Cybersecurity Bill

Bill No. /2017.

Read the first time on .

A BILL

i n t i t u l e d

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 establish a framework for the sharing of cybersecurity information, to regulate cybersecurity service providers, and for matters related thereto, and to make 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 2017 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 —

"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 other device as the Minister may, by notification in the Gazette, prescribe;

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

(*a*) an information technology (IT) system; and

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

"critical information infrastructure" means a computer or a computer system that is necessary for the continuous delivery of essential services which Singapore relies on, the loss or compromise of which will lead to a debilitating impact on the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore.

"cybersecurity" means the security of a computer or computer system against unauthorised access or attack, to preserve the availability and integrity of the computer or computer system, or the confidentiality of information stored or processed therein;

"cybersecurity incident" means an act or activity on or through a computer or computer system, that jeopardised or adversely impacted, without lawful authority, the security, availability or integrity of a computer or computer system, or the availability, confidentiality or integrity of information stored on, processed by, or transiting a computer or computer system;

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

"cybersecurity threat" means an act or activity on or through a computer or computer system, which is known or suspected, that may imminently jeopardise or adversely impact, without lawful authority, the security, availability or integrity of a computer or computer system, or the availability, confidentiality or integrity of information stored on, processed by, or transiting a computer or computer system.

"essential services" means any of the services specified in the First Schedule;

["information system" means [a computer system or a set of components for collecting, creating, storing, processing, and distributing information, typically including hardware and software, system users, and the data itself];]

"full-time national serviceman" means a person who has been directed to present himself for enlistment under the provisions of any written law for the time being in force relating to national service or enlistment;

"owner of a critical information infrastructure" means a person who —

(*a*) has effective control over the operations of the critical information infrastructure and has the ability and right

to carry out changes to the critical information infrastructure; or

(*b*) is responsible for ensuring the continuous functioning of the critical information infrastructure.

(2) Where a critical information infrastructure is owned or operated by the Government or a statutory body, the owner of the critical information infrastructure is, for the purposes of this Act, deemed to be —

(*a*) the Permanent Secretary of the Ministry, which owns or operates the critical information infrastructure, having responsibility for the approval of budget and expenditure in relation to the critical information infrastructure; or

(*b*) the Chief Executive, or similar officer known by any other designation, of the statutory body, which owns or operates the critical information infrastructure.

Application of Act

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

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

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

(4) For the avoidance of doubt, no person is immune from prosecution for any offence under this Act by reason that the person is an employee of 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, by notification in the Gazette, appoint —

(*a*) an officer to be known as the Commissioner of Cybersecurity; and

(*b*) a Deputy Commissioner and such numbers of Assistant Commissioners of Cybersecurity as the Minister may think necessary to assist the Commissioner in the proper discharge of the Commissioner's duties and functions.

(2) The Minister may under subsection (1)(*b*), appoint as an Assistant Commissioner —

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

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

where that other Ministry has supervisory or regulatory responsibility over an industry to which one or more owner of a critical information infrastructure belongs.

(3) The Minister may in writing appoint such number of cybersecurity officers, either temporary or permanent, as the Minister may think necessary for carrying this Act into effect.

(4) The Commissioner is, subject to any general or special directions of the Minister, 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 which are exercisable under sections [7, 12….].

(6) Subject to such conditions or limitations as the Commissioner may specify, an Assistant Commissioner and a cybersecurity officer have 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 those which are exercisable under sections [7, 12, 21(4)….].

Duties and functions of Commissioner of Cybersecurity

5. The Commissioner has the following duties and functions:

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

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

(*c*) to monitor cybersecurity threats and respond to cybersecurity incidents that threaten Singapore's national security, defence, economy, foreign relations, public health, public order, public safety, or essential services, whether such cybersecurity threats or incidents occur in or outside Singapore;

(*d*) to identify and designate critical information infrastructure;

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

(*f*) to represent the Government and advance Singapore's interests on cybersecurity issues internationally;

(*g*) to cooperate with Computer Emergency Response Teams ("CERTs") internationally on cybersecurity incidents;

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

(*i*) to establish standards and to promulgate regulations in relation to cybersecurity practitioners and cybersecurity products or services within Singapore, including certification or accreditation schemes;

(*j*) to promote, develop, maintain and improve competencies, expertise and professional standards in the cybersecurity community;

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

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

(*m*) 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 consultation with the Minister, in writing appoint any of the following persons to be an authorised officer to assist the Commissioner in carrying Part 4 of this Act into effect:

(*a*) a public officer;

(*b*) an officer of any statutory authority;

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

(2) In exercising any of the powers of enforcement under this Act, 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 a written notice, designate a 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 fulfils the criteria of a critical information infrastructure; and

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

(2) Any notice made under subsection (1) must —

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

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

(*c*) inform the owner of the critical information infrastructure, regarding the owner's duties and responsibilities under the Act that arise from the designation;

(*d*) provide the name and contact particulars of the Assistant Commissioner appointed to oversee the critical information infrastructure.

(*e*) inform the owner that any representations against the designation are to be made to the Commissioner not later than 14 days after the date of the notice; and

(*f*) inform the owner of the avenue to appeal to the Minister against the designation, and the applicable procedure.

(3) Any notice made under subsection (1) continues to have effect for a period of 5 years unless it is withdrawn by the Commissioner before the expiry of the period.

(4) An owner of a computer or computer system that is designated as a critical information infrastructure by a notice under

subsection (1) must, not later than 14 days after the receipt of the notice —

(*a*) acknowledge receipt of the notice in writing; and

(*b*) appoint a contact person for the critical information infrastructure.

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

8.—(1) Where the Commissioner has reason to suspect that a computer or computer system may fulfil the criteria of a critical information infrastructure, the Commissioner may by notice in the form and manner prescribed, require any person who appears to be operating the computer or computer system, to provide to the Commissioner, within a reasonable period specified in the notice, all such relevant information relating to that computer or computer system as may be required by the Commissioner.

(2) Without prejudice to the generality of subsection (1), the Commissioner may in a notice issued under that subsection require any person who appears to be operating the computer or computer system to provide —

(*a*) information relating to —

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

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

(*b*) technical information relating to the information described in paragraph (*a*); 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.

