Cybersecurity (Amendment) Bill

Bill No. 15/2024.

Read the first time on 3 April 2024.

A BILL

i n t i t u l e d

An Act to amend the Cybersecurity Act 2018.

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

Short title and commencement

1. This Act is the Cybersecurity (Amendment) Act 2024 and comes into operation on a date that the Minister appoints by notification in the *Gazette*.

Amendment of long title

2. In the Cybersecurity Act 2018 (called in this Act the principal Act), in the long title, replace "owners of critical information infrastructure" with "certain persons in relation to the cybersecurity of certain computers or computer systems".

Amendment of section 2

3. In the principal Act, in section 2 —

(*a*) in subsection (1), in the definition of "code of practice", replace "section 11(1)" with "section 35A(1)";

(*b*) in subsection (1), delete the definition of "critical information infrastructure";

(*c*) in subsection (1), after the definition of "Deputy Commissioner", insert —

""designated provider responsible for third-party-owned critical information infrastructure" means a provider of an essential service in respect of whom a designation under section 16A(1), as a provider of an essential service who is responsible for the cybersecurity of a third-party-owned critical information infrastructure, is in effect;

"digital service" means any service normally provided for remuneration, that is delivered by one party to another party at the individual request of the other party, entirely through electronic means, and without needing the parties' simultaneous physical presence, but

does not include such services as the Minister may, by notification in the *Gazette*, prescribe;

"entity of special cybersecurity interest" means an entity in respect of whom a designation under section 18(1) is in effect;";

(*d*) in subsection (1), after the definition of "essential service", insert —

" "foundational digital infrastructure service" means any service which promotes the availability, latency, throughput or security of digital services, and is specified in the Third Schedule;";

(*e*) in subsection (1), after the definition of "licensee", insert —

" "major foundational digital infrastructure" means the computer or computer system (or class of computers or computer systems) that is necessary for a major foundational digital infrastructure service provider's continuous delivery of the foundational digital infrastructure service in relation to which a designation of the major foundational digital infrastructure service provider under section 18G(1) is in effect;

"major foundational digital infrastructure service provider" means a provider of a foundational digital infrastructure service in respect of whom a designation under section 18G(1) is in effect;";

(*f*) in subsection (1), replace the definition of "owner" with —

" "owner", in relation to a provider-owned critical information infrastructure, third-party-owned critical information infrastructure or system of temporary cybersecurity concern —

(*a*) means the legal owner of the provider-owned critical information infrastructure, third-party-owned critical information infrastructure or system of temporary cybersecurity concern (as the case may be); and

(*b*) where the provider-owned critical information infrastructure, third-party-owned critical information infrastructure or system of temporary cybersecurity concern (as the case may be) is jointly owned by more than one person, includes every joint owner;

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

(*g*) in subsection (1), in the definition of "standard of performance", replace "section 11(1)" with "section 35A(1)";

(*h*) in subsection (1), in the definition of "standard of performance", replace the full-stop at the end with a semi-colon;

(*i*) in subsection (1), after the definition of "standard of performance", insert —

" "system of special cybersecurity interest" means the computer or computer system (or class of computers or computer systems) in relation to which a designation of an entity of special cybersecurity interest under section 18(1) is in effect;

"system of temporary cybersecurity concern" means a computer or computer system in

respect of which a designation under section 17(1) is in effect;

"third-party-owned critical information infrastructure" means the computer or computer system in relation to which a designation of a designated provider responsible for third-party-owned critical information infrastructure under section 16A(1) is in effect;

"virtual computer" means a purely digital analogue of a computer, created by the simulation of software and hardware, performing logical, arithmetic or storage functions and including communications functions, but does not include the physical computing resources used for the simulation;

"virtual computer system" means a purely digital analogue of a computer system, created by the simulation of an arrangement of interconnected computers that is designed to perform one or more specific functions, but does not include the physical computing resources used for the simulation."; and

(*j*) after subsection (2), insert —

"(3) For the purposes of this section (except the definitions of "computer", "computer system" and "owner"), sections 3 and 43, Part 2, Part 3 (except section 7(1A)) and Parts 3A, 3B, 3C and 4 —

(*a*) "computer" includes a virtual computer;

(*b*) "computer system" includes a virtual computer system;

(*c*) "control", in relation to a virtual computer or virtual computer system, means —

(i) having the control over the operations of the virtual computer or virtual computer system;

(ii) having the right and ability to perform security configuration and management tasks in respect of the virtual computer or virtual computer system, including to make any modification as necessary for the cybersecurity of the virtual computer or virtual computer system; and

(iii) where applicable, having responsibility for the security of the virtual computer or virtual computer system under a person's contractual arrangement with a cloud computing service provider;

(*d*) "owner", in relation to a provider-owned critical information infrastructure, third-party-owned critical information infrastructure or system of temporary cybersecurity concern that is a virtual computer or virtual computer system —

(i) means the person who has exclusive control of the provider-owned critical information infrastructure, third-party-owned critical information infrastructure or system of temporary cybersecurity concern (as the case may be); and

(ii) where the provider-owned critical information infrastructure, third-party-owned critical information infrastructure or system of temporary cybersecurity concern

(as the case may be) is jointly controlled by more than one person, includes every joint controller;

(*e*) "change in the beneficial or legal ownership (including any share in such ownership)", in relation to a provider-owned critical information infrastructure or third-party-owned critical information infrastructure that is a virtual computer or virtual computer system —

(i) in a case where the virtual computer or virtual computer system is jointly controlled by more than one person — means change in any joint controller; or

(ii) in any other case — means change in the person who has exclusive control of the virtual computer or virtual computer system; and

(*f*) a virtual computer or virtual computer system is wholly or partly in Singapore if one or more of the physical computing resources deployed for the simulation of the virtual computer or virtual computer system (as the case may be) is located in Singapore.".

Amendment of section 3

4. In the principal Act, in section 3 —

(*a*) in subsection (1), replace "section 8" with "sections 7(1A) and 8";

(*b*) after subsection (1), insert —

"(1A) Section 7(1A) applies to any computer or computer system located wholly outside Singapore that is owned by a person in Singapore."; and

(*c*) after subsection (2), insert —

"(2A) Subject to subsection (2B) —

(*a*) Part 3A (except section 16B) applies to any provider of an essential service who is located in Singapore, and is responsible for the cybersecurity of third-party-owned critical information infrastructure; and

(*b*) section 16B applies to any person in Singapore who appears to be a provider of an essential service for which a computer or computer system necessary for the continuous delivery of the essential service is not owned by that person.

(2B) Part 3A does not apply to any provider of an essential service in relation to any computer or computer system which is a provider-owned critical information infrastructure.

(2C) Subject to subsection (2D) —

(*a*) Part 3B (except section 17A) applies to any system of temporary cybersecurity concern located wholly or partly in Singapore; and

(*b*) section 17A applies to any computer or computer system located wholly or partly in Singapore.

(2D) Part 3B does not apply to any computer or computer system which is a provider-owned critical information infrastructure or a third-party-owned critical information infrastructure.

(2E) Subject to subsection (2F) —

(*a*) Part 3C (except section 18A) applies to any entity of special cybersecurity interest incorporated or established under any written law; and

(*b*) section 18A applies to any entity incorporated or established under any written law whom the Commissioner has reason to believe may fulfil the criteria to be designated as an entity of special cybersecurity interest.

(2F) Part 3C does not apply to any entity in relation to any computer or computer system which is a provider-owned critical information infrastructure or a third-party-owned critical information infrastructure.

(2G) Subject to subsection (2H) —

(*a*) Part 3D (except section 18H) applies to any major foundational digital infrastructure service provider that —

(i) provides the foundational digital infrastructure service, whether from within or outside Singapore, to persons in Singapore within the meaning of section 18G; or

(ii) provides the foundational digital infrastructure service wholly or partially from Singapore within the meaning of section 18G; and

(*b*) section 18H applies to any person who appears to be a provider of a foundational digital infrastructure service, whom the Commissioner has reason to believe may fulfil the criteria to be designated as a major foundational digital infrastructure service provider.

(2H) Part 3D does not apply to any provider of a foundational digital infrastructure service in relation to any computer or computer system which is a provider-owned critical information infrastructure or

a third-party-owned critical information infrastructure.”.

Amendment of section 4

5. In the principal Act, in section 4 —

(*a*) replace subsection (2) with —

“(2) The Minister may appoint as an Assistant Commissioner under subsection (1)(*b*) in respect of a provider-owned critical information infrastructure or a system of temporary cybersecurity concern —

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

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

where that other Ministry or statutory body has supervisory or regulatory responsibility over an industry or a sector to which the owner of the provider-owned critical information infrastructure or the system of temporary cybersecurity concern (as the case may be) belongs.

(2A) The Minister may appoint as an Assistant Commissioner under subsection (1)(*b*) in respect of a designated provider responsible for third-party-owned critical information infrastructure, an entity of special cybersecurity interest or a major foundational digital infrastructure service provider —

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

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

where that other Ministry or statutory body has supervisory or regulatory responsibility over an industry or a sector to which the designated provider responsible for third-party-owned critical information infrastructure, entity of special cybersecurity interest or major foundational digital

infrastructure service provider (as the case may be) belongs.";

(*b*) in subsection (5), replace "section 7 or 9" with "section 7, 9, 9A, 16A, 16C, 16D, 17, 17B, 17C, 18, 18B, 18C, 18G, 18I or 18J";

(*c*) in subsection (6)(*a*), replace "9 or 20(5)" with "9, 9A, 16A, 16C, 16D, 17, 17B, 17C, 18, 18B, 18C, 18G, 18I, 18J, 20(5), 37A or 37C"; and

(*d*) in subsection (6)(*b*), replace "section 6, 7, 9, 11, 12 or 20(5)" with "section 6, 6A, 7, 9, 9A, 12, 16A, 16C, 16D, 16G, 17, 17B, 17C, 17E, 18, 18B, 18C, 18E, 18G, 18I, 18J, 18L, 20(5), 35A, 37A or 37C".

Amendment of section 5

6. In the principal Act, in section 5 —

(*a*) renumber the section as subsection (1) of that section;

(*b*) in subsection (1), replace paragraph (*e*) with —

"(*e*) to identify and designate provider-owned critical information infrastructure or systems of temporary cybersecurity concern, and to regulate owners of provider-owned critical information infrastructure or systems of temporary cybersecurity concern with regard to the cybersecurity of the provider-owned critical information infrastructure or systems of temporary cybersecurity concern;

(*ea*) to identify and designate designated providers responsible for third-party-owned critical information infrastructure, entities of special cybersecurity interest or major foundational digital infrastructure service providers, and to regulate those providers

or entities with regard to the cybersecurity of the third-party-owned critical information infrastructure, system of special cybersecurity interest or major foundational digital infrastructure;";

(*c*) in subsection (1)(*f*), replace "critical information infrastructure" with "provider-owned critical information infrastructure or systems of temporary cybersecurity concern, or by designated providers responsible for third-party-owned critical information infrastructure, entities of special cybersecurity interest or major foundational digital infrastructure service providers";

(*d*) in subsection (1)(*k*), after "certification or accreditation schemes", insert "or international certification schemes"; and

(*e*) after subsection (1), insert —

"(2) The office of the Commissioner is to be known as the Cyber Security Agency of Singapore.".

New section 6A

7. In the principal Act, after section 6, insert —

"**Cyber Security Agency of Singapore's symbols, etc.**

6A.—(1) The Commissioner has the exclusive right to the use of one or more symbols or representations of the Cyber Security Agency of Singapore as the Commissioner may select or devise (each called in this section the Cyber Security Agency of Singapore's symbol or representation), and to display or exhibit those symbols or representations in connection with the Cyber Security Agency of Singapore's activities or affairs.

(2) The Commissioner must publish any symbol or representation mentioned in subsection (1) in the *Gazette*.

(3) A person who —

(*a*) uses, without the Commissioner's prior written permission, a symbol or representation that is

identical to the Cyber Security Agency of Singapore's symbol or representation; or

(*b*) uses a symbol or representation that so resembles the Cyber Security Agency of Singapore's symbol or representation as to deceive or cause confusion, or to be likely to deceive or to cause confusion,

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.".

