensing officer on the licence.

(2) On the occurrence of a contravention or failure to comply mentioned in subsection (1), the licensing officer may, in addition to or instead of taking any action under section 30(1) or (2), order the licensee to pay a financial penalty of an amount not exceeding $10,000 for each contravention or failure to comply, but not exceeding in the aggregate $50,000.

(3) The order mentioned in subsection (2) must specify the date by which the financial penalty is to be paid.

Licensing officer to give opportunity to make representations before ordering financial penalty

33.—(1) Subsections (2) to (6) apply before the licensing officer makes an order under section 32(2).

(2) The licensing officer must give the licensee written notice of —

(*a*) the licensing officer's intention to make the order under section 32(2); and

(*b*) the date on which the licensing officer intends to make the order.

(3) The date mentioned in subsection (2)(*b*) must not be earlier than 21 days after the date of the written notice in subsection (2).

(4) The licensee may make representations to the licensing officer at any time before the date mentioned in subsection (2)(*b*).

(5) The licensing officer must consider any representation made by the licensee before the date mentioned in subsection (2)(*b*).

(6) The licensing officer must, on or after the date mentioned in subsection (2)(*b*), give the licensee written notice of the licensing officer's final decision.

Recovery of financial penalties

34.—(1) Any person who fails to pay any financial penalty imposed by the licensing officer by the date specified in the order under section 32(2) or where there is an appeal to the Minister, by the date specified by the Minister, is liable to pay to the licensing officer interest on the amount unpaid at the same rate as for a judgment debt.

(2) Any financial penalty payable pursuant to an order under section 32(2), and any interest under subsection (1), is recoverable by the licensing officer, or any person duly authorised by the licensing officer to act on his or her behalf, as a debt due to the Government.

(3) The licensing officer may, in any case in which the licensing officer thinks fit, waive, remit or refund in whole or in part any financial penalty imposed or any interest due on any financial penalty.

(4) Any financial penalty and any interest on any financial penalty collected under this section must be paid into the Consolidated Fund.

(5) In any proceedings for the recovery of any financial penalty or interest due on any financial penalty which any person is liable to pay, a certificate purporting to be under the hand of the licensing officer certifying the amount of the financial penalty or interest due on the financial penalty that is payable by the person is prima facie evidence of the facts stated in the certificate.

Appeal to Minister

35.—(1) Any person whose application for a licence or for the renewal of a licence has been refused by the licensing officer may, within the relevant period after being notified of such refusal, appeal against the refusal in the prescribed manner to the Minister.

(2) Where a licence is granted or renewed by the licensing officer subject to conditions or where any condition is added or modified under section 27(3), the licensee concerned may, within the relevant period after being notified of such conditions, addition or modification, appeal against the conditions in the prescribed manner to the Minister.

(3) If the licensing officer has made any order under section 30(1) or (2) in respect of any licensee, the licensee may, within the relevant period after being served with the notice of the order, appeal against the order in the prescribed manner to the Minister.

(4) Any person aggrieved by the licensing officer's order under section 32(2) may, within the relevant period after being notified of the order, appeal against the order in the prescribed manner to the Minister.

(5) In any appeal under this section against an order of the licensing officer made consequent upon the conviction of the licensee for a criminal offence, the Minister must accept the licensee's conviction as final and conclusive.

(6) An appeal under this section against a decision of the licensing officer (except an order mentioned in section 30(6)(*b*) or 32(2)) does not affect the effect of the decision appealed against or prevent the taking of action to implement the decision and the decision appealed against must be complied with until the determination of the appeal.

(7) The decision of the Minister on an appeal under this section is final.

(8) In this section, "relevant period" means 14 days or such longer period as the Minister allows in a particular case, whether allowed before or after the end of the 14 days.

PART 6

GENERAL

Offences by corporations

36.—(1) Where, in a proceeding for an offence under this Act, it is necessary to prove the state of mind of a corporation in relation to a particular conduct, evidence that —

(*a*) an officer, employee or agent of the corporation engaged in that conduct within the scope of his or her actual or apparent authority; and

(*b*) the officer, employee or agent had that state of mind,

is evidence that the corporation had that state of mind.

(2) Where a corporation commits an offence under this Act, a person —

(*a*) who is —

(i) an officer of the corporation, or a member of the corporation (in the case where the affairs of the corporation are managed by its members); or

(ii) an individual involved in the management of the corporation and in a position to influence the conduct of the corporation in relation to the commission of the offence; and

(*b*) who —

(i) consented or connived, or conspired with others, to effect the commission of the offence;

(ii) is in any other way, whether by act or omission, knowingly concerned in, or is party to, the commission of the offence by the corporation; or

(iii) knew or ought reasonably to have known that the offence by the corporation (or an offence of the same type) would be or is being committed, and failed to take all reasonable steps to prevent or stop the commission of that offence,

shall be guilty of that same offence as is the corporation, and shall be liable on conviction to be punished accordingly.

(3) A person mentioned in subsection (2) may rely on a defence that would be available to the corporation if it were charged with the offence with which the person is charged and, in doing so, the person bears the same burden of proof that the corporation would bear.

(4) To avoid doubt, this section does not affect the application of —

(*a*) Chapters V and VA of the Penal Code (Cap. 224); or

(*b*) the Evidence Act (Cap. 97) or any other law or practice regarding the admissibility of evidence.

(5) To avoid doubt, subsection (2) also does not affect the liability of the corporation for an offence under this Act, and applies whether or not the corporation is convicted of the offence.

(6) In this section —

"corporation" includes a limited liability partnership within the meaning of section 2(1) of the Limited Liability Partnerships Act (Cap. 163A);

"officer", in relation to a corporation, means any director, partner, chief executive, manager, secretary or other similar officer of the corporation, and includes —

(*a*) any person purporting to act in any such capacity; and

(*b*) for a corporation whose affairs are managed by its members, any of those members as if the member were a director of the corporation;

"state of mind" of a person includes —

(*a*) the knowledge, intention, opinion, belief or purpose of the person; and

(*b*) the person's reasons for the intention, opinion, belief or purpose.

Offences by unincorporated associations or partnerships

37.—(1) Where, in a proceeding for an offence under this Act, it is necessary to prove the state of mind of an unincorporated association or a partnership in relation to a particular conduct, evidence that —

(*a*) an employee or agent of the unincorporated association or the partnership engaged in that conduct within the scope of his or her actual or apparent authority; and

(*b*) the employee or agent had that state of mind,

is evidence that the unincorporated association or partnership had that state of mind.