(3) Subject to subsection (5), any person to whom a notice is issued under subsection (1) must comply with the notice.

(4) Any person who fails to comply with a notice issued 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 thereof during which the offence continues after conviction.

(5) Any person to whom a notice is issued under subsection (1) is not obliged to disclose any information where the person is prohibited by any written law from disclosing 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.

[Confidentiality provision]

Duties of owner of critical information infrastructure

10. An owner of a critical information infrastructure has the duty to —

(*a*) provide the Commissioner with information on the technical architecture of the critical information infrastructure;

(*b*) comply with such codes of practice, standards of performance or directions in relation to the critical information infrastructure as may be issued by Commissioner;

(*c*) notify the Commissioner of —

(i) any cybersecurity incident that occurs in respect of the critical information infrastructure;

(ii) any cybersecurity incident that occurs in respect of any computer or computer system under the owner's control that is interconnected with or communicates with the critical information infrastructure; and

(iii) any cybersecurity incident of a type as prescribed by notification or as specified by the Commissioner.

(*d*) cause regular audits of the compliance of the critical information infrastructure with the Act, codes of practice and standards of performance to be carried out by an auditor approved or appointed by the Commissioner;

(*e*) carry out regular risk assessments of the critical information infrastructure as required by the Commissioner; and

(*f*) participate in cybersecurity exercises as required by the Commissioner.

Technical information relating to critical information infrastructure

11.—(1) The Commissioner may by notice in the form and manner prescribed, require an 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 that is interconnected with or communicates with the critical information infrastructure;

(*c*) information relating to the operation of the critical information infrastructure, including any other computer or computer system that is interconnected with or communicates with the critical information infrastructure;

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

(2) If material changes are made to the design, configuration, security or operation of the critical information infrastructure after the 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 changes not later than 30 days after the changes are made.

(3) The owner to whom a notice is issued under subsection (1) is not obliged to disclose any information where the owner is prohibited by any written law from disclosing such information.

(4) Subject to subsection (3), an owner of a critical information infrastructure who, in good faith, discloses any information to the Commissioner under this section is not treated as being in breach of any restriction upon the disclosure of information imposed by law, contract or rules of professional conduct.

(5) For the purposes of subsection (2), a change is a material change if the change affects or may potentially affect the cybersecurity of the critical information infrastructure or the ability of the owner to respond to a cybersecurity incident affecting the critical information infrastructure.

(6) An 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 thereof during which the offence continues after conviction.

(7) An owner of a critical information infrastructure who fails, without reasonable excuse, 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 [1 year] or to both.

Codes of practice or standards of performance

12.—(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 cybersecurity of 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 issued or approved by the Commissioner is inconsistent with any provision of this Act, such provision, to the extent of the inconsistency —

(*a*) has effect subject to the provisions of this Act; or

(*b*) having regard to the provisions of this Act, 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, of the code of practice or standard of performance in such manner as will secure adequate publicity for such issue, approval, amendment or revocation;

(*b*) specify in the notice referred to in paragraph (*a*) 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 to an owner of a critical information infrastructure free of charge.

(4) No code of practice or standard of performance, no amendment to an approved code of practice or standard of performance, and no revocation of any such approved code of practice or standard of performance, has any force or effect as an approved code of practice or standard of performance until the notice relating thereto is published in accordance with subsection (3).

(5) Any code of practice or standard of performance issued or approved by the Commissioner under this section does not have legislative effect.

(6) Subject to subsection (7), every owner of a critical information infrastructure must comply with the relevant codes of practice and standards of performance issued or approved under this section.

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

(8) In this section, a reference to code of practice includes recommended technical standards.

Power of Commissioner to issue written directions

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

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

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

issue written directions, either of a general or specific nature, or for or with respect to codes of practice or standards of performance, to any owner of a critical information infrastructure, and that owner or class of owners must comply with such directions within the period specified in the direction.

(2) Without prejudice to the generality of subsection (1), any written direction issued under that subsection may relate to —

(*a*) the appropriate actions to be taken by an owner of a critical information infrastructure or class of such owner, in relation to a cybersecurity threat;

(*b*) the appointment of an auditor approved by the Commissioner to audit the owner or class of owner, on the cybersecurity of its critical information infrastructure; and

(*c*) such other matters as the Commissioner may consider necessary or expedient or in the interests of the cybersecurity of critical information infrastructure.

(3) A direction under subsection (1) —

(*a*) is to require the owner of a critical information infrastructure concerned (according to the circumstances of the case) to do, or not to do, such things as are specified in the direction or are of a description as specified therein;

(*b*) takes effect at such time, being the earliest practicable time, as is determined by or under that direction; and

(*c*) may be revoked at any time by the Commissioner.

(4) Before giving a direction to any owner of a critical information infrastructure under subsection (1), the Commissioner must, unless the Commissioner in respect of any particular direction considers that it is not practicable or desirable, give notice —

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

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

and must consider any representations or objections which are duly made.

(5) Any person who fails to comply with a written direction issued 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 thereof during which the offence continues after conviction.

Change in ownership of critical information infrastructure

14.—(1) An owner of a critical information infrastructure must inform the Commissioner of any intended change in ownership of the critical information infrastructure, not later than 90 days before the date of the intended change in ownership.

(2) Any owner of a critical information infrastructure who 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.

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

15.—(1) An owner of a critical information infrastructure must notify the Commissioner in such manner and form as may be prescribed, within the prescribed period after the occurrence of any of the following events:

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

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

(*c*) any other type of cybersecurity incident in respect of the critical information infrastructure that the Minister may prescribe by notification or the Commissioner may specify by written direction.

(2) An owner of a critical information infrastructure must establish mechanisms and processes as may be necessary in order to detect any cybersecurity threat in respect of its critical information infrastructure.

(3) Any owner of a critical information infrastructure who 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

16.—(1) An owner of a critical information infrastructure must, at least once every three years —

(*a*) cause an audit, of the compliance of the owner's critical information infrastructure with respect to the Act, codes of practice and standards of performance, to be carried out by an auditor approved or appointed by the Commissioner; and

(*b*) conduct a cybersecurity risk assessment of the owner's critical information infrastructure.