Amendment of section 7

8. In the principal Act, in section 7 —

(*a*) after subsection (1), insert —

"(1A) The Commissioner may, by written notice to the owner of a computer or computer system that is located wholly outside Singapore, designate the computer or computer system as a provider-owned critical information infrastructure for the purposes of this Act, if the Commissioner is satisfied that —

(*a*) the computer or computer system is necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore; and

(*b*) the computer or computer system would have been designated as a provider-owned critical information infrastructure under subsection (1) had it been located wholly or partly in Singapore.";

(*b*) in subsections (2), (3), (4) and (5), after "subsection (1)", insert "or (1A)"; and

(*c*) in subsection (2)(*d*), after "critical information infrastructure", insert "in relation to its cybersecurity".

New section 9A

9. In the principal Act, after section 9, insert —

"**Extension of designation of provider-owned critical information infrastructure**

9A.—(1) At any time before the expiry of the designation of a provider-owned critical information infrastructure, the Commissioner may, by written notice, extend the designation of the provider-owned critical information infrastructure, if the Commissioner is of the opinion that the computer or computer system continues to fulfil the criteria to be designated as a provider-owned critical information infrastructure.

(2) Any extension of a designation under subsection (1) has effect for a period of 5 years starting from the expiry of the earlier designation, unless the designation is withdrawn by the Commissioner before the extension takes effect or before the expiry of the period of extension.".

Deletion of section 11

10. In the principal Act, delete section 11.

Amendment of section 12

11. In the principal Act, in section 12 —

(*a*) in subsection (2), after paragraph (*a*), insert —

"(*aa*) compliance with any prescribed technical or other standards relating to cybersecurity in respect of the provider-owned critical information infrastructure;"; and

(*b*) replace subsection (3) with —

"(3) A direction under subsection (1) must specify a deadline for compliance, and may be revoked at any time by the Commissioner.".

Amendment of section 14

12. In the principal Act, in section 14(1), after paragraph (*b*), insert —

"(*ba*) a prescribed cybersecurity incident in respect of any other computer or computer system under the owner's control that does not fall within paragraph (*b*);

(*bb*) a prescribed cybersecurity incident in respect of any computer or computer system under the control of a supplier to the owner that is interconnected with or that communicates with the provider-owned critical information infrastructure;".

Amendment of section 15

13. In the principal Act, in section 15 —

(*a*) in subsection (1)(*a*), after "with this Act", insert ", any prescribed technical or other standards relating to cybersecurity that are to be maintained in respect of the provider-owned critical information infrastructure,"; and

(*b*) replace subsection (4) with —

"(4) Where it appears to the Commissioner that —

(*a*) the owner of a provider-owned critical information infrastructure has not complied with a provision of this Act, a prescribed technical or other standard relating to cybersecurity, or an applicable code of practice or standard of performance; or

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

the Commissioner may for the purpose of ascertaining the owner's compliance with this Act, a prescribed technical or other standard relating to

cybersecurity, or an applicable code of practice or standard of performance, or ascertaining the accuracy or completeness of the information (as the case may be) —

(*c*) by order require an audit in respect of the provider-owned critical information infrastructure to be carried out by an auditor appointed by the Commissioner, and the cost of such audit must be borne by the owner; or

(*d*) authorise the Deputy Commissioner, an Assistant Commissioner, a cybersecurity officer or an authorised officer to carry out an inspection of the provider-owned critical information infrastructure.".

Deletion of sections 17 and 18 and insertion of new Part 3A

14. In the principal Act, replace sections 17 and 18 with —

"PART 3A

PROVIDERS OF ESSENTIAL SERVICE RESPONSIBLE FOR CYBERSECURITY OF THIRD-PARTY-OWNED CRITICAL INFORMATION INFRASTRUCTURE

Designation of provider of essential service responsible for cybersecurity of third-party-owned critical information infrastructure

16A.—(1) The Commissioner may, by written notice to a provider of an essential service, designate the provider as a provider of an essential service responsible for the cybersecurity of third-party-owned critical information infrastructure for the purposes of this Act, if the Commissioner is satisfied that —

(*a*) a computer or computer system (called a third-party-owned critical information infrastructure) (whether located in or outside Singapore) is necessary for the continuous delivery of the essential service provided by that provider, and

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

(*b*) the computer or computer system is not owned by the provider of the essential service.

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

(*a*) identify the third-party-owned critical information infrastructure in relation to which the provider is designated as a designated provider responsible for third-party-owned critical information infrastructure;

(*b*) identify the provider of the essential service so designated as a designated provider responsible for third-party-owned critical information infrastructure;

(*c*) identify the person who appears to be the owner of the third-party-owned critical information infrastructure;

(*d*) inform the designated provider responsible for third-party-owned critical information infrastructure regarding the provider's duties and responsibilities under this Act that arise from the designation;

(*e*) provide the name and contact particulars of the officer assigned by the Commissioner to supervise the designated provider responsible for third-party-owned critical information infrastructure in relation to the cybersecurity of the third-party-owned critical information infrastructure;

(*f*) inform the designated provider responsible for third-party-owned critical information infrastructure that any representations against the designation are to be made to the Commissioner by a specified date, being a date not earlier than 14 days after the date of the notice; and

(*g*) inform the designated provider responsible for third-party-owned critical information infrastructure that the provider may appeal to the Minister against

the designation, and provide information on the applicable procedure.

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

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

Power to obtain information to ascertain if criteria for designated provider responsible for cybersecurity of third-party-owned critical information infrastructure fulfilled

16B.—(1) This section applies where the Commissioner has reason to believe that a computer or computer system may fulfil the criteria in section 16A(1).

(2) The Commissioner may, by notice given in the prescribed form and manner, require any person who appears to be a provider of an essential service for which a computer or computer system necessary for the continuous delivery of the essential service is not owned by the person, to provide to the Commissioner, within a reasonable period specified in the notice, such relevant information relating to that computer or computer system that is within that person's knowledge or which the person can reasonably obtain, as may be required by the Commissioner for the purpose of ascertaining whether the computer or computer system fulfils the criteria in section 16A(1).

(3) Without limiting subsection (2), the Commissioner may in the notice require the person to provide —

(*a*) information relating to —

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

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

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

(*c*) any other information that the Commissioner may require in order to ascertain whether the computer or computer system fulfils the criteria in section 16A(1).

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

(5) Where a person fails to comply with a notice under subsection (2), and the computer or computer system in relation to which the notice was issued appears to be necessary for the delivery of an essential service provided by the person, the Commissioner may order the person to cease using, directly or indirectly, the computer or computer system in relation to which the notice was issued.

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

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

Withdrawal of designation of designated provider responsible for third-party-owned critical information infrastructure

16C. The Commissioner may, by written notice, withdraw the designation of any designated provider responsible for third-party-owned critical information infrastructure at any time if the Commissioner is of the opinion that the criteria in section 16A(1) are no longer fulfilled.

Extension of designation of designated provider responsible for third-party-owned critical information infrastructure

16D.—(1) At any time before the expiry of the designation of a designated provider responsible for third-party-owned critical information infrastructure, the Commissioner may, by written notice, extend the designation of the designated provider responsible for third-party-owned critical information infrastructure, if the Commissioner is of the opinion that the criteria in section 16A(1) continue to be fulfilled.

(2) Any extension of a designation under subsection (1) has effect for a period of 5 years starting from the expiry of the earlier designation, unless the designation is withdrawn by the Commissioner before the extension takes effect or before the expiry of the period of extension.

Furnishing of information relating to third-party-owned critical information infrastructure

16E.—(1) A designated provider responsible for third-party-owned critical information infrastructure must obtain a legally binding commitment from the owner of the third-party-owned critical information infrastructure for which the provider is responsible for its cybersecurity, that the owner of the third-party-owned critical information infrastructure will —

(*a*) upon the request of the designated provider responsible for third-party-owned critical information infrastructure pursuant to a notice

issued by the Commissioner under subsection (4), furnish the provider the following within a reasonable period:

(i) information on the design, configuration and security of the third-party-owned critical information infrastructure;

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

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

(iv) any other information that the Commissioner may require in order to ascertain the level of cybersecurity of the third-party-owned critical information infrastructure; and

(*b*) notify the designated provider responsible for third-party-owned critical information infrastructure when a material change is made by or on behalf of the owner of the third-party-owned critical information infrastructure to the design, configuration, security or operation of the third-party-owned critical information infrastructure after any information has been furnished to the provider pursuant to a request mentioned in paragraph (*a*), not later than 30 days after the change is made, so that the provider may notify the Commissioner in accordance with subsection (8).

(2) Where subsection (1) is not complied with, the Commissioner may order the designated provider responsible for third-party-owned critical information infrastructure to cease using, directly or indirectly, the third-party-owned critical information infrastructure for which the provider is responsible for its cybersecurity.

(3) Any designated provider responsible for third-party-owned critical information infrastructure who, without reasonable excuse, fails to comply with an order issued under subsection (2) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part of a day during which the offence continues after conviction.

(4) The Commissioner may by notice given in the prescribed form and manner, require the designated provider responsible for third-party-owned 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 third-party-owned critical information infrastructure;

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

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

(*d*) any other information relating to the third-party-owned critical information infrastructure

that the Commissioner may require in order to ascertain the level of cybersecurity of the third-party-owned critical information infrastructure.

(5) Any designated provider responsible for third-party-owned critical information infrastructure who, without reasonable excuse, fails to comply with a notice mentioned in subsection (4) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part of a day during which the offence continues after conviction.

(6) The designated provider responsible for third-party-owned critical information infrastructure to whom a notice is issued under subsection (4) is not obliged to disclose any information that is subject to any right, privilege or immunity conferred, or obligation or limitation imposed, by or under any law or rules of professional conduct in relation to the disclosure of such information, except that the performance of a contractual obligation is not an excuse for not disclosing the information.

(7) The designated provider responsible for third-party-owned critical information infrastructure is not treated as being in breach of any contractual obligation mentioned in subsection (6) for doing or omitting to do any act, if the act is done or omitted to be done with reasonable care and in good faith and for the purpose of complying with a notice issued under subsection (4).

(8) If a material change is made by or on behalf of the owner of the third-party-owned critical information infrastructure to the design, configuration, security or operation of the third-party-owned critical information infrastructure after any information has been furnished to the Commissioner pursuant to a notice mentioned in subsection (4), the designated provider responsible for third-party-owned critical information infrastructure must notify the Commissioner of the change not later than 14 days after the provider becomes aware of it.

(9) For the purposes of subsections (1)(*b*) and (8), a change is a material change if the change affects or may affect the cybersecurity of the third-party-owned critical information infrastructure, or the ability of the owner of the third-party-owned critical information infrastructure or the designated provider responsible for third-party-owned critical information infrastructure, to respond to a cybersecurity threat or incident affecting the third-party-owned critical information infrastructure.

(10) Any designated provider responsible for third-party-owned critical information infrastructure who, without reasonable excuse, fails to comply with subsection (8) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $25,000 or to imprisonment for a term not exceeding 12 months or to both.

Provider to ensure third-party-owned critical information infrastructure conforms with prescribed standards

16F.—(1) A designated provider responsible for third-party-owned critical information infrastructure must obtain a legally binding commitment from the owner of the third-party-owned critical information infrastructure, that the owner will ensure that any applicable prescribed technical or other standards relating to cybersecurity are maintained in respect of that third-party-owned critical information infrastructure.

(2) Where subsection (1) is not complied with, the Commissioner may order the designated provider responsible for third-party-owned critical information infrastructure to cease using, directly or indirectly, the third-party-owned critical information infrastructure for which the provider is responsible for its cybersecurity.

(3) Where it appears to the Commissioner that —

(*a*) the standards mentioned in subsection (1) are not maintained in respect of the third-party-owned critical information infrastructure despite the issuance of

directions mentioned in section 16G(2)(*c*) and any steps taken by the designated provider responsible for third-party-owned critical information infrastructure; and

(*b*) there is no reasonable excuse for such failure to maintain the standards,

the Commissioner may order the designated provider responsible for third-party-owned critical information infrastructure to cease using, directly or indirectly, the third-party-owned critical information infrastructure for which the provider is responsible for its cybersecurity.

(4) Any designated provider responsible for third-party-owned critical information infrastructure who, without reasonable excuse, fails to comply with an order issued under subsection (2) or (3) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part of a day during which the offence continues after conviction.

Power of Commissioner to issue written directions

16G.—(1) The Commissioner may, if the Commissioner thinks —

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

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

issue a written direction, either of a general or specific nature, to a designated provider responsible for third-party-owned critical information infrastructure or a class of such providers.

(2) Without limiting subsection (1), a direction under that subsection may relate to —

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

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

(*c*) steps to be taken by the designated provider responsible for third-party-owned critical information infrastructure to require the owner of the third-party-owned critical information infrastructure to ensure that any prescribed technical or other standards relating to cybersecurity in respect of the third-party-owned critical information infrastructure are maintained;

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

(*e*) any other matter that the Commissioner may consider necessary or expedient to ensure the cybersecurity of the third-party-owned critical information infrastructure.