(2) Where an unincorporated association or a partnership commits an offence under this Act, a person —

(*a*) who is —

(i) an officer of the unincorporated association or a member of its governing body;

(ii) a partner in the partnership; or

(iii) an individual involved in the management of the unincorporated association or the partnership and in a position to influence the conduct of that unincorporated association or that partnership in relation to the commission of the offence; and

(*b*) who —

(i) consented or connived, or conspired with others, to effect the commission of the offence;

(ii) is in any other way, whether by act or omission, knowingly concerned in, or is party to, the commission of the offence by the unincorporated association or the partnership; or

(iii) knew or ought reasonably to have known that the offence by the unincorporated association or the partnership (or an offence of the same type) would be or is being committed, and failed to take all reasonable steps to prevent or stop the commission of that offence,

shall be guilty of the same offence as is that unincorporated association or that partnership, and shall be liable on conviction to be punished accordingly.

(3) A person mentioned in subsection (2) may rely on a defence that would be available to the unincorporated association or the partnership if it were charged with the offence with which the person is charged and, in doing so, the person bears the same burden of proof as that unincorporated association or that partnership would bear.

(4) To avoid doubt, this section does not affect the application of —

(*a*) Chapters V and VA of the Penal Code (Cap. 224); or

(*b*) the Evidence Act (Cap. 97) or any other law or practice regarding the admissibility of evidence.

(5) To avoid doubt, subsection (2) also does not affect the liability of an unincorporated association or a partnership for an offence under this Act, and applies whether or not that unincorporated association or that partnership is convicted of the offence.

(6) In this section —

"officer", in relation to an unincorporated association (other than a partnership), means the president, the secretary, or any member of the committee of the unincorporated association, and includes —

(*a*) any person holding a position analogous to that of president, secretary or member of a committee of the unincorporated association; and

(*b*) any person purporting to act in any such capacity;

"partner" includes a person purporting to act as a partner;

"state of mind" of a person includes —

(*a*) the knowledge, intention, opinion, belief or purpose of the person; and

(*b*) the person's reasons for the intention, opinion, belief or purpose.

Powers of investigation

38.—(1) An investigation officer authorised by the Commissioner may, in relation to any offence under this Act (except any offence under section 23) or any regulations made under this Act, on declaration of the investigation officer's office and production to the person against whom the investigation officer is acting such identification card as the Commissioner may direct to be carried —

(*a*) require any person whom the investigation officer reasonably believes to have committed that offence to furnish evidence of the person's identity;

(*b*) require, by written notice, any person whom the investigation officer reasonably believes has —

(i) any information; or

(ii) any document in the person's custody or control,

that is relevant to the investigation, to furnish that information or document within the time and manner specified in the written notice;

(*c*) require, by order in writing, the attendance before the investigation officer of any person within the limits of Singapore who, from any information given or otherwise obtained by the investigation officer, appears to be acquainted with the facts or circumstances of the case; or

(*d*) examine orally any person who appears to be acquainted with the facts or circumstances of the case —

(i) whether before or after that person or anyone else is charged with an offence in connection with the case; and

(ii) whether or not that person is to be called as a witness in any inquiry, trial or other proceedings in connection with the case.

(2) The person mentioned in subsection (1)(*d*) is bound to state truly the facts and circumstances with which the person is acquainted concerning the case except that the person need not say anything that might expose the person to a criminal charge, penalty or forfeiture.

(3) A statement made by a person examined under subsection (1)(*d*) must —

(*a*) be reduced to writing;

(*b*) be read over to the person;

(*c*) if the person does not understand English, be interpreted to the person in a language that the person understands; and

(*d*) after correction (if necessary), be signed by the person.

(4) If any person fails to attend as required by an order under subsection (1)(*c*), the investigation officer may report such failure to a Magistrate who may then issue a warrant to secure the attendance of that person as required by the order.

(5) An investigation officer may, without payment, take possession or make copies of any document (or any part of it) furnished under subsection (1), for further investigation.

(6) Any person who —

(*a*) refuses to give access to, or assaults, obstructs, hinders or delays, an investigation officer in the discharge of the investigation officer's duties under this Act;

(*b*) wilfully misstates or without lawful excuse refuses to give any information or produce any document required by an investigation officer under subsection (1); or

(*c*) fails to comply with a lawful demand of an investigation officer in the discharge of the investigation officer's duties under this Act,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 12 months or to both.

(7) In this section and section 39, "investigation officer" means the Deputy Commissioner, or any Assistant Commissioner or cybersecurity officer authorised by the Commissioner, exercising the powers of investigation under this section or section 39.

Power to enter premises under warrant

39.—(1) A Magistrate may, on the application of an investigation officer, issue a warrant in respect of any premises if the Magistrate is satisfied that there are reasonable grounds to suspect that there is on the premises any document —

(*a*) which has been required by an investigation officer under section 38 to be furnished, but has not been furnished in compliance with that requirement; or

(*b*) which, if required by an investigation officer under section 38 to be furnished, will be concealed, removed, tampered with or destroyed.

(2) If the Magistrate is also satisfied that there are reasonable grounds to suspect that there is on those premises any other document that relates to any matter relevant to the investigation concerned, the Magistrate may direct that the powers exercisable under the warrant extend to that other document.

(3) A warrant under subsection (1) may authorise a named investigation officer, and any other officer whom the Commissioner has authorised in writing to accompany the investigation officer —

(*a*) to enter and search the premises specified in the warrant, using such force as is reasonably necessary for the purpose;

(*b*) to take possession of, make copies of, or secure against interference, any document (or any part of it) that appears to

be a document mentioned in subsection (1) or (2) (called in this section the relevant document);

(*c*) to require any person on the premises to provide an explanation of any relevant document or, where applicable, to state, to the best of that person's knowledge and belief, where the relevant document may be found; and

(*d*) to require any relevant document that is stored in electronic form and accessible at the premises to be produced in a form that —

(i) can be taken away; and

(ii) is visible and legible.

(4) The warrant continues in force until the end of the period of one month beginning on the day on which it is issued.

(5) If the owner or occupier of the premises is present when the investigation officer proposes to execute the warrant, the investigation officer must —

(*a*) identify himself or herself to the owner or occupier;

(*b*) show the owner or occupier proof of the identity and authorisation of the investigation officer; and

(*c*) give the owner or occupier a copy of the warrant.

(6) If there is no one at the premises when the investigation officer proposes to execute the warrant, the investigation officer must, before executing it —

(*a*) take such steps as are reasonable in all the circumstances to inform the owner or occupier of the premises of the intended entry into the premises; and

(*b*) where the owner or occupier is so informed, give the owner or occupier or the legal or other representative of the owner or occupier a reasonable opportunity to be present when the warrant is executed.

(7) If the investigation officer is unable to inform the owner or occupier of the premises of the intended entry into the premises, the

investigation officer must, when executing the warrant, leave a copy of it in a prominent place on the premises.