(2) The owner of a 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 respective report to the Commissioner.

(3) Where it appears to the Commissioner from the audit report 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 further steps to address those aspects.

(4) Where it appears to the Commissioner —

(*a*) that any owner of a critical information infrastructure is not in compliance with a provision of the Act, code of practice or standard of performance; or

(*b*) that any information provided by any owner of a critical information infrastructure under section 11 is false, misleading, inaccurate or incomplete,

the Commissioner may by order require an audit of the owner's critical information infrastructure to be carried out by a person appointed by the Commissioner.

(5) Where it appears to the Commissioner from the cybersecurity risk assessment report furnished under subsection (2) that the cybersecurity risk 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 cybersecurity of the critical information infrastructure; or

(*b*) appoint a cybersecurity service provider to conduct a cybersecurity risk assessment of the critical information infrastructure.

(6) Where the owner of a critical information infrastructure has notified the Commissioner under section 11(2) of material changes

made to the design, configuration, security or operation of the critical information infrastructure, or the Commissioner has otherwise become aware of such material changes having been made, the Commissioner may by written notice, direct the owner of the critical information infrastructure to carry out an audit or cybersecurity risk assessment mentioned in subsection (1) outside the time interval mentioned in that subsection.

(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);

(*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 thereof during which the offence continues after conviction.

(8) Any owner of a critical information infrastructure who 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 [1 year] or to both and, in the case of a continuing offence, to a further fine not exceeding [$2,500] for every day or part thereof during which the offence continues after conviction.

National cybersecurity exercises

17.—(1) The Commissioner may conduct national cybersecurity exercises for the purposes of testing the state of readiness of owners of different critical information infrastructure in responding to significant cybersecurity incidents at the national level.

(2) An owner of a critical information infrastructure must participate in any national cybersecurity exercises as directed in writing by the Commissioner.

(3) Any person who fails to comply with a written direction 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 thereof during which the offence continues after conviction.

Appeal to Minister

18.—(1) Any owner of a critical information infrastructure who is aggrieved by —

(*a*) any decision of the Commissioner under section 7(1) designating the computer or computer system as a critical information infrastructure;

(*b*) any written direction of the Commissioner under section 13 or 17(2); or

(*c*) anything contained in any code of practice or standard of performance applicable to the owner,

may, within 30 days after the date of the notice or direction, or the issue or approval of the code of practice or standard of performance, as the case may be, (or such longer period as the Minister allows in exceptional circumstances, whether before or after the end of the 30 days), appeal to the Minister in the manner prescribed.

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

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

(*b*) submit to the Minister all relevant facts, evidence and arguments for or against the appeal, as the case may be.

(3) 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 mentioned in that subsection,

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 to provide such information must provide it in such manner and within such period as may be specified by the Minister.

(4) The Minister may reject any appeal of an appellant who fails to comply with subsection (2) or (3).

(5) Unless otherwise provided by this Act or 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.

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

(*a*) by confirming, varying or reversing any decision, notice or direction of, or code of practice or standard of performance issued by, the Commissioner; or

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

(7) Before determining an appeal under subsection (6) and for the purpose of forming an opinion on which to base such determination, the Minister may consult such 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 such consultation.

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

(9) The Minister may make rules 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

19.—(1) Where the Minister considers that an appeal lodged under section 18(1) involves issues of such nature or complexity that it ought to be considered and determined by persons with particular technical or other specialised knowledge, the Minister may establish by direction an Appeals Advisory Panel, comprising one or more of such persons with particular technical or other specialised knowledge and such other persons as the Minister considers appropriate, to provide advice to the Minister with regard to the discharge of the Minister's functions under section 18 in respect of any appeal that has been made to the Minister under section 18(1).

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

(*a*) determine or vary the terms of reference of the Appeals Advisory Panel;

(*b*) appoint persons 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 the procedure to be adopted by the Appeals Advisory Panel in considering any matter referred to it;

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

(3) An Appeals Advisory Panel may regulate its proceedings 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 and forms part of the expenses of the Commissioner.

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

PART 4

RESPONDING TO AND PREVENTION OF CYBERSECURITY INCIDENTS

Powers to investigate and prevent cybersecurity incidents

20.—(1) Where information regarding a cybersecurity threat or a cybersecurity incident has been received by the Commissioner, the Commissioner may exercise, or may authorise the Deputy Commissioner, an Assistant Commissioner or a cybersecurity officer to exercise, such of the following powers as may be necessary to determine the impact or potential impact of the cybersecurity threat or cybersecurity incident, to prevent further harm arising from the cybersecurity incident, or to prevent a further cybersecurity incident from arising from that cybersecurity threat or cybersecurity incident:

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

(*b*) require, by written notice, any person to produce to the investigating officer any physical or electronic record, document or copy thereof in the possession of that person, or to provide the investigating officer with any information, which the investigating officer considers to be related to any matter relevant to the investigation, and without giving any fee or reward, inspect, copy or take extracts from such record or document;

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

(2) The investigating officer may specify in the notice mentioned in subsection (1)(*b*) —

(*a*) the time and place at which any record or document 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.

(3) Any person examined under this section is bound to state truly what the person knows of the facts and circumstances concerning matters under this Act, except that the person need not say anything that might expose that person to a criminal charge, penalty or forfeiture.

(4) A statement made by any 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) A person examined under this section who, in good faith, discloses any information to an investigating officer is not treated as being in breach of any restriction upon the disclosure of information imposed by law, contract or rules of professional conduct.

(6) If any person fails to attend as required by a written notice under subsection (1)(*a*), the investigating 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 written notice.

(7) Any person who —

(*a*) wilfully mis-states or without lawful excuse refuses to give any information or produce any record, document or copy thereof required of the person by the investigating officer under subsection (1); or

(*b*) fails, without reasonable excuse, to comply with a lawful demand of the investigating officer in the discharge by the investigating officer of the investigating officer's duties under this section,

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.