(3) A direction under subsection (1) must specify a deadline for compliance, and may be revoked at any time by the Commissioner.

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

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

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

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

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

Change in ownership of third-party-owned critical information infrastructure

16H.—(1) A designated provider responsible for third-party-owned critical information infrastructure must obtain a legally binding commitment from the owner of the third-party-owned critical information infrastructure for which the provider is responsible for its cybersecurity, that the owner will notify the provider of any change in the beneficial or legal ownership (including any share in such ownership) of the third-party-owned critical information infrastructure, not later than 7 days after the date of that change in ownership.

(2) Where subsection (1) is not complied with, the Commissioner may order the designated provider responsible for third-party-owned critical information infrastructure to cease using, directly or indirectly, the third-party-owned critical information infrastructure for which the provider is responsible for its cybersecurity.

(3) Any designated provider responsible for third-party-owned critical information infrastructure who, without reasonable excuse, fails to comply with an order issued under subsection (2) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a continuing offence, to a further fine not

exceeding $5,000 for every day or part of a day during which the offence continues after conviction.

(4) Where there is any change in the beneficial or legal ownership (including any share in such ownership) of a third-party-owned critical information infrastructure, the designated provider responsible for third-party-owned critical information infrastructure must inform the Commissioner of the change in ownership not later than 7 days after the provider becomes aware of that change in ownership.

(5) Where the criteria in section 16A(1) are no longer fulfilled, the designated provider responsible for third-party-owned critical information infrastructure must inform the Commissioner of the change in circumstances not later than 7 days after the date of the change in circumstances.

(6) Any person who, without reasonable excuse, fails to comply with subsection (4) or (5) 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 third-party-owned critical information infrastructure, etc.

16I.—(1) A designated provider responsible for third-party-owned critical information infrastructure must obtain a legally binding commitment from the owner of the third-party-owned critical information infrastructure for which the provider is responsible for its cybersecurity, that the owner of the third-party-owned critical information infrastructure will notify the provider of the occurrence of any of the following within the prescribed period after becoming aware of such occurrence:

(*a*) a prescribed cybersecurity incident in respect of the third-party-owned critical information infrastructure;

(*b*) a prescribed cybersecurity incident in respect of any computer or computer system under the owner's

control that is interconnected with or that communicates with the third-party-owned critical information infrastructure;

(*c*) any other type of cybersecurity incident in respect of the third-party-owned critical information infrastructure that the Commissioner has specified by written direction to the designated provider responsible for third-party-owned critical information infrastructure.

(2) Where subsection (1) is not complied with, the Commissioner may order the designated provider responsible for third-party-owned critical information infrastructure to cease using, directly or indirectly, the third-party-owned critical information infrastructure for which the provider is responsible for its cybersecurity.

(3) Any designated provider responsible for third-party-owned critical information infrastructure who, without reasonable excuse, fails to comply with an order issued under subsection (2) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part of a day during which the offence continues after conviction.

(4) The designated provider responsible for third-party-owned critical information infrastructure must notify the Commissioner of the occurrence of any of the following in the prescribed form and manner, within the prescribed period after becoming aware of such occurrence:

(*a*) a prescribed cybersecurity incident in respect of the third-party-owned critical information infrastructure;

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

(*c*) a prescribed cybersecurity incident in respect of any other computer or computer system under the provider's control that does not fall within paragraph (*b*);

(*d*) any other type of cybersecurity incident in respect of the third-party-owned critical information infrastructure that the Commissioner has specified by written direction to the designated provider responsible for third-party-owned critical information infrastructure.

(5) The designated provider responsible for third-party-owned critical information infrastructure must establish such mechanisms and processes for the purposes of becoming aware of any cybersecurity threats and incidents in respect of the third-party-owned critical information infrastructure, as set out in any applicable code of practice.

(6) Any designated provider responsible for third-party-owned critical information infrastructure who, without reasonable excuse, fails to comply with subsection (4) 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 third-party-owned critical information infrastructure

16J.—(1) A designated provider responsible for third-party-owned critical information infrastructure must obtain a legally binding commitment from the owner of the third-party-owned critical information infrastructure for which the provider is responsible for its cybersecurity, that the owner of the third-party-owned critical information infrastructure will —

(*a*) at least once every 2 years (or at such higher frequency as the Commissioner may require in any particular case by written notice to the provider), starting from the date of the notice issued under section 16A(1), cause an audit of the adherence of the

third-party-owned critical information infrastructure to any prescribed technical or other standards relating to cybersecurity that are to be maintained in respect of the third-party-owned critical information infrastructure, to be carried out by an auditor approved by the Commissioner;

(*b*) at least once a year, starting from the date of the notice issued under section 16A(1), conduct a cybersecurity risk assessment of the third-party-owned critical information infrastructure in the prescribed form or manner;

(*c*) furnish a copy of the report of any audit mentioned in paragraph (*a*), and the report of any cybersecurity risk assessment mentioned in paragraph (*b*), to the provider, not later than 30 days after the completion of the audit or assessment (as the case may be);

(*d*) carry out again any aspect of an audit mentioned in paragraph (*a*) as required by the provider pursuant to a direction from the Commissioner under subsection (6);

(*e*) cause an audit in respect of the third-party-owned critical information infrastructure to be carried out by an auditor approved by the Commissioner, as required by the provider pursuant to a direction from the Commissioner under subsection (7);

(*f*) carry out further steps to evaluate the level of cybersecurity of the third-party-owned critical information infrastructure, or cause another cybersecurity risk assessment of the third-party-owned critical information infrastructure to be conducted by a cybersecurity service professional approved by the Commissioner, as required by the provider pursuant to a direction from the Commissioner under subsection (8); and

(*g*) carry out another audit or cybersecurity risk assessment in addition to the audit or cybersecurity

risk assessment mentioned in paragraphs (*a*) and (*b*), as required by the provider pursuant to a direction from the Commissioner under subsection (9).

(2) Where subsection (1) is not complied with, the Commissioner may order the designated provider responsible for third-party-owned critical information infrastructure to cease using, directly or indirectly, the third-party-owned critical information infrastructure for which the provider is responsible for its cybersecurity.

(3) Any designated provider responsible for third-party-owned critical information infrastructure who, without reasonable excuse, fails to comply with an order issued under subsection (2) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part of a day during which the offence continues after conviction.

(4) The designated provider responsible for third-party-owned critical information infrastructure must obtain from the owner each report of an audit and each report of a cybersecurity risk assessment mentioned in subsection (1)(*c*).

(5) The designated provider responsible for third-party-owned critical information infrastructure must, not later than 14 days after receiving from the owner a report of an audit or a cybersecurity risk assessment, furnish a copy of the report of the audit or assessment to the Commissioner.

(6) Where it appears to the Commissioner from the report of an audit furnished under subsection (5), that any aspect of the audit was not carried out satisfactorily, the Commissioner may direct the designated provider responsible for third-party-owned critical information infrastructure to require the owner of the third-party-owned critical information infrastructure to carry out that aspect of the audit again.

(7) Where it appears to the Commissioner that —

(*a*) the third-party-owned critical information infrastructure is not in conformity with any prescribed technical or other standard relating to cybersecurity that is to be maintained in respect of the third-party-owned critical information infrastructure; or

(*b*) any information furnished by the designated provider responsible for third-party-owned critical information infrastructure under section 16E is false, misleading, inaccurate or incomplete,

the Commissioner may for the purpose of ascertaining the third-party-owned critical information infrastructure's conformity with the applicable prescribed technical or other standard relating to cybersecurity, or ascertaining the accuracy or completeness of the information (as the case may be), direct the provider to require the owner of the third-party-owned critical information infrastructure to cause an audit in respect of the third-party-owned critical information infrastructure to be carried out by an auditor approved by the Commissioner.

(8) Where it appears to the Commissioner, from the report of a cybersecurity risk assessment furnished under subsection (5), that the assessment was not carried out satisfactorily, the Commissioner may direct the designated provider responsible for third-party-owned critical information infrastructure to require the owner of the third-party-owned critical information infrastructure to either —

(*a*) carry out further steps to evaluate the level of cybersecurity of the third-party-owned critical information infrastructure; or

(*b*) cause another cybersecurity risk assessment of the third-party-owned critical information infrastructure to be conducted by a cybersecurity service professional approved by the Commissioner.

(9) Where the designated provider responsible for third-party-owned critical information infrastructure has notified the Commissioner under section 16E(8) of a material change made to the design, configuration, security or operation of the third-party-owned critical information infrastructure, or the Commissioner otherwise becomes aware of such material change having been made, the Commissioner may by written notice direct the provider to require the owner of the third-party-owned critical information infrastructure to carry out another audit or cybersecurity risk assessment in addition to the audit or cybersecurity risk assessment mentioned in subsection (1)(*a*) or (*b*).

(10) Any designated provider responsible for third-party-owned critical information infrastructure who —

(*a*) without reasonable excuse, fails to comply with subsection (4);

(*b*) without reasonable excuse, fails to comply with the Commissioner's direction under subsection (6), (7), (8)(*a*) or (*b*) or (9); or

(*c*) obstructs or prevents an audit mentioned in subsection (7) or a cybersecurity risk assessment mentioned in subsection (8)(*b*) from being carried out, or impedes the effectiveness of such an audit or cybersecurity risk assessment carried out,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part of a day during which the offence continues after conviction.

(11) Any designated provider responsible for third-party-owned critical information infrastructure who, without reasonable excuse, fails to comply with subsection (5) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $25,000 or to imprisonment for a term not exceeding 12 months or to both and, in the case of a continuing

offence, to a further fine not exceeding $2,500 for every day or part of a day during which the offence continues after conviction.

Duty to notify material change to legally binding commitment

16K.—(1) If a material change is made to a legally binding commitment that was obtained by a designated provider responsible for third-party-owned critical information infrastructure for the purpose of meeting a requirement under section 16E(1), 16F(1), 16H(1), 16I(1) or 16J(1), the designated provider responsible for third-party-owned critical information infrastructure must notify the Commissioner of the change not later than 14 days after the change is made.

(2) For the purposes of subsection (1), a change is a material change if the change affects the ability of the designated provider responsible for third-party-owned critical information infrastructure to obtain the performance, by the owner of the third-party-owned critical information infrastructure, of the actions committed in accordance with the legally binding commitment.

(3) Any designated provider responsible for third-party-owned critical information infrastructure who, without reasonable excuse, fails to comply with subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $25,000 or to imprisonment for a term not exceeding 12 months or to both.

Cybersecurity exercises

16L.—(1) The Commissioner may conduct cybersecurity exercises for the purpose of testing the state of readiness of different designated providers responsible for third-party-owned critical information infrastructure in responding to significant cybersecurity incidents.

(2) A designated provider responsible for third-party-owned critical information infrastructure must participate in a

cybersecurity exercise if directed in writing to do so by the Commissioner.

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

New Part 3B

15. In the principal Act, after Part 3A (as inserted by section 14), insert —

"PART 3B

SYSTEMS OF TEMPORARY CYBERSECURITY CONCERN

Designation of system of temporary cybersecurity concern

17.—(1) The Commissioner may, by written notice to the owner of a computer or computer system, designate the computer or computer system as a system of temporary cybersecurity concern for the purposes of this Act, if the Commissioner is satisfied that —

(*a*) for a limited period —

(i) there is a high risk that a cybersecurity threat or cybersecurity incident may be carried out that will jeopardise or adversely affect, without lawful authority, the cybersecurity of the computer or computer system; and

(ii) the loss or compromise of the computer or computer system will have a serious detrimental effect on the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore; and

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

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

(*a*) identify the computer or computer system that is being designated as a system of temporary cybersecurity concern;

(*b*) identify the owner of the computer or computer system so designated as a system of temporary cybersecurity concern;

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

(*d*) specify the first and last day of the period of designation, which must not exceed one year;

(*e*) provide the name and contact particulars of the officer assigned by the Commissioner to supervise the system of temporary cybersecurity concern in relation to its cybersecurity;

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

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

(3) Any designation under subsection (1) has effect until the end of the period of designation specified in the notice, unless it is withdrawn by the Commissioner before the expiry of the period.

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

(*a*) the person is not able to comply with the requirements in this Part for the reason that the person has neither effective control over the operations of the computer or computer system, nor the ability or right to carry out changes to the computer or computer system; and

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

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

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

(7) Where —

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

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

the owner of the system of temporary cybersecurity concern must notify the Commissioner of this without delay.