(8) The investigation officer must —

(*a*) prepare and sign a list of all documents and other things taken under subsection (3)(*b*) and (*d*) in execution of the warrant; and

(*b*) give a copy of the list to the owner or occupier of the premises or the legal or other representative of the owner or occupier.

(9) On leaving the premises after executing the warrant, the investigation officer must, if the premises are unoccupied or the owner or occupier of the premises is temporarily absent, leave the premises as effectively secured as the investigation officer found them.

(10) In this section —

"occupier", in relation to any premises specified in a warrant under subsection (1), means a person whom the investigation officer named in the warrant reasonably believes to be the occupier of those premises;

"premises" includes any building, structure, vehicle, vessel or aircraft.

Jurisdiction of court

40. Despite any provision to the contrary in the Criminal Procedure Code (Cap. 68), a District Court has jurisdiction to try any offence under this Act and has power to impose the full penalty or punishment in respect of the offence.

Composition of offences

41.—(1) The Commissioner or any Assistant Commissioner authorised by the Commissioner may, in his or her discretion, compound any offence under this Act that is prescribed as a compoundable offence by collecting from a person reasonably suspected of having committed the offence a sum not exceeding the lower of the following:

(*a*) one half of the amount of the maximum fine that is prescribed for the offence;

(*b*) a sum of $5,000.

(2) Where any offence is compoundable under this section, the abetment of or a conspiracy to commit the offence, or an attempt to commit the offence when the attempt is itself an offence, may be compounded in like manner.

(3) On payment of such sum of money, no further proceedings may be taken against that person in respect of the offence.

(4) All sums collected under this section must be paid into the Consolidated Fund.

Service of documents

42.—(1) A document that is permitted or required by this Act to be served on a person may be served as described in this section.

(2) A document permitted or required by this Act to be served on an individual may be served —

(*a*) by giving it to the individual personally;

(*b*) by sending it by prepaid registered post to the address specified by the individual for the service of documents or, if no address is so specified, the individual's residential address or business address;

(*c*) by leaving it at the individual's residential address with an adult apparently resident there, or at the individual's business address with an adult apparently employed there;

(*d*) by affixing a copy of the document in a conspicuous place at the individual's residential address or business address;

(*e*) by sending it by fax to the fax number last known to the person giving or serving the document as the fax number for the service of documents on the individual; or

(*f*) by sending it by email to the individual's email address.

(3) A document permitted or required by this Act to be served on a partnership (other than a limited liability partnership) may be served —

(*a*) by giving it to any partner or other like officer of the partnership;

(*b*) by leaving it at, or by sending it by prepaid registered post to, the partnership's business address;

(*c*) by sending it by fax to the fax number used at the partnership's business address; or

(*d*) by sending it by email to the partnership's email address.

(4) A document permitted or required by this Act to be served on a body corporate (including a limited liability partnership) or an unincorporated association may be served —

(*a*) by giving it to the secretary or other like officer of the body corporate or unincorporated association, or the limited liability partnership's manager;

(*b*) by leaving it at, or by sending it by prepaid registered post to, the body corporate's or unincorporated association's registered office or principal office in Singapore;

(*c*) by sending it by fax to the fax number used at the body corporate's or unincorporated association's registered office or principal office in Singapore; or

(*d*) by sending it by email to the body corporate's or unincorporated association's email address.

(5) Service of a document under this section takes effect —

(*a*) if the document is sent by fax and a notification of successful transmission is received, on the day of transmission;

(*b*) if the document is sent by email, at the time that the email becomes capable of being retrieved by the person; and

(*c*) if the document is sent by prepaid registered post, 2 days after the day the document was posted (even if it is returned undelivered).

(6) This section does not apply to documents to be served in proceedings in court.

(7) In this section —

"business address" means —

(*a*) in the case of an individual, the individual's usual or last known place of business in Singapore; or

(*b*) in the case of a partnership (other than a limited liability partnership), the partnership's principal or last known place of business in Singapore;

"email address" means the last email address given by the addressee concerned to the person giving or serving the document as the email address for the service of documents under this Act;

"residential address" means an individual's usual or last known place of residence in Singapore.

Preservation of secrecy

43.—(1) Subject to subsections (3) and (7), every specified person must preserve, and aid in preserving, the secrecy of —

(*a*) all matters relating to a computer or computer system of any person;

(*b*) all matters relating to the business, commercial or official affairs of any person;

(*c*) all matters that have been identified as confidential under subsection (5); and

(*d*) all matters relating to the identity of persons furnishing information to any specified person,

that may come to the specified person's knowledge in the performance of his or her functions or the discharge of his or her duties under this Act.

(2) The specified person must not communicate any matter mentioned in subsection (1) to any person, except insofar as such communication —

(*a*) is necessary for the performance of any such function or the discharge of any such duty; or

(*b*) is lawfully required by any court, or lawfully required or allowed by or under this Act or any other written law.

(3) This section does not apply to any information provided in compliance with a direction or requirement under section 23.

(4) Any person who fails to comply with subsection (1) or (2) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 12 months or to both.

(5) Any person, when furnishing any information to a specified person, may identify information that the person claims to be confidential information.

(6) Every claim made under subsection (5) must be supported by a written statement giving reasons why the information is confidential.

(7) Despite subsection (1), the Commissioner may disclose any information relating to any matter mentioned in subsection (1) in any of the following circumstances:

(*a*) where the written consent of the person to whom the information relates has been obtained;

(*b*) for the purposes of —

(i) a prosecution under this Act;

(ii) subject to subsection (8), enabling the Commissioner to give effect to any provision of this Act;

(iii) enabling the Commissioner to investigate a suspected offence under this Act or to enforce a provision of this Act;

(iv) disclosing to any police officer any information which discloses the commission of an offence under the Computer Misuse Act (Cap. 50A); or

(v) complying with such provision of an agreement between Singapore and a country or territory outside Singapore (called in this section a foreign country) as

may be prescribed, where the conditions specified in subsection (9) are satisfied.

(8) If the Commissioner is considering whether to disclose any information under subsection (7)(*b*)(ii), the Commissioner must have regard to —

(*a*) the need to exclude, so far as is practicable, information the disclosure of which would in his or her opinion be contrary to the public interest;

(*b*) the need to exclude, so far as is practicable —

(i) commercial information the disclosure of which would, or might, in his or her opinion, significantly harm the legitimate business interests of the undertaking to which it relates; or

(ii) information relating to the private affairs of an individual the disclosure of which would, or might, in his or her opinion, significantly harm the individual's interest; and

(*c*) the extent to which the disclosure is necessary for the purposes for which the Commissioner is proposing to make the disclosure.