(8) In this section and sections 21, 22 and 23, "investigating officer" means the Commissioner, Deputy Commissioner, any Assistant Commissioner or cybersecurity officer exercising the powers of investigation under this section or section 21, as the case may be.

Powers to investigate and prevent serious cybersecurity incidents

21.—(1) Where information has been received by the Commissioner regarding a cybersecurity threat or a cybersecurity incident that satisfies the severity threshold in subsection (2), the Commissioner may exercise, or may authorise the Deputy Commissioner, an Assistant Commissioner or a cybersecurity officer to exercise, such of the following powers as may be necessary to determine the impact or potential impact of the cybersecurity threat or cybersecurity incident, to prevent further harm arising from the cybersecurity incident, or to prevent a further cybersecurity incident from arising from that cybersecurity threat or cybersecurity incident:

(*a*) any power mentioned in section 20(1)(*a*), (*b*) or (*c*);

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

Explanation — The remedial measures directed to be carried out may include —

(*a*) the cleaning up of computers that have been infected by malware;

(*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 to designated computer servers.

(*c*) require the owner of a computer or computer system to carry out steps 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

(iv) allowing the investigating officer to install on the computer or computer system any software program, or interconnect any equipment to the computer or computer system, for the purpose of the investigation.

(*d*) after producing the investigating officer's identification card on demand being made, enter with reasonable notice any premises owned or occupied by any person suspected to have within the premises a computer or computer system that the investigating officer has reasonable cause to suspect is or was impacted by a cybersecurity incident;

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

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

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

(*h*) subject to subsection (4) or with the consent of the owner, take possession of any computer or other equipment for the purpose of carrying out further examination or analysis.

(2) A cybersecurity incident or cybersecurity threat satisfies the severity threshold mentioned in subsection (2) if —

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

(*b*) it creates a real risk of disruption being caused to the delivery of an essential service;

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

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

(3) The investigating officer exercising the power mentioned in subsection (1)(*e*) may require any assistance the investigating officer needs to gain such access from —

(*a*) any person whom the investigating officer reasonably suspects of using or having used the computer impacted by the cybersecurity incident; or

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

(4) Where the owner of the computer or other equipment does not consent to the exercise of the power mentioned in subsection (1)(*h*), the power may be exercised only after the Commissioner has issued to the investigating officer a written authorisation after being 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.

(5) Any person who —

(*a*) wilfully mis-states or without lawful excuse refuses to give any information or produce any record, document or copy thereof required of the person by the investigating officer under subsection (1)(*a*); or

(*b*) fails, without reasonable excuse, to comply with a lawful demand of the investigating officer in the discharge by the investigating officer of the investigating 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 investigating officer

22. Every investigating officer, when exercising any of the powers under this Part, must declare the investigating 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 investigation officer when exercising such power.

Appointment of cybersecurity technical experts

23.—(1) The Commissioner may, in writing, appoint any of the following individuals to be a cybersecurity technical expert for a specified period to assist any investigating officer in the investigating officer's exercise of any powers under section 20 or 21:

(*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 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.

(3) 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 under any provision in this Act.

(4) A cybersecurity technical expert whose appointment as such ceases must return any identification card issued to the cybersecurity technical expert under subsection (3) to the Commissioner.

(5) An individual mentioned in subsection (1)(*b*) [or (*c*)] who is appointed as a cybersecurity technical expert under that subsection does not, by virtue only of that appointment, become an employee or agent of the Government.

Emergency cybersecurity measures and requirements

24.—(1) Where the Minister is satisfied that it is necessary for the purposes of preventing, detecting or countering any threat to the essential services or national security, defence, foreign relations, economy, public health, public safety or public order of Singapore, the Minister may, by a certificate under the Minister's hand, authorise or direct any person or organisation specified in the certificate (referred to in this section as 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 [service][system] or any class of computers or computer [services][systems].

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

(*a*) the exercise by the specified person of the powers referred to 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 [service][system]; and

(ii) information relating to the security of any computer, computer program or computer [service][system];

(*c*) providing to the Minister or [the Commissioner][a public officer authorised by the Minister] 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 [service][system]; and

(ii) information relating to the security of any computer, computer program or computer [service][system]; and

(*d*) providing to the Minister or [the Commissioner][a public officer authorised by the Minister] a report of a breach or an attempted breach of security 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 referred to 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 notwithstanding 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 to be treated as being 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][a public officer authorised by the Minister], 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 [service][system] or class of computers or computer [services][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, the Computer Misuse and Cybersecurity 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

Interpretation of this Part

25.—(1) In this Part, unless the context otherwise requires —

"cybersecurity service" means a service provided 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;

"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;

"investigative cybersecurity service" means any cybersecurity service that is investigative in nature and —

(*a*) involves circumventing the controls implemented in another person's computer or computer system; or

(*b*) requires the person performing the service to obtain a deep level of access to the computer or computer system in respect of which the service is being performed, or to test the cybersecurity defences of the computer or computer system,

thereby giving rise to a potential for significant harm to be caused to the computer or computer system, and includes the following:

(*i*) assessing, testing or evaluating the cybersecurity of a computer or computer system of another person by searching for vulnerabilities in, and compromising, the cybersecurity defences of the computer or computer system;

(*ii*) conducting a forensic examination of a computer or computer system;

(*iii*) investigating and responding to a cybersecurity incident that has affected a computer or computer system by conducting a thorough scan and examination of the computer or computer system to identify and eradicate, and identify the root cause of, the cybersecurity threat, and which involves circumventing the controls implemented in the computer or computer system;

(*iv*) conducting a thorough examination of a computer or computer system to detect any cybersecurity threat that may have already penetrated the cybersecurity defences of the computer or computer system, and that may have evaded detection by conventional cybersecurity solutions.