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

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

Power to obtain information to ascertain if criteria for system of temporary cybersecurity concern fulfilled

17A.—(1) This section applies where the Commissioner has reason to believe that a computer or computer system may fulfil the criteria to be designated as a system of temporary cybersecurity concern.

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

(3) Without limiting subsection (2), for the purpose of ascertaining whether the computer or computer system fulfils the criteria to be designated as a system of temporary cybersecurity concern, the Commissioner may in the notice require the person who appears to be exercising control over the computer or computer system to provide —

(*a*) information relating to —

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

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

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

(*c*) any other information that the Commissioner may require in order to ascertain whether the computer or

computer system fulfils the criteria to be designated as a system of temporary cybersecurity concern.

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

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

Withdrawal of designation of system of temporary cybersecurity concern

17B. The Commissioner may, by written notice, withdraw the designation of a system of temporary cybersecurity concern at any time if the Commissioner is of the opinion that the computer or computer system no longer fulfils the criteria to be designated as a system of temporary cybersecurity concern.

Extension of designation of system of temporary cybersecurity concern

17C.—(1) At any time before the expiry of the designation of a system of temporary cybersecurity concern, the Commissioner may, by written notice, extend the designation of the system of temporary cybersecurity concern, if the Commissioner is of the opinion that the computer or computer system continues to fulfil the criteria to be designated as a system of temporary cybersecurity concern.

(2) Any extension of a designation under subsection (1) has effect for the period stated in the notice in subsection (1) (which must not exceed one year for each extension), starting from the

expiry of the earlier designation, unless the designation is withdrawn by the Commissioner before the extension takes effect or before the expiry of the period of extension.

Furnishing of information relating to system of temporary cybersecurity concern

17D.—(1) The Commissioner may by notice given in the prescribed form and manner, require the owner of a system of temporary cybersecurity concern to furnish, within a reasonable period specified in the notice, the following:

(*a*) information on the design, configuration and security of the system of temporary cybersecurity concern;

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

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

(*d*) any other information that the Commissioner may require in order to ascertain the level of cybersecurity of the system of temporary cybersecurity concern.

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

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

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

Power of Commissioner to issue written directions

17E.—(1) The Commissioner may, if the Commissioner thinks —

(*a*) it is necessary or expedient for ensuring the cybersecurity of a system of temporary cybersecurity concern or a class of systems of temporary cybersecurity concern; or

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

issue a written direction, either of a general or specific nature, to the owner of a system of temporary cybersecurity concern or a class of such owners.

(2) Without limiting subsection (1), a direction under that subsection may relate to —

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

(*b*) compliance with any prescribed technical or other standards relating to cybersecurity in respect of the system of temporary cybersecurity concern;

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

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

(*e*) any other matter that the Commissioner may consider necessary or expedient to ensure the cybersecurity of the system of temporary cybersecurity concern.

(3) A direction under subsection (1) must specify a deadline for compliance, and may be revoked at any time by the Commissioner.

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

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

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

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

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

Duty to report cybersecurity incident in respect of system of temporary cybersecurity concern, etc.

17F.—(1) The owner of a system of temporary cybersecurity concern must notify the Commissioner of the occurrence of any of the following in the prescribed form and manner, within the prescribed period after becoming aware of such occurrence:

(*a*) a prescribed cybersecurity incident in respect of the system of temporary cybersecurity concern;

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

(*c*) a prescribed cybersecurity incident in respect of any computer or computer system under the control of a supplier to the owner that is interconnected with or that communicates with the system of temporary cybersecurity concern.

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

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

New Part 3C

16. In the principal Act, before Part 4, insert —

"PART 3C

ENTITIES OF SPECIAL CYBERSECURITY INTEREST

Designation of entity of special cybersecurity interest

18.—(1) The Commissioner may, by written notice to an entity, designate the entity as an entity of special cybersecurity interest for the purposes of this Act, if the Commissioner is satisfied that —

(*a*) the entity —

(i) stores sensitive information in a computer or computer system (or class of computers or computer systems) under the entity's control; or

(ii) uses a computer or computer system (or class of computers or computer systems) under the entity's control to perform a function which, if disrupted, will have a significant detrimental effect on the defence, foreign relations, economy, public health, public safety or public order of Singapore; and

(*b*) the entity is incorporated or established under any written law.

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

(*a*) identify the entity that is being designated as an entity of special cybersecurity interest;

(*b*) describe the computer or computer system (or class of computers or computer systems) in relation to which the entity of special cybersecurity interest is being designated;

(*c*) inform the entity of special cybersecurity interest regarding the entity's duties and responsibilities under this Act that arise from the designation;

(*d*) provide the name and contact particulars of the officer assigned by the Commissioner to supervise the entity of special cybersecurity interest in relation to the

cybersecurity of the entity's computers or computer systems;

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

(*f*) inform the entity of special cybersecurity interest that the entity may appeal to the Minister against the designation, and provide information on the applicable procedure.

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

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

(5) In this section and section 18A, "sensitive information" means information the disclosure of which will have a significant detrimental effect on the defence, foreign relations, economy, public health, public safety or public order of Singapore.

Power to obtain information to ascertain if criteria for entity of special cybersecurity interest fulfilled

18A.—(1) This section applies where the Commissioner has reason to believe that an entity may fulfil the criteria to be designated as an entity of special cybersecurity interest.

(2) The Commissioner may, by notice given in the prescribed form and manner, require any entity to provide to the Commissioner, within a reasonable period specified in the notice, such relevant information relating to that entity as may be required by the Commissioner for the purpose of ascertaining whether the entity fulfils the criteria to be designated as an entity of special cybersecurity interest.

(3) Without limiting subsection (2), for the purpose of ascertaining whether an entity fulfils the criteria to be designated as an entity of special cybersecurity interest, the Commissioner may in the notice require the entity to provide —

(*a*) information relating to —

(i) the extent to which the entity stores sensitive information in any computer or computer system (or class of computers or computer systems); and

(ii) the extent to which the entity uses any computer or computer system (or class of computers or computer systems) to perform a function which, if disrupted, will have a significant detrimental effect on the defence, foreign relations, economy, public health, public safety or public order of Singapore;

(*b*) information relating to the design of any computer or computer system (or class of computers or computer systems) which the entity uses to store sensitive information or to perform a function which, if disrupted, will have a significant detrimental effect on the defence, foreign relations, economy, public health, public safety or public order of Singapore; and

(*c*) any other information that the Commissioner may require in order to ascertain whether the entity fulfils the criteria to be designated as an entity of special cybersecurity interest.

(4) Any person who, without reasonable excuse, fails to comply with a notice issued under subsection (2) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding the greater of $200,000 or 10 percent of the annual turnover of the person's business in Singapore and, in the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part of a day during which the offence continues after conviction.

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

Withdrawal of designation of entity of special cybersecurity interest

18B. The Commissioner may, by written notice, withdraw the designation of an entity of special cybersecurity interest at any time if the Commissioner is of the opinion that the entity no longer fulfils the criteria to be designated as an entity of special cybersecurity interest.

Extension of designation of entity of special cybersecurity interest

18C.—(1) At any time before the expiry of the designation of an entity of special cybersecurity interest, the Commissioner may, by written notice, extend the designation of the entity of special cybersecurity interest, if the Commissioner is of the opinion that the entity continues to fulfil the criteria to be designated as an entity of special cybersecurity interest.

(2) Any extension of a designation under subsection (1) has effect for a period of 5 years starting from the expiry of the earlier designation, unless the designation is withdrawn by the Commissioner before the extension takes effect or before the expiry of the period of extension.

Furnishing of information relating to system of special cybersecurity interest

18D.—(1) The Commissioner may by notice given in the prescribed form and manner, require the entity of special cybersecurity interest to furnish, within a reasonable period specified in the notice, the following:

(*a*) information on the design, configuration and security of the system of special cybersecurity interest;

(*b*) any other information that the Commissioner may require in order to ascertain the level of cybersecurity of the system of special cybersecurity interest.

(2) Any entity of special cybersecurity interest who, without reasonable excuse, fails 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 the greater of $200,000 or 10 percent of the annual turnover of the person's business in Singapore and, in the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part of a day during which the offence continues after conviction.

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

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

Power of Commissioner to issue written directions

18E.—(1) The Commissioner may, if the Commissioner thinks —

(*a*) it is necessary or expedient for ensuring the cybersecurity of a system of special cybersecurity interest; or

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

issue a written direction, either of a general or specific nature, to the entity of special cybersecurity interest or a class of such entities.

(2) Without limiting subsection (1), a direction under that subsection may relate to —

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

(*b*) compliance with any prescribed technical or other standards relating to cybersecurity in respect of the system of special cybersecurity interest;

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

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

(*e*) any other matter that the Commissioner may consider necessary or expedient to ensure the cybersecurity of the system of special cybersecurity interest.

(3) A direction under subsection (1) must specify a deadline for compliance, and may be revoked at any time by the Commissioner.

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

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

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

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

(6) Any person who, without reasonable excuse, fails to comply with a direction under subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding the greater of $200,000 or 10 percent of the annual turnover of the person's business in Singapore and, in the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part of a day during which the offence continues after conviction.

Duty to report cybersecurity incident affecting entity of special cybersecurity interest

18F.—(1) The entity of special cybersecurity interest must notify the Commissioner, in the prescribed form and manner, within the prescribed period after becoming aware of the occurrence of a prescribed cybersecurity incident in respect of the system of special cybersecurity interest or any other computer or computer system under the entity's control, where the incident —

(*a*) results in a breach in the availability, confidentiality or integrity of the entity's data; or

(*b*) has a significant impact on the business operations of the entity.

(2) The entity of special cybersecurity interest must establish such mechanisms and processes for the purposes of detecting cybersecurity threats and incidents in respect of the system of special cybersecurity interest, as set out in any applicable code of practice.

(3) Any entity of special cybersecurity interest who, without reasonable excuse, fails to comply with subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding the greater of $200,000 or 10 percent of the annual turnover of the person's business in Singapore.".

New Part 3D

17. In the principal Act, after Part 3C (as inserted by section 16), insert —

"PART 3D

MAJOR FOUNDATIONAL
DIGITAL INFRASTRUCTURE SERVICE PROVIDERS

Designation of major foundational digital infrastructure service provider

18G.—(1) The Commissioner may, by written notice to a provider of a foundational digital infrastructure service, designate the provider as a major foundational digital infrastructure service provider for the purposes of this Act, if the Commissioner is satisfied that —

(*a*) a computer or computer system (or class of computers or computer systems) is necessary for the continuous delivery of a foundational digital infrastructure service by the provider of the foundational digital infrastructure service; and

(*b*) the provider provides the foundational digital infrastructure service —

(i) whether from within or outside Singapore, to persons in Singapore, and the loss or impairment of the provision of that foundational digital infrastructure service is likely to lead to or cause disruption or deterioration of the operation of a large number of businesses or organisations in Singapore which rely on or are enabled by that foundational digital infrastructure service; or

(ii) wholly or partially from Singapore, and the loss or impairment of the provision of that foundational digital infrastructure service is likely to lead to or cause disruption or deterioration of the operation of a large number of businesses or organisations (in or outside Singapore) which rely on or are enabled by that foundational digital infrastructure service.

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

(*a*) identify the foundational digital infrastructure service in relation to which the provider is designated as a major foundational digital infrastructure service provider;

(*b*) identify the provider of the foundational digital infrastructure service so designated as a major foundational digital infrastructure service provider;

(*c*) describe the computer or computer systems (or class of computers or computer systems) stated to be necessary for the continuous delivery of the foundational digital infrastructure service;

(*d*) inform the major foundational digital infrastructure service provider regarding the provider's duties and responsibilities under this Act that arise from the designation;

(*e*) provide the name and contact particulars of the officer assigned by the Commissioner to supervise the major foundational digital infrastructure service provider in relation to the cybersecurity of the major foundational digital infrastructure;

(*f*) inform the major foundational digital infrastructure service provider that any representations against the designation are to be made to the Commissioner by a specified date, being a date not earlier than 14 days after the date of the notice; and

(*g*) inform the major foundational digital infrastructure service provider that the provider may appeal to the Minister against the designation, and provide information on the applicable procedure.

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

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

(5) A provider of a foundational digital infrastructure service mentioned in this section or section 18H who is located outside Singapore may appoint a person in Singapore to accept service of notices or directions under this Act.