(9) The conditions mentioned in subsection (7)(*b*)(v) are —

(*a*) the information or documents requested by the foreign country are available to the Commissioner;

(*b*) unless the Government otherwise allows, the foreign country undertakes to keep the information or documents given confidential at all times; and

(*c*) the disclosure of the information or documents is not likely to be contrary to the public interest.

(10) In this section, "specified person" means a person who is or has been —

(*a*) the Commissioner, the Deputy Commissioner, an Assistant Commissioner, a cybersecurity officer or a person appointed or employed to assist the Commissioner;

(*b*) an authorised officer appointed under section 6;

(*c*) a member of an Appeals Advisory Panel established under section 18;

(*d*) a cybersecurity technical expert appointed under section 22;

(*e*) an assistant licensing officer; or

(*f*) the Minister, or a person appointed or employed to assist the Minister.

Protection from personal liability

44.—(1) No liability shall lie against the Commissioner, the Deputy Commissioner, an Assistant Commissioner, a cybersecurity officer, an authorised officer appointed under section 6, an assistant licensing officer, a member of an Appeals Advisory Panel established under section 18 or any other person acting under the direction of the Commissioner who, acting in good faith and with reasonable care, does or omits to do anything in —

(*a*) the exercise or purported exercise of any power under this Act; or

(*b*) the performance or purported performance of any function or duty under this Act.

(2) Where the Commissioner provides a service to the public whereby information is supplied to the public pursuant to any written law, neither the Commissioner nor any person acting under the direction of the Commissioner who is involved in the supply of such information is liable for any loss or damage suffered by any person by reason of any error or omission of whatever nature appearing in the information or however caused, if the error or omission was made in good faith and despite the exercise of reasonable care in the ordinary course of the discharge of the duties of the Commissioner or such person.

Protection of informers

45.—(1) No witness in any proceedings for an offence under Part 3 is obliged or permitted —

(*a*) to disclose the name, address or other particulars of an informer who has given information with respect to that offence, or the substance of the information received from the informer; or

(*b*) to answer any question if the answer would lead, or would tend to lead, to the discovery of the name, address or other particulars of the informer.

(2) If any document which is in evidence or liable to inspection in any proceedings mentioned in subsection (1) contains any entry in which any informer is named or described or which might lead to the informer's discovery, the court must cause the entry to be concealed from view or to be obliterated so far only as may be necessary to protect the informer from discovery.

(3) If, during any proceedings —

(*a*) the court, after full inquiry into the case, believes that the informer wilfully made in the informer's complaint a material statement which the informer knew or believed to be false or did not believe to be true; or

(*b*) the court is of the opinion that justice cannot be fully done between the parties to the proceedings without the discovery of the informer,

it is lawful for the court to require the production of the original complaint, if in writing, and permit inquiry, and require full disclosure of the informer.

General exemption

46.—(1) The Minister may, by order in the *Gazette*, exempt any person or any class of persons from all or any of the provisions of this Act, either generally or in a particular case and subject to such conditions as may be prescribed.

(2) If any exemption is granted under subsection (1) with conditions, the exemption operates only if the conditions are complied with.

Amendment of Schedules

47.—(1) The Minister may at any time, by order in the *Gazette*, amend the First or Second Schedule.

(2) The Minister may, in any order made under subsection (1), make such transitional, incidental, consequential or supplementary provision as may be necessary or expedient.

(3) Any order made under subsection (1) must be presented to Parliament as soon as possible after publication in the *Gazette*.

Regulations

48.—(1) The Minister may make regulations for carrying out the purposes and provisions of this Act.

(2) Without limiting subsection (1), the Minister may make regulations for or with respect to all or any of the following matters:

(*a*) the procedure for the designation of a critical information infrastructure;

(*b*) the technical or other standards relating to cybersecurity to be maintained in respect of a critical information infrastructure;

(*c*) the responsibilities and duties of the owner of a critical information infrastructure;

(*d*) the type of changes that are considered material changes to the design, configuration, security or operations of a critical information infrastructure to be reported by the owner of the critical information infrastructure;

(*e*) the type of cybersecurity incidents in respect of a critical information infrastructure that are required to be reported by the owner of the critical information infrastructure;

(*f*) the requirements for, and the manner for the carrying out of, cybersecurity audits and cybersecurity risk assessments required to be conducted by the owner of a critical information infrastructure;

(*g*) the form and nature of cybersecurity exercises that may be conducted;

(*h*) the class or classes of licence to be issued, and the requirements for the grant or renewal of the licence;

(*i*) the conduct of licensees in carrying on their business;

(*j*) the fees to be paid in respect of any matter or thing required for the purposes of this Act, including the refund and remission (in whole or part) of such fees; and

(*k*) all matters and things which by this Act are required or permitted to be prescribed or which are necessary or expedient to be prescribed to give effect to this Act.

(3) Except as otherwise expressly provided in this Act, the regulations —

(*a*) may be of general or specific application;

(*b*) may provide that any contravention of any specified provision of the regulations shall be an offence; and

(*c*) may provide for penalties not exceeding a fine of $50,000 or imprisonment for a term not exceeding 12 months or both for each offence and, in the case of a continuing offence, a further penalty not exceeding a fine of 10% of the maximum fine prescribed for that offence for every day or part of a day during which the offence continues after conviction.

Related amendments to Computer Misuse and Cybersecurity Act

49. The Computer Misuse and Cybersecurity Act (Cap. 50A, 2007 Ed.) is amended —

(*a*) by deleting the words ", to require or authorise the taking of measures to ensure cybersecurity," in the long title;

(*b*) by deleting the words "and Cybersecurity" in section 1;

(*c*) by deleting the words "within the meaning of section 15A(12)" in section 11(4)(*b*);

(*d*) by inserting, immediately after subsection (5) of section 11, the following subsection:

"(5A) In subsection (4)(*b*), "essential service" means any of the following services:

(*a*) services directly related to communications infrastructure, banking and finance, public utilities, public transportation, land transport infrastructure, aviation, shipping, or public key infrastructure;

(*b*) emergency services such as police, civil defence or health services."; and

(*e*) by repealing section 15A.

Consequential amendments to other Acts

50.—(1) Part III of the Second Schedule to the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A, 2000 Ed.) is amended by deleting the words "and Cybersecurity" immediately above item 210.

(2) The Criminal Procedure Code (Cap. 68, 2012 Ed.) is amended —

(*a*) by deleting the words "and Cybersecurity" in the definition of "computer" in section 2(1); and

(*b*) by deleting the words "and Cybersecurity" in item 4 of the Second Schedule.

(3) Section 2(1) of the Goods and Services Tax Act (Cap. 117A, 2005 Ed.) is amended by deleting the words "and Cybersecurity" in the definitions of "computer" and "computer output".