"licensable cybersecurity service" means any licensable investigative cybersecurity service or licensable non-investigative cybersecurity service;

"licensable investigative cybersecurity service" means any investigative cybersecurity service specified as a licensable investigative cybersecurity service in Part 1 of the Second Schedule;

"licensable non-investigative cybersecurity service" means any non-investigative cybersecurity service specified as a licensable non-investigative cybersecurity service in Part 2 of the Second Schedule;

"non-investigative cybersecurity service" means any cybersecurity service that is not an investigative cybersecurity service, and includes the following activities:

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

(*b*) monitoring of the cybersecurity of a computer or computer system of another person by acquiring, identifying and scanning information that is stored on, processed by, or transiting the computer or computer

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

(*c*) maintaining control of the cybersecurity of a computer or computer system of another person by effecting management, operational and technical controls for the purpose of protecting against an unauthorised effort to adversely affect the cybersecurity of the computer or computer system;

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

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

(i) providing advice on a cybersecurity product; or

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

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

(*g*) 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.

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

(*a*) sells self-install computer programs intended for the protection of the cybersecurity of a computer; or

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

No person to [carry out][perform] licensable investigative cybersecurity service without licence

26.—(1) No person may —

(*a*) [carry out][perform], for reward (whether in the course of business or of employment), any licensable investigative cybersecurity service; or

(*b*) advertise, or in any way hold out, that the person [carries out][performs] or is willing to [carry out][perform] for reward any licensable investigative cybersecurity service,

except under and in accordance with an investigative cybersecurity service practitioner's licence granted under this Act.

(2) Any person who contravenes subsection (1) 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 2 years or to both.

(3) This section does not apply to a person employed under a contract of service by another person to carry out an investigative cybersecurity service for a computer or computer system belonging to that other person.

No person to supply licensable investigative cybersecurity practitioners without licence

27.—(1) No person may —

(*a*) engage in the business of supplying to other persons, for reward, the services of investigative cybersecurity practitioners for the [carrying out][performance] of a licensable investigative cybersecurity service; or

(*b*) advertise, or in any way hold out, that the person supplies for reward, or is willing to supply for reward, the services of investigative cybersecurity practitioners for the [carrying out][performance] of a licensable investigative cybersecurity service,

except under and in accordance with [a licensable][an] investigative cybersecurity service provider's licence granted under this Act.

(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.

Employees who are investigative cybersecurity service practitioners

28.—(1) No person may employ another person as an investigative cybersecurity service practitioner for the [carrying out][performance] of a licensable investigative cybersecurity service unless the other person is a licensed investigative cybersecurity service practitioner.

(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.

No person to provide licensable non-investigative cybersecurity service without licence

29.—(1) No person may —

(*a*) engage in the business of providing, for reward, any licensable non-investigative cybersecurity service to other persons; or

(*b*) advertise, or in any way hold out, that the person (who is in the business of providing a licensable non-investigative cybersecurity service) provides for reward, or is willing to provide for reward, the licensable non-investigative cybersecurity service,

except under and in accordance with a [licensable] non-investigative cybersecurity service provider's licence granted under this Act.

(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.

Licensing officer and assistant licensing officers

30.—(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 Commissioner may appoint such number of public officers to be assistant licensing officers as are necessary to assist the Commissioner in carrying out the Commissioner's functions and duties under this Part.

(3) The functions and duties conferred on the Commissioner by this Part may be performed by any assistant licensing officer appointed by the Commissioner under subsection (2) and subject to the direction and control of the Commissioner.

(4) The Minister may from time to time give to the Commissioner 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 Commissioner must comply with any direction so given.

Grant and renewal of licence

31.—(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 fees, 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 as the late renewal period) as may be prescribed.

(2) An applicant for a licence must, at the request of the licensing officer, provide any 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, with or without conditions; or

(*b*) refuse the application.

(4) Subject to the provisions of this Act, a person who applies to be licensed, or to renew the person's licence, is eligible to be granted a licence or a renewal of the licence if, and only if —

(*a*) the applicant has paid the prescribed fees for such licence or its renewal;

(*b*) where the applicant is an individual, the applicant satisfies the licensing officer that the applicant has the qualifications and the practical experience (whether in Singapore or elsewhere) prescribed for that licence; and

(*c*) the applicant satisfies such other requirements as may be prescribed for such licence or its renewal.

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

(*a*) where the person who applies to be licensed, or to renew the person's licence is an individual, the person is not a fit or proper person to hold or to continue to hold the licence;

(*b*) where the person who applies to be licensed, or to renew the person's licence is a business entity, an officer of the business entity is not a fit or proper person; 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 late 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 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*) by the intentional suppression of any material fact, furnishes any information which 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 [1 year] or to both.

(8) In deciding for the purposes of this section whether a person or an officer of a business entity is a fit and proper person, the licensing officer may consider any of the following matters as indicating that the person or officer may not be a fit and proper person:

(*a*) that the person or officer associates with a criminal in a way that indicates involvement in an unlawful activity;

(*b*) that in dealings in which the person or officer has been involved, the person or officer has shown dishonesty or lack of integrity;

(*c*) that the person or officer is or was suffering from a mental disorder;

(*d*) that the person or officer is an undischarged bankrupt or has entered into a composition with the debtors of the person or officer;

(*e*) that the person or officer has had a licence revoked by the licensing officer previously.

(9) Subsection (8) does not limit the circumstances in which a person or an officer of a business entity may be considered by the licensing officer not to be a fit and proper person.

Conditions of licence

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

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

(3) Before making any modification to the conditions of a licence under this section, 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 from the date of service of notice on the licensee concerned) within which written representations with respect to the proposed modification may be made.

(4) Upon receipt of any written representation mentioned in subsection (3)(*b*), the licensing officer must consider the representation and may —

(*a*) reject the representation; or

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

and, in either case, must thereupon issue a direction in writing to the licensee concerned requiring that effect be given to the proposed modification specified in the notice or to such modification as subsequently amended by the licensing officer within a reasonable time.

(5) A licensee who fails to comply with any licence condition of the licence 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 [1 year] or to both.

Form and validity of licence

33.—(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 may be specified therein, from the date of its issue under this Act.

(3) A licence that has been renewed in accordance with the provisions of this Part continues in force for such period (not

exceeding 5 years) as the licensing officer may specify in writing to the licensee, from the date immediately following that on which, but for its renewal, the licence would have expired.