(6) A major foundational digital infrastructure service provider who is located outside Singapore must appoint a person in Singapore to accept service of notices or directions under this Act.

(7) In this section —

(*a*) a provider provides a foundational digital infrastructure service —

(i) from within Singapore — when the provider is present in Singapore when providing the service; or

(ii) wholly or partially from Singapore — when all or part of the computers or computer systems used to provide the foundational digital infrastructure service are located in Singapore;

(*b*) the "loss or impairment" of the provision of a foundational digital infrastructure service includes the loss or impairment of the availability, confidentiality or integrity of data stored, transmitted or processed in relation to the provision of that service; and

(*c*) a reference to a person in Singapore is a reference to —

(i) an individual physically present in Singapore; or

(ii) an entity incorporated or established under any written law, or constituted or organised under a law of a foreign country or territory but registered under any written law.

Power to obtain information to ascertain if criteria for major foundational digital infrastructure service provider fulfilled

18H.—(1) This section applies where the Commissioner has reason to believe that a provider of a foundational digital infrastructure service may fulfil the criteria to be designated as a major foundational digital infrastructure service provider.

(2) The Commissioner may, by notice given in the prescribed form and manner, require any person who appears to be a provider of a foundational digital infrastructure service, to provide to the Commissioner, within a reasonable period specified in the notice, such relevant information relating to that service as may be required by the Commissioner for the purpose of ascertaining whether the provider fulfils the criteria to be designated as a major foundational digital infrastructure service provider.

(3) Without limiting subsection (2), for the purpose of ascertaining whether the provider of a foundational digital infrastructure service fulfils the criteria to be designated as a major foundational digital infrastructure service provider, the Commissioner may in the notice require the provider to provide —

(*a*) information relating to —

(i) the function that the foundational digital infrastructure service is employed to serve; and

(ii) the extent to which the operations of businesses or organisations in Singapore rely on or are enabled by that foundational digital infrastructure service;

(*b*) in the case of a person who appears to provide a foundational digital infrastructure service wholly or partially from Singapore, information relating to —

(i) whether the foundational digital infrastructure service is provided wholly or partially from Singapore; and

(ii) the extent to which the operations of businesses or organisations, in or outside Singapore, rely on or are enabled by that foundational digital infrastructure service; and

(*c*) any other information that the Commissioner may require in order to ascertain whether the provider of a foundational digital infrastructure service fulfils the criteria to be designated as a major foundational digital infrastructure service provider.

(4) Any person who —

(*a*) without reasonable excuse, fails to comply with a notice issued under subsection (2); and

(*b*) continues, after the expiry of the period specified in the notice, to provide a foundational digital infrastructure service —

(i) whether from within or outside Singapore, to persons in Singapore; or

(ii) wholly or partially from Singapore,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding the greater of $200,000 or 10 percent of the annual turnover of the person's business in Singapore and, in the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part of a day during which the offence continues after conviction.

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

Withdrawal of designation of major foundational digital infrastructure service provider

18I. The Commissioner may, by written notice, withdraw the designation of a major foundational digital infrastructure service provider at any time if the Commissioner is of the opinion that the provider no longer fulfils the criteria to be designated as a major foundational digital infrastructure service provider.

Extension of designation of major foundational digital infrastructure service provider

18J.—(1) At any time before the expiry of the designation of a major foundational digital infrastructure service provider, the Commissioner may, by written notice, extend the designation of the major foundational digital infrastructure service provider, if the Commissioner is of the opinion that the provider continues to fulfil the criteria to be designated as a major foundational digital infrastructure service provider.

(2) Any extension of a designation under subsection (1) has effect for a period of 5 years starting from the expiry of the earlier designation, unless the designation is withdrawn by the Commissioner before the extension takes effect or before the expiry of the period of extension.

Furnishing of information relating to major foundational digital infrastructure

18K.—(1) The Commissioner may by notice given in the prescribed form and manner, require the major foundational digital infrastructure service provider to furnish, within a reasonable period specified in the notice, the following:

(*a*) information on the measures in place to safeguard the cybersecurity of the major foundational digital infrastructure;

(*b*) information on the design features of the major foundational digital infrastructure which affect cybersecurity risk;

(*c*) any other information that the Commissioner may require in order to ascertain the level of cybersecurity of the major foundational digital infrastructure.

(2) Any major foundational digital infrastructure service provider who —

(*a*) without reasonable excuse, fails to comply with a notice mentioned in subsection (1); and

(*b*) continues to provide the foundational digital infrastructure service in relation to which the provider is designated under section 18G(1)(*b*)(i) or (ii) after the expiry of the period specified in the notice,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding the greater of $200,000 or 10 percent of the annual turnover of the person's business in Singapore and, in the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part of a day during which the offence continues after conviction.

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

(4) The major foundational digital infrastructure service provider is not treated as being in breach of any contractual obligation mentioned in subsection (3) for doing or omitting to

do any act, if the act is done or omitted to be done with reasonable care and in good faith and for the purpose of complying with a notice issued under subsection (1).

Power of Commissioner to issue written directions

18L.—(1) The Commissioner may, if the Commissioner thinks —

(*a*) it is necessary or expedient for ensuring the cybersecurity of a major foundational digital infrastructure; or

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

issue a written direction, either of a general or specific nature, to the major foundational digital infrastructure service provider or a class of such major foundational digital infrastructure service providers.

(2) Without limiting subsection (1), a direction under that subsection may relate to —

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

(*b*) compliance with any prescribed technical or other standards relating to cybersecurity in respect of the major foundational digital infrastructure;

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

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

(*e*) any other matter that the Commissioner may consider necessary or expedient to ensure the cybersecurity of the major foundational digital infrastructure.

(3) A direction under subsection (1) must specify a deadline for compliance, and may be revoked at any time by the Commissioner.

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

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

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

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

(6) Any person who —

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

(*b*) continues to provide the foundational digital infrastructure service in relation to which the person is designated under section 18G(1)(*b*)(i) or (ii) after the deadline for compliance specified in the direction,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding the greater of $200,000 or 10 percent of the annual turnover of the person's business in Singapore and, in the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part of a day during which the offence continues after conviction.

Duty to report cybersecurity incident affecting major foundational digital infrastructure service provider

18M.—(1) The major foundational digital infrastructure service provider must notify the Commissioner of the occurrence of any of the following in the prescribed form and manner, within the prescribed period after becoming aware of such occurrence:

(*a*) a prescribed cybersecurity incident in respect of the major foundational digital infrastructure or any other computer or computer system under the major foundational digital infrastructure service provider's control, where the incident results in a disruption or degradation to the continuous delivery, in Singapore, of the foundational digital infrastructure service for which the provider is designated;

(*b*) a prescribed cybersecurity incident in respect of the major foundational digital infrastructure or any other computer or computer system under the major foundational digital infrastructure service provider's control, where the incident has a significant impact on the major foundational digital infrastructure service provider's business operations in Singapore.

(2) The major foundational digital infrastructure service provider must establish such mechanisms and processes for the purposes of detecting cybersecurity threats and incidents in respect of the major foundational digital infrastructure, as set out in any applicable code of practice.

(3) Any major foundational digital infrastructure service provider who, without reasonable excuse, fails to comply with subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding the greater of $200,000 or 10 percent of the annual turnover of the person's business in Singapore.".

New section 29A

18. In the principal Act, after section 29, insert —

"**Monitoring powers of licensing officer**

29A.—(1) The licensing officer has, for the purposes of the execution of this Part, power to do all or any of the following:

(*a*) to enter, inspect and examine at a reasonable time the place of business of a licensee;

(*b*) to require a licensee to produce any records, accounts and documents kept by the licensee within such reasonable time as is specified by the licensing officer;

(*c*) to inspect, examine and make copies of any records, accounts and documents so produced;

(*d*) to make such inquiry as may be necessary to ascertain whether a licensee has complied with any condition of a licence, or any provisions of this Part.

(2) Where any records, accounts and documents mentioned in subsection (1) are kept in electronic form, then —

(*a*) the power of the licensing officer in subsection (1)(*b*) to require any records, accounts or documents to be produced for inspection includes the power to require a copy of the records, accounts or documents to be made available for inspection in legible form (and subsection (1)(*c*) is to accordingly apply in relation to any copy so made available); and

(*b*) the power of the licensing officer under subsection (1)(*c*) to inspect any records, accounts or documents includes the power to require any person on the premises in question to give the licensing officer such assistance as he or she may reasonably require to enable him or her —

(i) to inspect and make copies of the records, accounts or documents in legible form or to make records of information contained in them; or

(ii) to inspect and check the operation of any computer, and any associated apparatus or material, that is or has been in use in connection with the keeping of the records, accounts or documents.

(3) Any person who, without reasonable excuse, fails to comply with any requirement imposed under this section 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.".

New sections 35A, 35B and 35C

19. In the principal Act, before section 36, insert —

"**Codes of practice and standards of performance**

35A.—(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 following persons with respect to measures to be taken by them to ensure the cybersecurity of the computers or computer systems indicated:

(i) owners of provider-owned critical information infrastructure — the provider-owned critical information infrastructure;

(ii) designated providers responsible for third-party-owned critical information infrastructure — the third-party-owned critical information infrastructure for which they are responsible;

(iii) owners of systems of temporary cybersecurity concern — the systems of temporary cybersecurity concern;

(iv) entities of special cybersecurity interest — the systems of special cybersecurity interest in relation to which they are designated;

(v) major foundational digital infrastructure service providers — the major foundational digital infrastructure in relation to which they are designated; and

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

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

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

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

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

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

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

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

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

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

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

(6) Subject to subsections (4) and (7), every person mentioned in subsection (1) must comply with the codes of practice and standards of performance that apply to the person.

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

Appeal to Minister against decision, etc., under Parts 3, 3A, 3B, 3C and 3D, etc.

35B.—(1) This section applies to appeals to the Minister against any decision, order or written direction of the Commissioner under Part 3, 3A, 3B, 3C or 3D set out in subsection (2), or any code of practice or standard of performance issued, approved or amended by the Commissioner.

(2) A person who is aggrieved by —

(*a*) the decision of the Commissioner to issue a notice under —

(i) section 7(1) or (1A) designating the provider-owned critical information infrastructure as such;

(ii) section 16A(1) designating the designated provider responsible for third-party-owned critical information infrastructure as such;

(iii) section 17(1) designating the system of temporary cybersecurity concern as such;

(iv) section 18(1) designating the entity of special cybersecurity interest as such; or

(v) section 18G(1) designating the major foundational digital infrastructure service provider as such;

(*b*) the decision of the Commissioner to issue a notice under —

(i) section 9A(1) extending the designation of the provider-owned critical information infrastructure as such;

(ii) section 16D(1) extending the designation of the designated provider responsible for third-party-owned critical information infrastructure as such;

(iii) section 17C(1) extending the designation of the system of temporary cybersecurity concern as such;

(iv) section 18C(1) extending the designation of the entity of special cybersecurity interest as such; or

(v) section 18J(1) extending the designation of the major foundational digital infrastructure service provider as such;

(*c*) an order of the Commissioner under section 16B(5), 16E(2), 16F(2) or (3), 16H(2), 16I(2) or 16J(2);

(*d*) a written direction of the Commissioner under section 12(1), 16(2), 16G(1), 16L(2), 17E(1), 18E(1) or 18L(1); or

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

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

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

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

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

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

(5) Where an appeal has been made to the Minister under subsection (2), the Minister may require —

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

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

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

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

(7) Unless otherwise provided by this Act or allowed by the Minister, where an appeal is lodged under this section, the decision, order, direction or other thing appealed against must be complied with until the determination of the appeal.

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

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

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

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

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

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

Appeals Advisory Panel

35C.—(1) Where the Minister considers that an appeal lodged under section 35B(2) involves issues the resolution or understanding of which require particular technical skills or specialised knowledge, the Minister may establish an Appeals Advisory Panel to provide advice to the Minister in respect of the appeal.

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

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

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

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

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

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

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

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

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

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

New sections 37A to 37D

20. In the principal Act, after section 37, insert —

"**Civil penalty**

37A.—(1) Whenever it appears to the Commissioner that any person has contravened any provision in Part 3, 3A, 3B, 3C or 3D that is punishable as an offence, the Commissioner may, with the consent of the Public Prosecutor, bring an action in a court against the person to seek an order for a civil penalty in respect of that contravention in lieu of prosecution.