(4) Section 65B(4) of the Income Tax Act (Cap. 134, 2014 Ed.) is amended by deleting the words "and Cybersecurity".

(5) Section 20(4) of the Manufacture of Optical Discs Act (Cap. 170C, 2005 Ed.) is amended by deleting the words "and Cybersecurity".

(6) The Second Schedule to the Mutual Assistance in Criminal Matters Act (Cap. 190A, 2001 Ed.) is amended by deleting the words "and Cybersecurity" immediately above item 39.

(7) The Schedule to the Organised Crime Act 2015 (Act 26 of 2015) is amended by deleting the words "and Cybersecurity" immediately above item 19.

(8) Section 13(5) of the Private Lotteries Act (Cap. 250, 2012 Ed.) is amended by deleting the words "and Cybersecurity" in the definitions of "computer" and "computer output".

(9) Section 64A(11) of the Property Tax Act (Cap. 254, 2005 Ed.) is amended by deleting the words "and Cybersecurity" in the definitions of "computer" and "computer output".

(10) Part II of the First Schedule to the Registration of Criminals Act (Cap. 268, 1985 Ed.) is amended by deleting the words "and Cybersecurity" in the item relating to "Computer Misuse and Cybersecurity Act".

(11) Section 6E(3) of the Road Traffic Act (Cap. 276, 2004 Ed.) is amended by deleting the words "and Cybersecurity".

(12) Section 2(1) of the Strategic Goods (Control) Act (Cap. 300, 2003 Ed.) is amended by deleting the words "and Cybersecurity" in the definition of "computer".

(13) Section 77(6) of the Co-operative Societies Act (Cap. 62, 2009 Ed.) is amended by deleting the words "and Cybersecurity" in the definition of "computer".

Saving and transitional provisions

51.—(1) Despite anything in this Act, any person who, immediately before the date of commencement of Part 5, is engaged in the business of providing a licensable cybersecurity service, may continue to engage in that business —

(*a*) for 6 months starting on the date of commencement of Part 5; and

(*b*) if, within the period in paragraph (*a*), the person applies for a licence under section 26, until the earlier of the following:

(i) the date on which the licensing officer grants the licence to the person;

(ii) the date that the application is finally refused or withdrawn.

(2) For a period of 2 years after the date of commencement of any provision of this Act, the Minister may, by regulations, prescribe such additional provisions of a saving or transitional nature consequent on the enactment of that provision as the Minister may consider necessary or expedient.

FIRST SCHEDULE

Sections 2(1) and 47(1)

ESSENTIAL SERVICES

Services relating to energy

1. Electricity generation, electricity transmission or electricity distribution services
2. Services for the supply or transmission of natural gas for electricity generation

Services relating to info-communications

3. Fixed telephony services
4. Mobile telephony services
5. Broadband internet access services
6. National domain name registry services

Services relating to water

7. Water supply services
8. Services relating to collection and treatment of used water
9. Services relating to management of storm water

Services relating to healthcare

10. Acute hospital care services
11. Services relating to disease surveillance and response

FIRST SCHEDULE — *continued*

Services relating to banking and finance

12. Banking services, including cash withdrawal and deposits, corporate lending, treasury management, and payment services
13. Payments clearing and settlement services
14. Securities trading, clearing, settlement and depository services
15. Derivatives trading, clearing and settlement services
16. Services relating to maintenance of monetary and financial stability
17. Currency issuance
18. Services relating to cash management and payments for the Government

Services relating to security and emergency services

19. Civil defence services
20. Police and security services
21. Immigration services
22. Registration services under the National Registration Act (Cap. 201)
23. Prison security and rehabilitation services

Services relating to aviation

24. Air navigation services
25. Airport passenger control and operations
26. Airport baggage and cargo handling operations
27. Aerodrome operations
28. Flight operations of aircraft

Services relating to land transport

29. Rapid transit systems operated under a licence granted under the Rapid Transit Systems Act (Cap. 263A)
30. Bus services operated under a bus service licence granted under the Bus Services Industry Act 2015 (Act 30 of 2015)
31. Monitoring and management of rapid transit systems operated under a licence granted under the Rapid Transit Systems Act
32. Monitoring and management of bus services operated under a bus service licence granted under the Bus Services Industry Act 2015
33. Monitoring and management of road traffic

FIRST SCHEDULE — *continued*

Services relating to maritime

34. Monitoring and management of shipping traffic

35. Container terminal operations

36. General and bulk cargo terminal operations

37. Cruise and ferry passenger terminal operations

38. Pilotage, towage and water supply

39. Bunker supply

40. Salvage operations

41. Passenger ferry operations

Services relating to functioning of Government

42. Services relating to the electronic delivery of Government services to the public

43. Services relating to the electronic processing of internal Government functions

Services relating to media

44. Services relating to broadcasting of free-to-air television and radio

45. Services relating to publication of newspapers

46. Security printing services

SECOND SCHEDULE

Sections 2(1) and 47(1)

LICENSABLE CYBERSECURITY SERVICES

1. The following cybersecurity services are licensable cybersecurity services for the purposes of this Act:

(*a*) managed security operations centre (SOC) monitoring service;

(*b*) penetration testing service.

2. In this Schedule —

"managed security operations centre (SOC) monitoring service" means a service for the monitoring of the level of cybersecurity of a computer or computer system of another person by acquiring, identifying and scanning information that is stored in, processed by, or transmitted through the computer or computer system for the purpose of identifying cybersecurity threats to the computer or computer system;

"penetration testing service" means a service for assessing, testing or evaluating the level of cybersecurity of a computer or computer system, by searching for vulnerabilities in, and compromising, the cybersecurity defences of the computer or computer system, and includes any of the following activities:

(*a*) determining the cybersecurity vulnerabilities of a computer or computer system, and demonstrating how such vulnerabilities may be exploited and taken advantage of;

(*b*) determining or testing the organisation's ability to identify and respond to cybersecurity incidents through simulation of attempts to penetrate the cybersecurity defences of the computer or computer system;

(*c*) identifying and quantifying the cybersecurity vulnerabilities of a computer or computer system, indicating vulnerabilities and providing appropriate mitigation procedures required to eliminate vulnerabilities or to reduce vulnerabilities to an acceptable level of risk;

(*d*) utilising social engineering to assess the level of vulnerability of an organisation to cybersecurity threats.

EXPLANATORY STATEMENT

This Bill seeks to establish a framework for the protection of critical information infrastructure (CII) against cybersecurity threats, the taking of measures to prevent, manage and respond to cybersecurity threats and incidents in Singapore, and the regulation of providers of licensable cybersecurity services.