Duty to keep records

34.—(1) A licensed cybersecurity service provider who holds a licence mentioned in section 27 or 29 must —

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

(i) the name and address of the person engaging those services;

(ii) the date on which the services are provided;

(iii) details of the services provided; and

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

(*b*) retain every such record for a period of not less than the following minimum retention period from the date of the occasion to which the record relates:

(i) in the case of a licensee holding a licence mentioned in section 27 — 5 years;

(ii) in the case of a licensee holding a licence mentioned in section 29 — 3 years.

(2) Every person required under this section to keep records must furnish to the licensing officer such records at such time and in such format and through such medium (whether electronic or otherwise) as the licensing officer may require.

(3) Any person who contravenes 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 [1 year] or to both.

(4) If a person who is required under this section to keep or submit records —

(*a*) makes a record that —

(i) is false or misleading; or

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

(*b*) knows that the record is as described in paragraph (*a*); and

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

the person 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 2 years or to both.

(5) Subsection (4) shall not apply —

(*a*) if the record is not false or misleading in a material particular; or

(*b*) if the record did not omit any matter or thing without which the record is misleading in a material particular.

Revocation or suspension of licence

35.—(1) Subject to subsection (3), 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 imposed by the licensing officer on the licence;

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

(*c*) a circumstance which the licensing officer becomes aware of would have required or permitted the licensing officer to refuse to grant or renew the licensee's licence, had the licensing officer been aware of the circumstance immediately before the licence was granted or renewed;

(*d*) the licensee holding a licence mentioned in section 27 or 29 has ceased to carry on in Singapore the business or activity 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 dishonesty;

(*g*) where the licensee is an individual — the licensee is no longer a fit and proper person to continue to hold the licence;

(*h*) where the licensee is a business entity — an officer of the business entity is no longer a fit and proper person; or

(*i*) it is in the public interest to do so.

(2) Subject to subsection (3), 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 directions or restrictions as the licensing officer considers appropriate on —

(i) the holder of an investigative cybersecurity service practitioner's licence mentioned in section 26; or

(ii) on the licensee's business or functions as a licensed cybersecurity service provider.

(3) The licensing officer must not exercise the licensing officer's powers under subsection (1) or (2) unless an opportunity of being heard (whether in person or by a representative and whether in writing or otherwise) had been given to the licensee against whom the licensing officer intends to exercise the licensing officer's powers, being a period of not more than 14 days after the licensing officer informs the licensee of such intention.

(4) 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 made under those subsections.

(5) Despite subsection (3), where a licensee has been charged with or convicted of a prescribed offence, being an offence which would make it undesirable in the public interest for the licensee to continue to carry out the functions of a licensee —

(*a*) the licensing officer may serve on the licensee a notice of immediate suspension of the licence, which takes immediate effect and remains in force until the licensing officer makes an order under subsection (7) and any appeal to the Minister under section 37 against such an order is determined; and

(*b*) the licensee must, upon a notice being served under paragraph (*a*) but subject to subsection (7), immediately cease to carry out any function of a licensee to which the licence refers.

(6) A licensee whose licence has been suspended with immediate effect under subsection (5) may, within 14 days after the licensing officer has served the notice of immediate suspension under paragraph (*a*) of that subsection, apply to the licensing officer to review the licensing officer's decision under subsection (7).

(7) The licensing officer may, on reviewing the licensing officer's decision, by order —

(*a*) revoke the licence in question;

(*b*) suspend that licence for a period not exceeding 6 months starting from the date of immediate suspension of that licence; or

(*c*) rescind the immediate suspension of that licence.

(8) Where the licensing officer has by order revoked or suspended a licence under subsection (7) in respect of a licensee, the licensing officer must serve on the licensee concerned a notice of the order made under that subsection.

(9) Subject to section 37, an order under subsection (1), (2) or (7)(*a*) or (*b*) by the licensing officer revoking or suspending a licence does not take effect until the expiration of 14 days after notice has been served on the licensee under subsection (4) or (8).

(10) In any proceedings under this section in relation to the conviction of a licensee for a criminal offence, the licensing officer is to accept the licensee's conviction as final and conclusive.

(11) In deciding for the purposes of this section whether a person or an officer of a business entity is a fit and proper person, the

licensing officer may consider any of the following matters as indicating that the person or officer may not be a fit and proper person:

(*a*) that the person or officer associates with a criminal in a way that indicates involvement in an unlawful activity; or

(*b*) that in dealings in which the person or officer has been involved, the person or officer has shown dishonesty or lack of integrity.

(12) Subsection (11) does not limit the circumstances in which a person or an officer of a business entity may be considered by the licensing officer not to be a fit and proper person.

Effect of revocation or suspension of licence

36.—(1) Where an order of revocation or suspension of a licence becomes effective —

(*a*) the licensing officer must cause notice of the revocation or suspension to be served on the licensee concerned; and

(*b*) the licensee concerned must, as from the date of the notice, cease to carry on business or any function as a licensee in Singapore except to the extent allowed by the licensing officer.

(2) Subsection (1)(*b*) does not prejudice the enforcement by any person of any right or claim against the corporation, partnership or limited liability partnership or by the corporation, partnership or limited liability partnership of any right or claim against any person.

Appeal to Minister

37.—(1) Any person whose application for a licence or for the renewal of a licence has been refused by the licensing officer may, within 14 days after being notified of such refusal, appeal in the prescribed manner to the Minister whose decision is final.

(2) Where a licence is granted or renewed by the licensing officer subject to conditions, the licensee concerned may, within 14 days after being notified of such conditions, appeal in the prescribed manner to the Minister whose decision is final.

(3) If the licensing officer has made any order under section 35(1), (2) or (7)(*a*) or (*b*) in respect of any licensee, the licensee concerned may, within 14 days after being served with the notice of the order, appeal to the Minister against the order, and the decision of the Minister is final.

(4) In any appeal under this section in relation to the conviction of the licensee for a criminal offence, the Minister is to, on appeal from any order of the licensing officer, accept the licensee's conviction as final and conclusive.

(5) Where the licensee concerned has appealed under this section to the Minister against an order by the licensing officer under section 35(1), (2) or (7)(*a*) or (*b*), the order does not take effect unless the order is confirmed by the Minister or the appeal is for any reason dismissed by the Minister or withdrawn.