(2) If the court is satisfied, on a balance of probabilities, that the person has contravened a provision in Part 3, 3A, 3B, 3C or 3D that is punishable as an offence, the court may make an order against the person for the payment of a civil penalty of a sum not exceeding —

(*a*) in a case of a contravention punishable under section 8(4), 10(2), 12(6), 13(2), 14(3), 15(7), 16B(4) or (6), 16E(3) or (5), 16F(4), 16G(6), 16H(3) or (6), 16I(3) or (6), 16J(3) or (10), 17A(4), 17D(2), 17E(6) or 17F(3), the greater of the following:

(i) 10 percent of the annual turnover of the person's business in Singapore;

(ii) $500,000;

(*b*) in a case of a contravention punishable under section 18A(4), 18D(2), 18E(6), 18F(3), 18H(4), 18K(2), 18L(6) or 18M(3), the greater of the following:

(i) 5 percent of the annual turnover of the person's business in Singapore;

(ii) $200,000;

(*c*) in the case of a contravention punishable under section 10(7), 15(8), 16E(10), 16J(11) or 16K(3) — $150,000; or

(*d*) in the case of a contravention punishable under section 16(3) or 16L(3) or in any other case — $100,000.

(3) Despite subsection (2), the court may make an order against a person against whom an action has been brought under this section if the Commissioner, with the consent of the Public Prosecutor, has agreed to allow the person to consent to the order with or without admission of a contravention of a provision in Part 3, 3A, 3B, 3C or 3D that is punishable as an offence, and the order may be made on such terms as may be agreed between the Commissioner and the defendant.

(4) Nothing in this section prevents the Commissioner from entering into an agreement with any person to pay, with or without admission of liability, a civil penalty within the limits referred to in subsection (2) for a contravention of any provision in Part 3, 3A, 3B, 3C or 3D that is punishable as an offence.

(5) A civil penalty imposed under this section must be paid into the Consolidated Fund and is to be treated as a judgment debt due to the Government for the purposes of section 10 of the Government Proceedings Act 1956.

(6) If the person fails to pay the civil penalty imposed on the person within the time specified in the court order mentioned in subsection (3) or specified under the agreement mentioned in subsection (4), the Commissioner may recover the civil penalty on behalf of the Government as though the civil penalty were a judgment debt due to the Commissioner.

(7) Any defence that is available to a person who is prosecuted for a contravention of any provision in Part 3, 3A, 3B, 3C or 3D that is punishable as an offence, is also available to a defendant in an action under this section in respect of that contravention.

(8) For the purposes of this section —

(*a*) sections 36(1) and 37(1) apply, with the necessary modifications, to a proceeding for a civil penalty to be ordered in respect of a contravention of a provision in Part 3, 3A, 3B, 3C or 3D that is punishable as an offence; and

(*b*) the annual turnover of a person's business is ascertained from the person's latest audited accounts.

Action under section 37A not to commence, etc., in certain situations

37B.—(1) An action under section 37A must not be commenced after the expiration of 6 years from the date of the contravention of any of the provisions in Part 3, 3A, 3B, 3C or 3D that is punishable as an offence.

(2) An action under section 37A must not be commenced if the person has been convicted or acquitted in criminal proceedings for the contravention of any of the provisions in Part 3, 3A, 3B, 3C or 3D that is punishable as an offence, except where the person has been acquitted on the ground of the withdrawal of the charge against the person.

(3) An action under section 37A must be stayed after criminal proceedings have been commenced against the person for the contravention of any of the provisions in Part 3, 3A, 3B, 3C or 3D that is punishable as an offence, and may thereafter be continued only if —

(*a*) that person has been discharged in respect of that contravention and the discharge does not amount to an acquittal; or

(*b*) the charge against the person in respect of that contravention has been withdrawn.

(4) No proceedings shall be instituted against a person for an offence in respect of a contravention of any of the provisions in Part 3, 3A, 3B, 3C or 3D after —

(*a*) a court has made an order against the person for the payment of a civil penalty under section 37A; or

(*b*) the person has entered into an agreement with the Commissioner to pay, with or without admission of liability, a civil penalty under section 37A(4),

in respect of that contravention.

Civil penalty against officer of corporation, etc.

37C.—(1) Where it appears to the Commissioner that a corporation, unincorporated association or partnership (called in this section the contravening person) has contravened any provision in Part 3, 3A, 3B, 3C or 3D that is punishable as an offence, the Commissioner may, with the consent of the Public Prosecutor, bring an action in a court against a person (called in this section the defendant) to seek an order for a civil penalty in respect of that contravention as if the defendant had committed the contravention, in lieu of prosecution of the defendant under section 36(2) or 37(2), if it appears to the Commissioner that —

(*a*) the defendant is —

(i) in a case where the contravening person is a corporation —

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

(B) an individual involved in the management of the corporation and in a position to influence the conduct of the corporation in relation to the commission of the contravention; or

(ii) in a case where the contravening person is an unincorporated association or a partnership —

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

(B) a partner in the partnership; or

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

(*b*) the defendant —

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

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

(iii) knew or ought reasonably to have known that the contravention by the contravening person (or a contravention 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 contravention.

(2) Subject to section 37D(2), the action mentioned in subsection (1) may be brought against the defendant in respect of the contravention, whether or not any action is brought against the contravening person under section 37A in respect of the same contravention.

(3) If the court is satisfied, on a balance of probabilities, that the contravening person has contravened a provision in Part 3, 3A, 3B, 3C or 3D that is punishable as an offence and the defendant played a role in the contravention mentioned in subsection (1)(*b*), the court may make an order against the defendant for the payment of a civil penalty of a sum not exceeding —

(*a*) in a case of a contravention punishable under section 8(4), 10(2), 12(6), 13(2), 14(3), 15(7), 16B(4) or (6), 16E(3) or (5), 16F(4), 16G(6), 16H(3) or (6), 16I(3) or (6), 16J(3) or (10), 17A(4), 17D(2), 17E(6) or 17F(3) — $500,000;

(*b*) in a case of a contravention punishable under section 18A(4), 18D(2), 18E(6), 18F(3), 18H(4), 18K(2), 18L(6) or 18M(3) — $200,000;

(*c*) in the case of a contravention punishable under section 10(7), 15(8), 16E(10), 16J(11) or 16K(3) — $150,000; or

(*d*) in the case of a contravention punishable under section 16(3) or 16L(3) or in any other case — $100,000.

(4) Section 37A(3) to (6) applies in relation to an action brought against a defendant under subsection (1) as those provisions apply in relation to an action under section 37A.

(5) Any defence that would be available to —

(*a*) the contravening person if it were prosecuted for its contravention; or

(*b*) the defendant if he or she were prosecuted under section 36 or 37 in respect of that contravention,

is also available to the defendant in an action under subsection (1) in respect of that contravention.

(6) In this section —

"corporation" includes a limited liability partnership within the meaning of section 2(1) of the Limited Liability Partnerships Act 2005;

"officer" —

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

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

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

(*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, and includes —

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

(ii) any person purporting to act in any such capacity;

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

Actions not to commence or stayed in certain situations

37D.—(1) An action against a defendant under section 37C must not be commenced after the expiration of 6 years from the date of the contravention of a provision in Part 3, 3A, 3B, 3C or 3D that is punishable as an offence (called in this section the primary contravention) by a contravening person mentioned in section 37C(1).

(2) Except with the permission of court, no action may be brought against a defendant under section 37C which relates to a primary contravention by a contravening person mentioned in section 37C(1) (in relation to the defendant), after the commencement of —

(*a*) criminal proceedings in respect of the primary contravention against the contravening person; or

(*b*) an action under section 37A in respect of the primary contravention against the contravening person,

and any such action pending on the date of commencement of the proceedings or action in paragraph (*a*) or (*b*) must be stayed, and may not thereafter be continued except with the permission of court.

(3) Permission under subsection (2) must not be granted if —

(*a*) in the criminal proceedings mentioned in subsection (2)(*a*), the contravening person has been acquitted of the primary contravention; or

(*b*) in the action under section 37A mentioned in subsection (2)(*b*), the court is not satisfied that the contravening person has committed the primary contravention.

(4) An action under section 37C must not be commenced if the defendant has been convicted or acquitted in criminal proceedings under section 36(2) or 37(2) for an offence in respect of the primary contravention, except where the defendant has been acquitted on the ground of the withdrawal of the charge against the defendant.

(5) An action under section 37C must be stayed after criminal proceedings have been commenced against the defendant under section 36(2) or 37(2) for an offence in respect of the primary contravention, and may thereafter be continued only if —

(*a*) that defendant has been discharged in respect of that contravention and the discharge does not amount to an acquittal; or

(*b*) the charge against the defendant in respect of that contravention has been withdrawn.

(6) No proceedings shall be instituted against a defendant under section 36(2) or 37(2) for an offence in respect of a contravention of any of the provisions in Part 3, 3A, 3B, 3C or 3D after —

(*a*) a court has made an order against the defendant for the payment of a civil penalty under section 37C; or

(*b*) the defendant has entered into an agreement with the Commissioner to pay, with or without admission of liability, a civil penalty under section 37A(4) read with section 37C(4),

in respect of that contravention.".

Amendment of section 40

21. In the principal Act, in section 40 —

(*a*) renumber the section as subsection (1) of that section; and

(*b*) after subsection (1), insert —

"(2) A District Court has jurisdiction to hear and determine any action for a civil penalty to be imposed in respect of a contravention of a provision under Part 3, 3A, 3B, 3C or 3D regardless of the monetary amount of the civil penalty.".

New section 41A

22. In the principal Act, after section 41, insert —

"**Extension of time**

41A.—(1) A person who, in any particular case, is unable to do any thing that the person is required to do under Part 3, 3A, 3B, 3C or 3D (including any direction or order issued under those Parts) within the time specified for it may apply in writing to the Commissioner for an extension of time.

(2) The Commissioner may grant an extension of time (whether for the same or less than the period of extension applied for), upon being satisfied that there are good reasons to do so.".

Amendment of section 43

23. In the principal Act, in section 43 —

(*a*) in subsection (7)(*b*), after sub-paragraph (i), insert —

"(i*a*) bringing an action to seek an order for a civil penalty under section 37A(1) or 37C(1) — where the information relates to the contravention in respect of which the civil penalty is sought;"; and

(*b*) in subsection (10)(*c*), replace "section 18" with "section 35C".

Amendment of section 44

24. In the principal Act, in section 44(1), replace "section 18" with "section 35C".

Amendment of section 45

25. In the principal Act, in section 45(1), replace "Part 3" with "Part 3, 3A, 3B, 3C or 3D, or for a civil penalty under section 37A or 37C,".

Amendment of section 47

26. In the principal Act, in section 47(1), replace "First or Second Schedule" with "First, Second or Third Schedule".

New section 47A

27. In the principal Act, after section 47, insert —

"**Rules of Court**

47A. The Rules Committee appointed under section 80(3) of the Supreme Court of Judicature Act 1969 may make Rules of Court —

(*a*) to regulate and prescribe the procedure and practice to be followed in respect of proceedings for a civil penalty to be imposed in respect of a contravention of a provision under Part 3, 3A, 3B, 3C or 3D; and

(*b*) to provide for costs and fees of such proceedings, and for regulating any matter relating to the costs of such proceedings.".

Amendment of section 48

28. In the principal Act, in section 48 —

(*a*) in subsection (2)(*a*), replace "critical information infrastructure" with "provider-owned critical information infrastructure, designated provider responsible for third-party-owned critical information infrastructure, system of temporary cybersecurity concern, entity of special cybersecurity interest or major foundational digital infrastructure service provider";

(*b*) in subsection (2)(*b*), replace "critical information infrastructure" with "provider-owned critical information infrastructure, third-party-owned critical information infrastructure, system of temporary cybersecurity concern, system of special cybersecurity interest or major foundational digital infrastructure";

(*c*) in subsection (2)(*c*), replace "critical information infrastructure" with "provider-owned critical information infrastructure or system of temporary cybersecurity concern, designated provider responsible for third-party-owned critical information infrastructure, entity of special cybersecurity interest or major foundational digital infrastructure service provider";

(*d*) in subsection (2)(*d*), replace "critical information infrastructure to be reported by the owner of the critical information infrastructure" with "provider-owned critical information infrastructure or a third-party-owned critical information infrastructure to be reported by the owner of the provider-owned critical information infrastructure or the designated provider responsible for third-party-owned critical information infrastructure";

(*e*) in subsection (2), replace paragraph (*e*) with —

"(*e*) the type of cybersecurity incidents relating to —

(i) a provider-owned critical information infrastructure that are

required to be reported by the owner of the provider-owned critical information infrastructure;

(ii) a third-party-owned critical information infrastructure that are required to be reported by the designated provider responsible for third-party-owned critical information infrastructure;

(iii) a system of temporary cybersecurity concern that are required to be reported by the owner of the system of temporary cybersecurity concern;

(iv) a system of special cybersecurity interest that are required to be reported by the entity of special cybersecurity interest; or

(v) a major foundational digital infrastructure that are required to be reported by the major foundational digital infrastructure service provider;";

(*f*) in subsection (2)(*f*), replace "critical information infrastructure" with "provider-owned critical information infrastructure or the owner of a third-party-owned critical information infrastructure";

(*g*) in subsection (2), after paragraph (*i*), insert —

"(*ia*) the use of any accreditation, certification or inspection mark of the Cyber Security Agency of Singapore;"; and

(*h*) after subsection (3), insert —

"(4) The powers conferred by this section do not extend to any matter for which Rules of Court may be made under section 47A.".