Part 1 introduces the fundamental concepts used in the Bill and provides for the application of the Bill.

Part 2 provides for the administration of the Bill and the appointment of a Commissioner of Cybersecurity (Commissioner) and other officers for the purposes of the Bill.

Part 3 provides for the designation of CII and the regulation of owners of CII with regard to the cybersecurity of the CII.

Part 4 provides for the taking of measures to prevent, manage and respond to cybersecurity threats and incidents in Singapore.

Part 5 provides for the licensing of providers of licensable cybersecurity services.

Part 6 contains general provisions.

The Bill also makes consequential and related amendments to certain other Acts.

PART 1

PRELIMINARY

Clause 1 relates to the short title and commencement.

Clause 2 is a general definition provision. It contains definitions of terms used in the provisions of the Bill.

A "cybersecurity threat" is defined as an act or activity (known or suspected) carried out on or through a computer or computer system, that may imminently jeopardise or affect adversely, without lawful authority, the cybersecurity of a computer or computer system. An example of a cybersecurity threat is a phishing email, or an email that is infected with a malicious computer program.

A "cybersecurity incident" is defined as an act or activity carried out without lawful authority on or through a computer or computer system that jeopardises or adversely affects its cybersecurity or the cybersecurity of another computer or computer system. A cybersecurity incident is essentially a cybersecurity threat that has been realised. An example of a cybersecurity incident is the unauthorised hacking of a computer by a hacker, the accessing of a hyperlink in a phishing email by the recipient resulting in the installation of a malicious computer program on the recipient's computer, or the opening of an infected document in an email by the

recipient resulting in the execution of a malicious computer program on the recipient's computer.

Clause 3 provides for the application of Part 3 of the Bill to any CII located wholly or partly in Singapore. The Bill applies to the Government.

PART 2

ADMINISTRATION

Clause 4 provides for the appointment of a Commissioner, a Deputy Commissioner and one or more Assistant Commissioners of Cybersecurity by the Minister. The clause empowers the Minister to appoint as an Assistant Commissioner, a public officer from another Ministry or an employee of a statutory body under the charge of another Minister, where that Ministry or statutory body has supervisory or regulatory responsibility over an industry or a sector to which the owner of a CII belongs.

The Commissioner may appoint public officers as cybersecurity officers.

The Commissioner is responsible for the administration of the Bill.

Clause 5 relates to the duties and functions of the Commissioner.

Clause 6 empowers the Commissioner to appoint as an authorised officer to assist for the purposes of Part 4, a public officer of another Ministry, an employee of any statutory body or an auxiliary police officer.

PART 3

CRITICAL INFORMATION INFRASTRUCTURE

Clause 7 empowers the Commissioner to, by a written notice to the owner of a computer or computer system, designate the computer or computer system as a CII if the Commissioner is satisfied that it fulfils the criteria for a CII, viz, the computer or computer system (located wholly or partly in Singapore) is necessary for the continuous delivery of an essential service and its loss or compromise will have a debilitating effect on the availability of the essential service in Singapore. An essential service is defined in clause 2 as any service essential to the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore, and specified in the First Schedule.

The designation has effect for a period of 5 years unless it is withdrawn by the Commissioner before the expiry of the period.

The person who receives a notice of designation may request the Commissioner to amend the notice by addressing it to another person who has effective control of the CII (controller), by showing proof that the person who received the notice is not able to comply with the requirements in Part 3 because that person has neither

effective control over the CII's operations nor the ability or right to carry out changes to the CII, whilst the controller has both. If the Commissioner addresses and sends an amended notice to the controller, the controller will be subject to all the requirements under Part 3 during the period when the notice is in effect, as if the controller were the owner.

Clause 7(8) also provides, where a CII is owned by the Government and operated by a Ministry, that the Permanent Secretary allocated to the Ministry who has responsibility for the CII is treated as the owner of the CII for the purposes of the Bill.

Clause 8 empowers the Commissioner to require any person appearing to be exercising control over a computer or computer system, to provide relevant information for the purpose of ascertaining whether the computer or computer system fulfils the criteria of a CII.

Clause 9 empowers the Commissioner to withdraw the designation of any CII at any time if the Commissioner is of the opinion that the computer or computer system no longer fulfils the criteria of a CII.

Clauses 10 to 16 set out the duties of the owner of a CII, which include —

(*a*) to provide the Commissioner with information relating to the CII (clause 10);

(*b*) to comply with codes of practice, standards of performance or written directions in relation to the CII as may be issued by the Commissioner (clauses 11 and 12);

(*c*) to notify the Commissioner of any change in ownership of the CII (clause 13);

(*d*) to notify the Commissioner of any prescribed cybersecurity incidents relating to the CII (clause 14);

(*e*) to cause regular audits of the compliance of the CII with the Bill, codes of practice and standards of performance, to be carried out by an auditor approved or appointed by the Commissioner (clause 15);

(*f*) to carry out regular cybersecurity risk assessments of the CII (clause 15); and

(*g*) to participate in cybersecurity exercises as required by the Commissioner (clause 16).

Clause 10(1) empowers the Commissioner to require by notice the owner of a CII to furnish information relating to the CII, including information relating to —

(*a*) the design, configuration and security of the CII;

(*b*) the design, configuration and security of any other computer or computer system under the owner's control that is interconnected with the CII or that communicates with the CII;

(*c*) the operation of the CII, and of any other computer or computer system under the owner's control that is interconnected with the CII or that communicates with the CII; and

(*d*) such other information as the Commissioner may require in order to ascertain the level of cybersecurity of the CII.

The owner of a CII is required to notify the Commissioner of any material change made to the design, configuration, security or operation of the CII, not later than 30 days after the change is made. A material change is defined as a change that affects or may affect the cybersecurity of the CII or the ability of the owner to respond to a cybersecurity threat or incident affecting the CII.

Clause 10(3) provides that the owner of a CII who receives a notice under clause 10(1) is not obliged to disclose any information that is subject to any right, privilege or immunity conferred, or obligation or limitation imposed, by or under any law or rules of professional conduct in relation to the disclosure of such information, except that the performance of a contractual obligation is not an excuse for not disclosing the information.

Clause 11 empowers the Commissioner to issue or approve one or more codes of practice or standards of performance for the regulation of owners of CII with respect to measures to be taken by them to ensure the cybersecurity of the CII. The Commissioner is also empowered to amend or revoke any code of practice or standard of performance issued or approved. A code of practice or standard of performance is not subsidiary legislation but non-compliance can be enforced through the issuance of a written direction under clause 12.

Clause 12 empowers the Commissioner to issue a written direction to the owner of a CII, either of a general or specific nature, for the purpose of ensuring the cybersecurity of a CII or a class of CII, or for the effective administration of the Bill. Non-compliance with a direction is an offence.