Unlicensed cybersecurity service provider not to recover fees, etc.

38. Any person who supplies or 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 [licensable] investigative cybersecurity service provider's licence mentioned in section 27 or a valid [licensable] non-investigative cybersecurity service provider's licence mentioned in section 29, as the case may be.

PART 6

GENERAL

Offences by bodies corporate, etc.

39.—(1) Where an offence under this Act committed by a body corporate is proved —

(*a*) to have been committed with the consent or connivance of an officer; or

(*b*) to be attributable to any neglect on the officer's part,

the officer as well as the body corporate shall be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

(2) Where the affairs of a body corporate are managed by its members, subsection (1) applies in relation to the acts and defaults of a member in connection with the member's functions of management as if the member were a director of the body corporate.

(3) Where an offence under this Act committed by a partnership is proved —

(*a*) to have been committed with the consent or connivance of a partner; or

(*b*) to be attributable to any neglect on the partner's part,

the partner as well as the partnership shall be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

(4) Where an offence under this Act committed by an unincorporated association (other than a partnership) is proved —

(*a*) to have been committed with the consent or connivance of an officer of the unincorporated association or a member of its governing body; or

(*b*) to be attributable to any neglect on the part of such an officer or member,

the officer or member as well as the unincorporated association shall be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

(5) In this section —

"body corporate" includes a limited liability partnership;

"officer" —

(*a*) in relation to a body corporate, means any director, partner, member of the committee of management, chief executive, manager, secretary or other similar officer of the body corporate and includes any person purporting to act in any such capacity; or

(*b*) 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, or any person holding a position analogous to that of president, secretary or member of a committee and includes any person purporting to act in any such capacity;

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

(6) Regulations may provide for the application of any provision of this section, with such modifications as the Minister considers appropriate, to any body corporate or unincorporated association formed or recognised under the law of a territory outside Singapore.

Offences by corporations

40.—(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

(ii) an individual who is involved in the management of the corporation and is 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 (1) 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

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

41.—(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 who is involved in the management of the unincorporated association or partnership and who is in a position to influence the conduct of the unincorporated association or partnership (as the case may be) 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 partnership; or

(iii) knew or ought reasonably to have known that the offence by the unincorporated association or 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 the unincorporated association or partnership (as the case may be), 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 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 that the unincorporated association or 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 (1) also does not affect the liability of an unincorporated association or a partnership for an offence under this Act, and applies whether or not the unincorporated association or 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

42.—(1) In addition to the powers conferred on an investigation officer by this Act or any other written law, an investigation officer authorised by the Commissioner may, in relation to any offence under this Act (except any offence under section 24) or any regulations made thereunder, 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 such time and manner as may be 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 or trial 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 only that the person may decline to make with regard to any fact or circumstance a statement which would have a tendency to expose the person to a criminal charge or to 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 thereupon issue a warrant to secure the attendance of that person as required by the order.

(5) An investigation officer may, without payment, take possession of 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 duties by such investigation officer under this Act or that written law;

(*b*) wilfully mis-states or without lawful excuse refuses to give any information or produce any book, document or copy

thereof required of that person by an investigation officer under subsection (1); or

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

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 [6 months] or to both.

(7) In this section and section 43, "investigation officer" means the Commissioner or Deputy Commissioner, or any Assistant Commissioner or cybersecurity officer authorised by the Commissioner, exercising the powers of investigation under this section or section 43.

Power to enter premises under warrant

43.—(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 42 to be furnished, but has not been furnished in compliance with that requirement; or

(*b*) which, if required by an investigation officer under section 42 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 [cybersecurity] 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 referred to 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 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 occupier of the premises of the intended entry into the premises; and

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

(7) If the investigation officer is unable to inform the 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 occupier of the premises or the occupier's legal or other representative.

(9) On leaving the premises after executing the warrant, the investigation officer must, if the premises are unoccupied or the 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

44. 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

45.—(1) The Commissioner or any Assistant Commissioner authorised by the Commissioner may, in his or her discretion, compound any offence under this Act which 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 sums:

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

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

[(1A) 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.]

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

(3) The Minister may make regulations to prescribe the offences which may be compounded.

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

Offence against other laws

46. Nothing in this Act prevents any person from being prosecuted under any other written law for any act or omission which constitutes an offence under that law, or from being liable under that other written law to any punishment or penalty higher or other than that provided by this Act, but no person may be punished twice for the same offence.

Service of documents

47.—(1) Any notice, order or document required or authorised by this Act to be served on any person may be served on the person —

(*a*) by delivering it to the person or to some adult member or employee of the person's family or household at the person's last known place of residence;

(*b*) by leaving it at the person's usual or last known place of residence or place of business in an envelope addressed to the person;

(*c*) by sending it by registered post addressed to the person at the person's usual or last known place of residence or place of business; or

(*d*) in the case of an incorporated company, a partnership or a body of persons —

(i) by delivering it to the secretary or other like officer of the company, partnership or body of persons at its registered office or principal place of business; or

(ii) by sending it by registered post addressed to the company, partnership or body of persons at its registered office or principal place of business.

(2) Any notice, order or document sent by registered post to any person in accordance with subsection (1) is deemed to be duly served on the person at the time when the notice, order or document, as the case may be, would in the ordinary course of post be delivered and, in proving service of the notice, order or document, it is sufficient to prove that the envelope containing the same was properly addressed, stamped and posted by registered post.

(3) Any notice, order or document required or authorised by this Act to be served on the owner or occupier of any premises may be served by delivering it or a true copy thereof to some adult person on the premises or, if there is no such person on the premises to whom it can with reasonable diligence be delivered, by affixing the notice, order or document to some conspicuous part of the premises.

(4) Any notice, order or document required or authorised by this Act to be served on the owner or occupier of any premises is deemed to be properly addressed if addressed by the description of the owner or occupier of the premises without further name or description.