Amendment of Second Schedule

29. In the principal Act, in the Second Schedule, in paragraph 2, before the definition of "managed security operations centre (SOC) monitoring service", insert —

""computer" includes a virtual computer;

"computer system" includes a virtual computer system;".

New Third Schedule

30. In the principal Act, after the Second Schedule, insert —

"THIRD SCHEDULE

Sections 2(1) and 47(1)

FOUNDATIONAL DIGITAL INFRASTRUCTURE SERVICES

1. The following services are specified as foundational digital infrastructure services:

(*a*) cloud computing service;

(*b*) data centre facility service.

2. In this Schedule —

"cloud computing service" means a service, delivered from a computer or computer system in Singapore or outside Singapore, that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations;

"data centre facility service" means any service which relies on a computer or computer system in Singapore to facilitate data storage, processing and transmission by another person through the centralised accommodation, interconnection and operation of one or more computers or computer systems, encompassed within a facility in Singapore dedicated to that purpose, which —

(*a*) includes a service to host the computers or computer systems within the facility; and

(*b*) excludes a service provided from a facility which is owned by the sole party using the service.".

Miscellaneous amendments

31. In the principal Act —

(*a*) in the following provisions, replace "critical information infrastructure" wherever it appears with "provider-owned critical information infrastructure":

Section 3(1)

Section 7(1), (2)(*a*), (*b*) and (*d*), (6), (7) and (8)

Section 8(1), (2) and (3)(*c*)

Section 9

Section 10(1), (2), (3), (4), (5), (6) and (7)

Section 12(1) and (2)(*d*)

Section 13(1) and (3)(*a*) and (*b*)

Section 14(1), (2) and (3)

Section 15(1), (2), (3), (5)(*a*) and (*b*), (6), (7) and (8)

Section 16(1) and (2)

Section 20(3)(*a*) and (*d*);

(*b*) in Part 3, in the Part heading, before "CRITICAL INFORMATION INFRASTRUCTURE", insert "PROVIDER-OWNED";

(*c*) in the following sections, in the section heading, before "**critical information infrastructure**", insert "**provider-owned**":

Section 7

Section 9

Section 10

Section 13

Section 14

Section 15;

(*d*) in section 8, replace the section heading with —

"**Power to obtain information to ascertain if criteria for provider-owned critical information infrastructure fulfilled**"; and

(*e*) in sections 8(1), (2) and (3)(*c*) and 9, replace "criteria of" with "criteria to be designated as".

Saving and transitional provisions

32.—(1) Despite section 5(*a*), any Assistant Commissioner appointed in respect of a critical information infrastructure under section 4(1)(*b*) read with section 4(2) of the principal Act as in force immediately before the date of commencement of section 5(*a*), and whose appointment as such is valid on that date, is deemed to be appointed in respect of a provider-owned critical information infrastructure under section 4(1)(*b*) read with section 4(2) of the principal Act as replaced by section 5(*a*).

(2) Despite section 10, any code of practice or standard of performance issued or approved (and not revoked) under section 11 of the principal Act as in force immediately before the date of commencement of section 10 is deemed to be issued or approved under section 35A of the principal Act (as inserted by section 19).

(3) Despite section 14, any appeal made under section 17 of the principal Act as in force immediately before the date of commencement of section 14, and which is not withdrawn or determined as at that date, is deemed to be made under section 35B of the principal Act (as inserted by section 19).

(4) Despite section 14, any Appeals Advisory Panel established under section 18 of the principal Act as in force immediately before the date of commencement of section 14, and which is not dissolved as at that date, is deemed to be an Appeals Advisory Panel established under section 35C of the principal Act (as inserted by section 19).

(5) Sections 37A and 37C of the principal Act (as inserted by section 20) do not apply to any contravention of a provision of the principal Act committed before the date of commencement of section 20.

(6) Any notice of designation of a critical information infrastructure issued under section 7 of the principal Act as in force immediately before the date of commencement of section 31, and in respect of which the designation is not withdrawn as at that date, is deemed to be a notice of designation of a provider-owned critical information infrastructure issued under section 7 of the principal Act as amended by section 31.

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

EXPLANATORY STATEMENT

This Bill seeks to amend the Cybersecurity Act 2018 (the Act) for the following main purposes:

(*a*) to make changes to the regime in Part 3 governing critical information infrastructure (CII), which are renamed as "provider-owned critical information infrastructure";

(*b*) to regulate 4 new classes of persons:

(i) designated providers responsible for the cybersecurity of a new category of CII (called "third-party-owned critical information infrastructure") which is not owned by the provider of the essential service which depends on the CII for the delivery of the essential service (regulated under the new Part 3A inserted by clause 14);

(ii) owners of systems of temporary cybersecurity concern (regulated under the new Part 3B inserted by clause 15);

(iii) entities of special cybersecurity interest (regulated under the new Part 3C inserted by clause 16);

(iv) major foundational digital infrastructure service providers (regulated under the new Part 3D inserted by clause 17);

(*c*) to introduce provisions for a court to order the payment of a civil penalty against a person who contravenes a provision of Part 3, 3A, 3B, 3C or 3D that is punishable as an offence, in lieu of prosecution;

(*d*) to confer additional powers on the Commissioner of Cybersecurity (the Commissioner) to monitor licensed cybersecurity service providers;

(*e*) to apply certain portions of the Act to virtual computers and virtual computer systems.

Clause 1 relates to the short title and commencement.

Clause 2 amends the long title to extend the scope of the Act to cover the regulation of certain persons in relation to the cybersecurity of certain computers or computer systems, which are designated providers responsible for third-party-owned CII, owners of systems of temporary cybersecurity concern, entities of special cybersecurity interest, and major foundational digital infrastructure service providers.

Clause 3 amends section 2 to insert new definitions necessary to support other amendments to the Act and, in particular, definitions relating to the 4 new classes of regulated persons. Clause 3(*c*) inserts a definition of "digital service" which is adapted with modification from the definition of "service" in Article 1(*b*) of the Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (Official Journal of the European Union, L 241, 17.9.2015, p. 3).

Clause 3(*i*) inserts new definitions of "virtual computer" and "virtual computer system" in section 2(1). Clause 3(*j*) inserts a new section 2(3) which includes "virtual computer" and "virtual computer system" into the existing definitions of "computer" and "computer system" for the purposes of Part 3 (except section 7(1A)) and Parts 3A, 3B, 3C and 4 and certain other sections. (A similar inclusion of "virtual computer" and "virtual computer system" in the meaning of the terms "computer" and "computer system" is made for the purposes of the Second Schedule by clause 29). The new section 2(3)(*d*) contains a definition of "owner" in relation to a provider-owned CII, third-party-owned CII or system of temporary cybersecurity concern that is a virtual computer or virtual computer system. The new section 2(3)(*e*) provides for what a change in the beneficial or legal ownership (including any share in such ownership) means in relation to a provider-owned CII or third-party-owned CII that is a virtual computer or virtual computer system.

Clause 4 amends section 3 to provide for the scope of application of certain new provisions inserted in the Act.

Clause 5 amends section 4 to cater for the expanded scope of the Act and the expanded powers of the Commissioner. Clause 5(*a*) replaces the existing section 4(2) with 2 new subsections, namely, a new section 4(2) to provide for the appointment of Assistant Commissioners in respect of provider-owned CII and systems of temporary cybersecurity concern, and new section 4(2A) to provide for

the appointment of Assistant Commissioners in respect of designated providers responsible for third-party-owned CII, entities of special cybersecurity interest, and major foundational digital infrastructure service providers.

Clause 6 amends section 5 to expand the Commissioner's duties and functions in line with the Commissioner's expanded powers. In addition, clause 6(*d*) adds a reference to "international certification schemes" in the renumbered section 5(1)(*k*). Clause 6(*e*) establishes that the office of the Commissioner is to be known as the Cyber Security Agency of Singapore.

Clause 7 inserts a new section 6A to make it an offence for a person to use the Cyber Security Agency of Singapore's gazetted symbol or representation without the Commissioner's prior written consent.

Clause 8(*a*) inserts a new section 7(1A) which will empower the Commissioner to designate as a provider-owned CII, a computer or computer system located wholly outside Singapore, if the conditions in section 7(1A)(*a*) and (*b*) are met. To avoid doubt, the new section 7(1A) will not enable the Commissioner to take any enforcement action outside Singapore.

Clause 9 inserts a new section 9A which empowers the Commissioner to extend the designation of the provider-owned CII if the Commissioner is of the opinion that the designation criteria in section 7(1) or new section 7(1A) continue to be fulfilled.

Clause 10 deletes section 11, which will be replaced by a new section 35A (inserted by clause 19).

Clause 11(*a*) inserts a new section 12(2)(*aa*) to provide that a direction may be issued under section 12(1) relating to compliance with any prescribed technical or other standards relating to cybersecurity in respect of the provider-owned CII. Clause 11(*b*) replaces section 12(3) to provide that a direction issued under section 12(1) must specify a deadline for compliance.

Clause 12 amends section 14 to insert the following 2 new types of prescribed cybersecurity incidents to the list of such incidents which must be reported to the Commissioner. The 2 new types are —

(*a*) prescribed cybersecurity incidents in respect of any computer (or computer system) under the control of the owner of a provider-owned CII, where the computer (or computer system) is not interconnected with and does not communicate with the provider-owned CII (new section 14(1)(*ba*)); and

(*b*) prescribed cybersecurity incidents in respect of any computer (or computer system) under the control of a supplier to the owner that is interconnected with or that communicates with the provider-owned CII (new section 14(1)(*bb*)).

Clause 13(*a*) inserts a reference in section 15(1)(*a*) to any prescribed technical or other standards relating to cybersecurity that are to be maintained in respect of the provider-owned CII. Clause 13(*b*) amends section 15(4) to empower the Commissioner (under the new section 15(4)(*d*)) to authorise certain officers to inspect the provider-owned CII if it appears to the Commissioner that —

(*a*) the owner of the provider-owned CII has not complied with a provision of the Act, a prescribed technical or other standard relating to cybersecurity, or an applicable code of practice or standard of performance; or

(*b*) any information provided by the owner of the provider-owned CII under section 10 is false, misleading, inaccurate or incomplete.

Clause 14 deletes sections 17 and 18 (which are re-enacted as part of new sections 35B and 35C, respectively, by clause 19), and inserts new Part 3A in their place. The new Part 3A (comprising new sections 16A to 16L) regulates providers of an essential service which are made responsible for the cybersecurity of third-party-owned CII on which the delivery of their essential service is dependent (such a provider is referred to as a designated provider responsible for third-party-owned critical information infrastructure).

The new section 16A empowers the Commissioner to designate such a provider of an essential service as a designated provider responsible for third-party-owned CII. The new Part 3A contains provisions which are adapted from the provisions of Part 3 as amended by the Bill, and additional provisions requiring the designated provider to obtain legally binding commitments from the owner of the third-party-owned CII to perform certain actions, which in turn enable the designated provider to fulfil its own obligations under Part 3A. Where sections 10, 13, 14 and 15 in Part 3 impose a requirement on the owner of the provider-owned CII, Part 3A requires the designated provider to obtain a legally binding commitment from the owner of the third-party-owned CII to perform actions that enable the designated provider to meet that requirement (new sections 16E(1), 16H(1), 16I(1) and 16J(1)). If the legally binding commitment is not obtained, the Commissioner may direct the designated provider to stop using that third-party-owned CII (new sections 16E(2), 16H(2), 16I(2) and 16J(2)).