Clause 13 requires the owner of a CII to inform the Commissioner of any change in the beneficial or legal ownership (including any share in such ownership) of the CII not later than 7 days after the date of the change in ownership.

Clause 14 requires the owner of a CII to notify the Commissioner of the occurrence of a prescribed cybersecurity incident in respect of the CII or any computer or computer system under the owner's control that is interconnected with the CII, or any other type of cybersecurity incident in respect of the CII as specified by a written direction.

Clause 15 requires the owner of a CII to cause an audit of the compliance of the CII with the Bill and applicable codes of practice and standards of performance, to be carried out at least once every 2 years (or more frequently as directed by the Commissioner in any particular case) by an auditor approved or appointed by the Commissioner. Clause 15 also requires the owner of a CII to conduct a cybersecurity risk assessment of the CII at least once a year.

Clause 16 empowers the Commissioner to require the owner of a CII to participate in cybersecurity exercises for the purposes of testing the state of readiness of the owner in responding to significant cybersecurity incidents.

Clause 17 provides for an avenue of appeal by the owner of a CII to the Minister against —

(*a*) the decision of the Commissioner to issue the notice under clause 7(1) designating the CII as such;

(*b*) a written direction of the Commissioner under clause 12 or 16(2); or

(*c*) any provision in any code of practice or standard of performance that applies to the owner, or any amendment made to it.

An appeal must be made within 30 days (or such longer period allowed by the Minister) after the date of the notice or direction, or the issue, approval or amendment of the code of practice or standard of performance.

Before determining an appeal, the Minister may consult any Appeals Advisory Panel established under clause 18 to provide advice to the Minister in respect of the appeal. The Minister is not bound by the advice of the Panel, and the Minister's decision in any appeal is final.

Clause 18 empowers the Minister to establish an Appeals Advisory Panel to provide advice to the Minister in respect of an appeal, if the resolution or understanding of issues involved requires particular technical skills or specialised knowledge.

PART 4

RESPONSES TO CYBERSECURITY THREATS AND INCIDENTS

Part 4 empowers the Commissioner to respond to a cybersecurity threat or incident by exercising, or authorising the exercise of investigatory powers under clause 19 or 20, depending on the severity of the cybersecurity threat or incident. Part 4 also empowers the Minister to authorise the taking of emergency cybersecurity measures.

Clause 19 empowers the Commissioner to exercise or authorise the exercise by an incident response officer of information and record gathering powers as

necessary to investigate a cybersecurity threat or incident for the purpose of assessing its impact, preventing harm arising from the cybersecurity incident or preventing a further cybersecurity incident from arising. The powers which are to be exercised against persons affected by the cybersecurity threat or incident, typically the victims, are the following:

(*a*) require the person to attend at a specified place and time to answer questions or to provide a signed statement concerning the cybersecurity threat or incident;

(*b*) require the person to produce any record or document, or provide any relevant information to the incident response officer;

(*c*) inspect, copy or take extracts from such record or document;

(*d*) examine orally the person who appears to be acquainted with the facts and circumstances relating to the cybersecurity threat or incident.

Clause 19(6) provides that any person examined or who receives a notice under clause 19(2) or an order of a Magistrate under clause 19(5) is not obliged to disclose any information that is subject to any right, privilege or immunity conferred, or obligation or limitation imposed, by or under any law or rules of professional conduct in relation to the disclosure of such information, except that the performance of a contractual obligation is not an excuse for not disclosing the information. For example, the person is not obliged to produce to the incident response officer an email infected by a malicious program if that email contains information that is subject to legal privilege. However, the person is not entitled to withhold an infected email that is subject to a contractual obligation of confidentiality, and the person is not treated as in breach of that contractual obligation if the person produces that email with reasonable care and in good faith for the purpose of complying with a requirement made under clause 19.

Clause 20 empowers the Commissioner to exercise or authorise the exercise by an incident response officer of a set of more intrusive powers as necessary to investigate a cybersecurity threat or incident that satisfies the severity threshold in clause 20(3), for the purpose of assessing its impact, eliminating the cybersecurity threat or otherwise preventing harm arising from the cybersecurity threat or incident or preventing a further cybersecurity incident from arising. A cybersecurity threat or incident satisfies the severity threshold if —

(*a*) it creates a risk of significant harm being caused to a CII (even if the harm may not be of a nature that creates a risk of disruption to the provision of that essential service related to that CII);

(*b*) it creates a risk of disruption to the provision of an essential service;

(*c*) it creates a threat to the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore; or

(*d*) the cybersecurity threat or incident is of a severe nature, in terms of the severity of the harm that may be caused to persons in Singapore or the number of computers or value of the information put at risk, whether or not the computers or computer systems put at risk are themselves CII.

For the purpose of investigating a cybersecurity threat or incident that satisfies the severity threshold, the powers that may be exercised by an incident response officer against persons affected by the cybersecurity threat or incident, typically the victims, are the following:

(*a*) any power mentioned in clause 19(2)(*a*), (*b*), (*c*) or (*d*);

(*b*) direct the person to carry out such remedial measures, or to cease carrying on such activities, in relation to the affected computer or computer system, in order to minimise cybersecurity vulnerabilities;

(*c*) require the person to take any action to assist with the investigation, including but not limited to —

(i) preserving the state of the affected computer or computer system by not using it;

(ii) monitoring the affected computer or computer system;

(iii) performing a scan of the affected computer or computer system to detect cybersecurity vulnerabilities and to assess the impact of the cybersecurity incident; and

(iv) allowing the incident response officer to connect any equipment to, or install any computer program on, the affected computer or computer system as necessary;

(*d*) after giving reasonable notice, enter premises where the affected computer or computer system is reasonably suspected to be located;

(*e*) access, inspect and check the operation of the affected computer or computer system, or use the computer or computer system to search any data contained in or available to such computer or computer system;

(*f*) perform a scan of the affected computer or computer system to detect cybersecurity vulnerabilities;

(*g*) take a copy of or extracts from, any electronic record or computer program affected by the cybersecurity incident;

(*h*) with the consent of the owner, take possession of any computer or other equipment for the purpose of carrying out further examination or analysis.

Clause 20(5) also provides for the Commissioner to exercise the power to take possession of a computer or equipment for further examination or analysis where the owner does not consent, only if —

(*a*) the exercise of the power is necessary for the purposes of the investigation;

(*b*) there is no less disruptive method of achieving the purpose of the investigation;

(*c*) after consultation with the owner, and having regard to the importance of the computer or other equipment to the business or operational needs of the owner, the benefit from the exercise of the power outweighs the detriment caused to the owner; and

(*d*) the Commissioner has issued to the incident response officer a written authorisation to exercise the power.