Preservation of secrecy

48.—(1) Subject to subsection (5), every specified person must preserve, and aid in the preserving of, secrecy with regard to —

(*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 (3); and

(*d*) all matters relating to the identity of persons furnishing information to the Commissioner [or an assistant licensing officer appointed under section 30],

that may come to the specified person's knowledge in the performance of his or her functions and discharge of his or her duties under this Act and, must not communicate any such matter to any person, except in so far as such communication —

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

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

(2) Any person who fails to comply with subsection (1) 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.

(3) Any person, when furnishing any information to the Commissioner [or an assistant licensing officer appointed under section 30], may identify information that the person claims to be confidential information.

(4) Every claim made under subsection (3) must be supported by a written statement giving reasons why the information is confidential.

(5) Despite subsection (1), the Commissioner [or an assistant licensing officer] may disclose any information relating to any matter referred to in subsection (1) in any of the following circumstances:

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

(*b*) for the purposes of —

(i) a prosecution under this Act;

(ii) subject to subsection (6), 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 thereof; or

(iv) complying with such provision of an agreement between Singapore and a country or territory outside Singapore (called in this section as a foreign country) as may be prescribed, where the conditions specified in subsection (7) are satisfied.

(6) If the Commissioner [or the assistant licensing officer] is considering whether to disclose any information under subsection (5)(*b*)(ii), the Commissioner [or the assistant licensing officer] must have regard to —

(*a*) the need for excluding, 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 for excluding, 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 [or the assistant licensing officer] is proposing to make the disclosure.

(7) The conditions referred to in subsection (5)(*b*)(iv) 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 given confidential at all times; and

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

(8) 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 19;

(*d*) a cybersecurity technical expert appointed under section 23; or

(*e*) the Minister, or an officer person appointed or employed to assist the Minister.

Protection from personal liability

49.—(1) No liability shall lie against the Commissioner, the Deputy Commissioner, an Assistant Commissioner, a cybersecurity officer, an authorised officer, an assistant licensing officer appointed under section 30, a member of an Appeals Advisory Panel or any other person acting under the direction of the Commissioner for anything which is done or intended to be done in good faith and with reasonable care 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 member of the public by reason of any error or omission of whatever nature

appearing therein or however caused if made in good faith and with reasonable care in the ordinary course of the discharge of the duties of the Commissioner or such person.

Protection of informers

50.—(1) No witness in any proceedings for an offence under this Act is obliged or permitted to disclose the name or address of an informer or the substance of the information received from the informer or to state any matter which might lead to the informer's discovery.

(2) If any document which is in evidence or liable to inspection in any proceedings 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 thereto 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

51.—(1) The Minister may, by an order published 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 terms or 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

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

(2) The Minister may, in any order made under subsection (1), make such 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*.

Power to make regulations

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

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

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

(*b*) the technical or other standards to be maintained by an owner of a critical information infrastructure;

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

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

(*f*) the requirements and manner of cybersecurity audits and cybersecurity risk assessments to be conducted by an owner of a critical information infrastructure;

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

(*h*) in relation to any licence, the class or classes of licence to be issued, and the circumstances in which the licence may be granted;

(*i*) regulating the conduct of licensees in the discharge of their functions;

(*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 whether in whole or in 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 thereof 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 thereof during which the offence continues after conviction.

FIRST SCHEDULE

Section 2(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. Broadband internet access services.

7. National domain name services.

Services relating to water:

8. Water supply services.

9. Services relating to collection and treatment of used water

10. Services relating to management of storm water

Services relating to healthcare:

11. Emergency healthcare services.

12. Hospital care services.

13. Disease surveillance and response.

Services relating to banking and finance:

14. Retail and commercial banking services.

15. Payments clearing and settlement services.

16. Securities trading, clearing, settlement and depository services.

17. Derivatives trading, clearing and settlement services.

18. Monetary management operations (MMO) and intervention operations (IO) services.

19. Services related to mobilisation of official foreign reserves (OFR).
20. Currency issuance.
21. Services related to cash management and payments for the Government.

Services relating to security and emergency services:

22. Civil defence services.
23. Police and security services.
24. Immigration and registration services.

Services relating to aviation:

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

Services relating to land transport:

30. Public transport services, including train and bus services.
31. Monitoring and management of train and public bus network.
32. Monitoring and management of road traffic.

Services relating to maritime:

33. Monitoring and management of shipping traffic.
34. Container terminal operations.
35. General and bulk cargo terminal operations.
36. Cruise and ferry terminal operations.
37. Pilotage, towage and water supply.
38. Bunker supply.
39. Salvage operations.
40. Passenger ferry operations.

Services relating to Government

41. Services relating to functioning of Government

Services relating to media:

42. Services relating to broadcasting of free-to-air television and radio.
43. Services relating to publication of newspapers.
44. Security printing services.

SECOND SCHEDULE

Section 25

LICENSABLE CYBERSECURITY SERVICES

PART 1

LICENSABLE INVESTIGATIVE CYBERSECURITY SERVICES

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

(*a*) penetration testing service.

PART 2

LICENSABLE NON-INVESTIGATIVE CYBERSECURITY SERVICES

2. The following non-investigative cybersecurity services are licensable non-investigative cybersecurity services for the purposes of this Act:

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

PART 3

INTERPRETATION

3. In this Schedule —

"managed security operations centre (SOC) monitoring service" means a service for the monitoring, assessment and defence of an organisation's computer or computer system for the purpose of preventing, detecting and responding to any cybersecurity threats or cybersecurity incidents occurring in the computer or computer system, including preventing unauthorised access to, modification of or copying of any information stored in or processed by the computer or computer system;

"penetration testing service" means a service for assessing, testing or evaluating the cybersecurity of a computer or computer system [and the integrity of any information stored in or processed by the 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 weaknesses of a computer or computer system, and demonstrating how such weaknesses 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 cybersecurity vulnerabilities of a computer or computer system, indicating weaknesses and providing appropriate mitigation procedures required to eliminate weaknesses or to reduce weaknesses 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

EXPENDITURE OF PUBLIC MONEY

This Bill will not involve the Government in any extra financial expenditure.

EXPENDITURE OF PUBLIC MONEY

This Bill will involve the Government in extra financial expenditure, the exact amount of which cannot at present be ascertained.