The new section 16F (a new substantive provision) requires the designated provider responsible for third-party-owned CII to obtain a legally binding commitment from the owner of the third-party-owned CII that the owner will ensure that any applicable prescribed technical or other standards relating to cybersecurity are maintained in respect of the third-party-owned CII. If the standards are not maintained, the Commissioner may issue a direction mentioned in the new section 16G(2)(*c*) relating to the steps to be taken by the provider to require the owner of the third-party-owned CII to ensure that the standards are maintained. If the standards are still not maintained, the Commissioner may order

the designated provider (under new section 16F(3)) to stop using the third-party-owned CII.

Clause 15 inserts a new Part 3B (comprising new sections 17 to 17F) which regulates owners of systems of temporary cybersecurity concern in relation to the cybersecurity of such systems.

Under the new section 17(1), the Commissioner may designate a computer or computer system located wholly or partly in Singapore as a system of temporary cybersecurity concern on the basis that for a limited period there is a high risk to the cybersecurity of that computer or computer system, and the loss or compromise of that computer or computer system will have a serious detrimental effect on the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore.

The new section 17A empowers the Commissioner to require any person appearing to be exercising control over a computer or computer system, to provide relevant information for the purpose of ascertaining whether the computer or computer system fulfils the criteria to be designated as a system of temporary cybersecurity concern.

The new section 17B empowers the Commissioner to withdraw the designation of a system of temporary cybersecurity concern at any time if the Commissioner is of the opinion that the computer or computer system no longer fulfils the criteria to be designated as such.

The new section 17C empowers the Commissioner to extend the designation of the system of temporary cybersecurity concern if the Commissioner is of the opinion that the computer or computer system continues to fulfil the criteria to be designated as such.

The new section 17D empowers the Commissioner to require the owner of a system of temporary cybersecurity concern to furnish information relating to the system of temporary cybersecurity concern.

The new section 17E empowers the Commissioner to issue a written direction to the owner of a system of temporary cybersecurity concern for the purpose of ensuring the cybersecurity of a system of temporary cybersecurity concern, or for the effective administration of the Act. A direction may relate to compliance with any prescribed technical or other standards relating to cybersecurity in respect of the system of temporary cybersecurity concern, or compliance with any code of practice or standard of performance applicable to the owner.

The new section 17F requires the owner of a system of temporary cybersecurity concern to notify the Commissioner of the occurrence of a prescribed cybersecurity incident in respect of a system of temporary cybersecurity concern or in respect of any computer or computer system under the owner's

control, or under the control of a supplier to the owner, that is interconnected with or that communicates with the system of temporary cybersecurity concern.

Clause 16 inserts a new Part 3C (comprising new sections 18 to 18F) which regulates entities of special cybersecurity interest in relation to the cybersecurity of systems of special cybersecurity interest.

Under the new section 18(1), the Commissioner may designate an entity as an entity of special cybersecurity interest on the basis that the entity stores sensitive information in a computer or computer system (or class of computers or computer systems) under the entity's control, or uses a computer or computer system (or class of computers or computer systems) under the entity's control to perform a function which, if disrupted, will have a significant detrimental effect on the defence, foreign relations, economy, public health, public safety or public order of Singapore (such a computer or computer system (or class of computers or computer systems) is referred to as a system of special cybersecurity interest).

The new section 18A empowers the Commissioner to require any entity whom the Commissioner has reason to believe may fulfil the criteria to be designated as an entity of special cybersecurity interest, to provide relevant information for the purpose of ascertaining whether the entity fulfils such criteria.

The new section 18B empowers the Commissioner to withdraw the designation of an entity of special cybersecurity interest at any time if the Commissioner is of the opinion that the entity no longer fulfils the criteria to be designated as such.

The new section 18C empowers the Commissioner to extend the designation of the entity of special cybersecurity interest if the Commissioner is of the opinion that the entity continues to fulfil the criteria to be designated as such.

The new section 18D empowers the Commissioner to require the entity of special cybersecurity interest to furnish information relating to the system of special cybersecurity interest.

The new section 18E empowers the Commissioner to issue a written direction to the entity of special cybersecurity interest for the purpose of ensuring the cybersecurity of the system of special cybersecurity interest, or for the effective administration of the Act. A direction may relate to compliance with any prescribed technical or other standards relating to cybersecurity in respect of the system of special cybersecurity interest, or compliance with any code of practice or standard of performance applicable to the entity.

The new section 18F requires the entity of special cybersecurity interest to notify the Commissioner of the occurrence of a prescribed cybersecurity incident in respect of the system of special cybersecurity interest or any other computer or computer system under the entity's control, where the incident results in a breach in the availability, confidentiality or integrity of the entity's data or has a significant impact on the business operations of the entity.

Clause 17 inserts a new Part 3D (comprising new sections 18G to 18M) which regulates major foundational digital infrastructure service providers in relation to the cybersecurity of computers or computer systems (or classes of computers or computer systems) that are necessary for the continuous delivery of foundational digital infrastructure services in relation to which major foundational digital infrastructure service providers are designated (such a computer or computer system (or class of computers or computer systems) is referred to as a major foundational digital infrastructure).

Under the new section 18G(1), the Commissioner may designate a provider of a foundational digital infrastructure service as a major foundational digital infrastructure service provider on the basis that a computer or computer system (or class of computers or computer systems) is necessary for the continuous delivery of a foundational digital infrastructure service by the provider, and the loss or impairment of the provision of that service is likely to lead to or cause disruption or deterioration of —

(*a*) where the service is provided from within or outside Singapore to persons in Singapore — the operation of a large number of businesses or organisations in Singapore which rely on or are enabled by that service; or

(*b*) where the service is provided wholly or partially from Singapore — the operation of a large number of businesses or organisations in or outside Singapore which rely on or are enabled by that service.

"Foundational digital infrastructure service" (new definition in section 2(1), inserted by clause 3(*d*)) means any service which promotes the availability, latency, throughput or security of digital services, and is specified in the Third Schedule. Clause 30 inserts a new Third Schedule, which lists (at paragraph 1) 2 foundational digital infrastructure services:

(*a*) cloud computing service, which can be delivered from a computer or computer system in or outside Singapore; and

(*b*) data centre facility service, which relies on a computer or computer system in Singapore encompassed within a facility in Singapore.

Paragraph 2 of the new Third Schedule contains the full definitions of these 2 services.

As section 18G(1) empowers the Commissioner to designate as a major foundational digital infrastructure service provider, a foundational digital infrastructure service provider that is located outside Singapore (provided the conditions mentioned in the new section 18G(1)(*b*) are met), the new section 18G(6) provides that a major foundational digital infrastructure service provider who is located outside Singapore must appoint a person in Singapore to accept service of notices or directions under the Act.

The new section 18H empowers the Commissioner to require any provider of a foundational digital infrastructure service which the Commissioner has reason to believe may fulfil the criteria to be designated as a major foundational digital infrastructure service provider, to provide relevant information for the purpose of ascertaining whether the provider fulfils such criteria.

The new section 18I empowers the Commissioner to withdraw the designation of a major foundational digital infrastructure service provider at any time if the Commissioner is of the opinion that the provider no longer fulfils the criteria to be designated as such.

The new section 18J empowers the Commissioner to extend the designation of the major foundational digital infrastructure service provider if the Commissioner is of the opinion that the provider continues to fulfil the criteria to be designated as such.

The new section 18K empowers the Commissioner to require the major foundational digital infrastructure service provider to furnish information relating to the major foundational digital infrastructure.

The new section 18L empowers the Commissioner to issue a written direction to the major foundational digital infrastructure service provider for the purpose of ensuring the cybersecurity of the major foundational digital infrastructure, or for the effective administration of the Act. A direction may relate to compliance with any prescribed technical or other standards relating to cybersecurity in respect of the major foundational digital infrastructure, or compliance with any code of practice or standard of performance applicable to the major foundational digital infrastructure service provider.

The new section 18M requires the major foundational digital infrastructure service provider to notify the Commissioner of the occurrence of a prescribed cybersecurity incident in respect of the major foundational digital infrastructure or any other computer or computer system under the major foundational digital infrastructure service provider's control, where the incident results in a disruption or degradation to the continuous delivery in Singapore of the foundational digital infrastructure service for which the provider is designated, or has a significant impact on the major foundational digital infrastructure service provider's business operations in Singapore.

Clause 18 inserts a new section 29A to provide monitoring powers for licensing officers in respect of licensed cybersecurity service providers.

Clause 19 inserts in Part 6, new sections 35A, 35B and 35C, which replace section 11 (codes of practice and standards of performance), section 17 (appeal to Minister) and section 18 (Appeals Advisory Panel), respectively. These new sections 35A, 35B and 35C are consolidated provisions on the subject matter that apply to Parts 3, 3A, 3B, 3C and 3D.

Clause 20 inserts new sections 37A and 37B which provide for civil penalty actions to be brought by the Commissioner where it appears to the Commissioner that there are contraventions of provisions in Part 3, 3A, 3B, 3C or 3D which are punishable as offences. Similar to sections 221, 232 and 233 of the Securities and Futures Act 2001, the new sections 37A and 37B provide that civil penalty actions may only be brought with the consent of the Public Prosecutor (new section 37A(1)), and as an alternative to prosecution (new section 37B(2), (3) and (4)). The new sections 37C and 37D contain similar provisions for an action for a civil penalty to be brought by the Commissioner against officers (or persons with similar roles) of the persons regulated under Parts 3, 3A, 3B, 3C and 3D, where such officers (or persons with similar roles) are at fault in the manner set out in the new section 37C(1)(*b*) in the commission of the contraventions.

Clause 21 amends section 40 to provide that a District Court has jurisdiction to hear and determine any action for a civil penalty to be imposed in respect of a contravention of a provision under Part 3, 3A, 3B, 3C or 3D regardless of the monetary amount of the civil penalty.

Clause 22 inserts a new section 41A which provides for the Commissioner to grant extensions of time for anything a person is required to do under Part 3, 3A, 3B, 3C or 3D (including any direction or order issued under those Parts).

Clause 23(*a*) introduces a new section 43(7)(*b*)(i*a*) which provides an additional exception to section 43(1) (preservation of secrecy) for the purposes of bringing an action to seek an order for a civil penalty under section 37A(1) or 37C(1), where the information is related to the contravention for which the civil penalty is sought.

Clauses 23(*b*) and 24 amend sections 43(10)(*c*) and 44(1), respectively, to replace the reference to the deleted section 18 with a reference to the new section 35C.

Clause 25 amends section 45(1) to apply it to witnesses in any proceedings for an offence under Part 3, 3A, 3B, 3C or 3D, or for a civil penalty under section 37A or 37C.

Clause 26 amends section 47(1) to include a reference to the new Third Schedule.

Clause 27 inserts a new section 47A which provides for Rules of Court to be made for the procedure and practice of civil penalty proceedings brought under the amended Act.

Clause 28(*a*) to (*f*) amends section 48(2) to include references to the new classes of regulated persons and terms related to them. Clause 28(*g*) inserts a new section 48(2)(*ia*) to specify that the Minister may make regulations with respect to the use of any accreditation, certification or inspection mark of the Cyber Security Agency of Singapore. Clause 28(*h*) provides that the regulation-making powers

conferred by section 48 do not extend to any matter for which Rules of Court may be made under new section 47A.

Clause 29 inserts new definitions in paragraph 2 of the Second Schedule providing that a computer and a computer system includes a virtual computer and a virtual computer system, respectively.

Clause 30 inserts a new Third Schedule, which lists (in paragraph 1) 2 foundational digital infrastructure services.

Clause 31(*a*), (*b*) and (*c*) makes miscellaneous amendments to replace various references in the Act to "critical information infrastructure" with references to "provider-owned critical information infrastructure".

Clause 32 contains saving and transitional provisions.

Clause 32(1) deems any Assistant Commissioner appointed in respect of a CII under section 4(1)(*b*) read with section 4(2) as in force immediately before the date of commencement of clause 5(*a*) to be appointed in respect of a provider-owned CII under section 4(1)(*b*) read with section 4(2) as replaced by clause 5(*a*).

Clause 32(2), (3) and (4) provides for saving and transitional provisions relating to the replacement of sections 11, 17 and 18 by the new sections 35A, 35B and 35C.

Clause 32(5) contains a transitional provision for the application of the new sections 37A and 37C.

Clause 32(6) deems any notice of designation of a CII issued under section 7 before the date of commencement of clause 31 to be a notice of designation of a provider-owned CII issued under section 7 as amended by clause 31.

Clause 32(7) confers on the Minister the power to make regulations of a saving or transitional nature, in the 2 years after the date of commencement of any provision of the Bill.

EXPENDITURE OF PUBLIC MONEY

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