Clause 21 requires every incident response officer to, when exercising any powers under Part 4, declare his or her office and produce on demand his or her identification card to any person affected by the exercise of that power.

Clause 22 empowers the Commissioner to appoint a cybersecurity technical expert to assist in an investigation by providing technical advice to an incident response officer.

Clause 23 re-enacts with slight modifications section 15A of the Computer Misuse and Cybersecurity Act (Cap. 50A), which will be repealed by clause 49. Clause 23 empowers the Minister to authorise or direct any person or organisation to take emergency cybersecurity measures and comply with necessary requirements, for the purposes of preventing, detecting or countering any serious and imminent threat to the provision of any essential service, or to the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore.

PART 5

CYBERSECURITY SERVICE PROVIDERS

Part 5 sets out the framework for the licensing of providers of licensable cybersecurity services. Certain cybersecurity services are prescribed as licensable cybersecurity services in the Second Schedule.

Clause 24 creates an offence for a person to engage in the business of providing a licensable cybersecurity service without a licence. This prohibition does not apply to the provision of a cybersecurity service by a company to its related company.

Clause 24 also creates an offence for a person to advertise or otherwise hold out that the person provides a licensable cybersecurity service, unless the person holds a licence.

Clause 25 designates the Commissioner as the licensing officer, and the officer responsible for the administration of Part 5. The Commissioner may appoint public officers as assistant licensing officers.

Clause 26 deals with the procedure relating to applications for the grant or renewal of licences. The applicant, who may be an individual or business entity, must if required provide such further information or evidence as may be requested by the licensing officer. The licensing officer may refuse to grant or renew a licence if —

(*a*) the applicant is not a fit and proper person to hold or continue to hold the licence; or

(*b*) it is not in the public interest to grant or renew the licence, or the grant or renewal of the licence may pose a threat to national security.

Clause 27 empowers the licensing officer, in granting a licence to an applicant, to impose such conditions as the licensing officer thinks fit to impose. The licensing officer may add to, modify or revoke the conditions of a licence after observing the process prescribed in the clause.

Clause 28 relates to the form and period of validity of a licence.

Clause 29 requires a licensee to keep a record of prescribed types of information for each occasion on which the licensee's services are engaged.

Clause 30 empowers the licensing officer to revoke or suspend a licence, censure the licensee or impose other conditions on the licensee, if prescribed conditions are satisfied and after giving the licensee an opportunity to be heard. An order of revocation or suspension takes effect at the end of 14 days after service of the notice of the order, unless the licensing officer states in the order that it is undesirable in the public interest for the licensee to continue to carry on the licensee's business as a licensee, in which case the order takes effect immediately upon service of the notice of the order.

Clause 31 provides that a provider of a licensable cybersecurity service is not entitled to bring any proceeding to recover any commission, fee, gain or reward unless the provider held a valid licence at the time of providing the service.

Clause 32 provides that a licensing officer may, in addition to or instead of taking action under clause 30(1) or (2), order a licensee to pay a financial penalty for a contravention of a provision of Part 5 that is not an offence or for failure to comply with a licence condition.

Clause 33 relates to the process that must be observed by the licensing officer before making an order for a licensee to pay any financial penalty. The licensee

may make representations before the date on which the order is intended to be made.

Clause 34 provides for the recovery of any financial penalty as a debt due to the Government. The licensing officer is empowered to waive, remit or refund in whole or in part any financial penalty imposed, or any interest due on any financial penalty.

Clause 35 provides for an avenue of appeal to the Minister against decisions made by the licensing officer.

PART 6

GENERAL

Clauses 36 and 37 are standard provisions for the liability of officers of offenders which are corporations or unincorporated bodies like partnerships and associations.

Clause 38 confers various powers for investigating an offence under the Bill (except an offence under clause 23).

Clause 39 allows an investigation officer to enter premises under a Magistrate's warrant, for the purposes of an investigation under clause 38.

Clause 40 confers jurisdiction on a District Court to try any offence under the Bill and to impose the full punishment for any such offence.

Clause 41 provides powers of composition that may be exercised by the Commissioner or any Assistant Commissioner authorised by the Commissioner.

Clause 42 deals with the service of documents permitted or required by the Bill to be served on a person. The clause does not deal with service of court documents, as these are regulated by other written laws.

Clause 43 is a confidentiality provision which provides that a person who is or has been the Commissioner, the Deputy Commissioner, an Assistant Commissioner, a cybersecurity officer, an authorised officer, a member of an Appeals Advisory Panel, a cybersecurity technical expert or an assistant licensing officer, or the Minister or a person assisting the Minister, must not disclose certain information which has come to the person's knowledge in the performance of his or her functions, or the discharge of his or her duties, under the Bill, except in the circumstances specified in the clause.

Clause 44(1) is a standard provision providing immunity from suits for any act of the Commissioner, the Deputy Commissioner, an Assistant Commissioner, a cybersecurity officer, an authorised officer, an assistant licensing officer, a member of an Appeals Advisory Panel or any other person acting under the direction of the Commissioner, who, acting in good faith and with reasonable care, does or omits to

do anything in the exercise or purported exercise of any power under the Bill or the performance or purported performance of any function or duty under the Bill.

Clause 44(2) confers upon the Commissioner, and any person acting under the Commissioner's direction, protection from liability for any error or omission appearing in any information supplied to the public under a service pursuant to any written law, if made in good faith and despite the exercise of reasonable care in the discharge of the duties of the Commissioner or such person.

Clause 45 relates to the protection of the identity of informers of offences under Part 3.

Clause 46 confers on the Minister power to exempt, by order in the *Gazette*, any person or any class of persons from all or any of the provisions of the Bill.

Clause 47 empowers the Minister to amend the First or Second Schedule by order in the *Gazette*, and to make transitional, incidental, consequential or supplementary provision as necessary or expedient.

Clause 48 confers on the Minister the power to make regulations for the purposes of the Bill.

Clause 49 provides for related amendments to the Computer Misuse and Cybersecurity Act.

Clause 50 provides for consequential amendments to certain Acts.

Clause 51 contains saving and transitional provisions. The clause also confers on the Minister the power to make regulations of a saving or transitional nature, in the 2 years after the date of commencement of any provision of the Bill.

The First Schedule sets out a list of essential services.

The Second Schedule sets out the licensable cybersecurity services for the purposes of the Bill. Two cybersecurity services — managed security operations centre (SOC) monitoring service and penetration testing service — are prescribed as licensable cybersecurity services.

EXPENDITURE OF PUBLIC MONEY

This Bill will not involve the Government in any extra financial expenditure.