THIS DRAFT BILL IS FOR PUBLIC CONSULTATION ONLY.

Cybersecurity (Amendment) Bill 2023

Bill No. /2023.

Read the first time on *2023.*

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:

PART 1

PRELIMINARY

Short title and commencement

1. This Act is the Cybersecurity (Amendment) Act 2023 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, after "owners of", insert "provider-owned critical information infrastructure, major foundational digital infrastructure service providers, entities of special cybersecurity interest and owners of systems of temporary cybersecurity concern, to regulate providers of essential service responsible for the cybersecurity of non-provider-owned critical information infrastructure,".

Amendment of section 2

3. In the principal Act, in section 2(1) —

(*a*) delete the definition of "critical information infrastructure";

(*b*) 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;

(*c*) 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 for which it is designated.

"non-provider-owned critical information infrastructure" means a computer or computer system in relation to which a designation of a provider responsible for non-provider-owned critical information infrastructure under section 18AA(2) is in effect;

(*d*) replace the definition of "owner" with —

"owner", in relation to a provider-owned critical information infrastructure or system of temporary cybersecurity concern, means the legal owner of the provider-owned critical information infrastructure or system of temporary cybersecurity concern (as the case may be) and, where the provider-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) is in effect;

"provider responsible for non-provider-owned critical information infrastructure" means a provider of an essential service that is responsible for the cybersecurity of a non-provider-owned critical information infrastructure as designated under section 18AA(2); and

(*e*) 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) used by an entity

of special cybersecurity interest 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.".

Amendment of section 4

4. 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 provider responsible for non-provider-owned critical information infrastructure, a major foundational digital infrastructure service provider, or an entity of special cybersecurity interest —

(*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 provider responsible for non-provider-owned critical information infrastructure, major foundational digital infrastructure service provider, or entity of special cybersecurity interest (as the case may be) belongs.";

(*b*) in subsection (5), replace "section 7 or 9" with "section 7, 9, 18AA, 18AC, 18BB, 18BD, 18CB, 18CD, 18DB or 18DD";

(*c*) in subsection (6), in paragraph (*a*), replace "9" with "9, 18AA, 18AC, 18BB, 18BD, 18CB, 18CD, 18DB, 18DD"; and

(*d*) in subsection (6), in paragraph (*b*), replace "6, 7, 9, 11, 12" with "6, 6A, 7, 9, 11, 12, 18AA, 18AC, 18BB, 18BD, 18CB, 18CD, 18DB, 18DD".

Amendment of section 5

5. In the principal Act —

(*a*) renumber section 5 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 providers responsible for non-provider-owned critical information infrastructure, major foundational digital infrastructure service providers or entities of special cybersecurity interest, and to regulate providers responsible for non-provider-owned critical information infrastructure, major

foundational digital infrastructure service providers or entities of special cybersecurity interest with regard to the cybersecurity of the non-provider-owned critical information infrastructure, the major foundational digital infrastructure or the system of special cybersecurity interest;"

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

(*d*) after subsection (1), insert —

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

New section 6A

6. 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

with 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

7. 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 subsection (2), after "subsection (1)", insert "or (1A)";

(*c*) in subsection (3), after "subsection (1)", insert "or (1A)";

(*d*) in subsection (4), after "subsection (1)", insert "or (1A)";

(*e*) in subsection (5), after "subsection (1)", insert "or (1A)".

New section 9A

8. 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 of 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.".

Amendment of section 14

9. 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

10. In the principal Act, in section 15, 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, 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 or an applicable code of practice or standard of performance, or 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.".

New section 16A

11. In the principal Act, after section 16, insert —

"**Extension of time**

16A.—(1) A person that, in any particular case, is unable to do any thing that the person is required to do under this Part 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 17

12. In the principal Act, in section 17(1), after paragraph (*a*), insert —

"(*aa*) the decision of the Commissioner to issue the notice under section 9A(1) extending the designation of the provider-owned critical information infrastructure as such;".

New Part 3A

13. In the principal Act, after Part 3, insert —

"PART 3A

PROVIDER OF ESSENTIAL SERVICE RESPONSIBLE FOR CYBERSECURITY OF NON-PROVIDER-OWNED CRITICAL INFORMATION INFRASTRUCTURE

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

18AA.—(1) This Part does not apply to any provider of an essential service in relation to any computer or computer system for which a designation under section 7 is in effect.

(2) The Commissioner may, by written notice to a provider of an essential service, designate the provider as a provider of essential service responsible for the cybersecurity of non-provider-owned critical information infrastructure for the purposes of this Part if the Commissioner is satisfied that —

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

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

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

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

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

(*d*) inform the provider responsible for non-provider-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 provider responsible for non-provider-owned critical information infrastructure in relation to the non-provider-owned critical information infrastructure;

(*f*) inform the provider responsible for non-provider-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 provider responsible for non-provider-owned critical information infrastructure that the provider may appeal to the Minister against the designation, and provide information on the applicable procedure.

(4) Any designation under subsection (2) has effect for a period of 5 years, unless it is withdrawn by the Commissioner before the expiry of the period.

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

Power to obtain information to ascertain criteria in section 18AA(2)

18AB.—(1) This section applies where the Commissioner has reason to believe that a computer or computer system may fulfil the criteria in section 18AA(2).

(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 18AA(2).

(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 18AA(2).

(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 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 provider responsible for non-provider-owned critical information infrastructure

18AC. The Commissioner may, by written notice, withdraw the designation of any provider responsible for non-provider-owned critical information infrastructure at any time if the Commissioner is of the opinion that the criteria in section 18AA(2) is no longer fulfilled.

Extension of designation of provider responsible for non-provider-owned critical information infrastructure

18AD.—(1) At any time before the expiry of the designation of a provider responsible for non-provider-owned critical information infrastructure, the Commissioner may, by written notice, extend the designation of the provider responsible for non-provider-owned critical information infrastructure, if the Commissioner is of the opinion that the criteria in section 18AA(2) continues to be fulfilled.

(2) Any extension of 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 non-provider-owned critical information infrastructure

18AE.—(1) A provider responsible for non-provider-owned critical information infrastructure must obtain a legally binding commitment from the owner of the non-provider-owned critical information infrastructure for which the provider is responsible for its cybersecurity, that the owner of the non-provider-owned critical information infrastructure will —

(*a*) upon the request of the provider responsible for non-provider-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 non-provider-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 non-provider-owned critical information infrastructure;

(iii) information relating to the operation of the non-provider-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 non-provider-owned critical information infrastructure;

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

(*b*) notify the provider responsible for non-provider-owned critical information infrastructure when a material change is made by or on behalf of the owner of the non-provider-owned critical information infrastructure to the design, configuration, security or operation of the non-provider-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) below.

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

(3) Any provider responsible for non-provider-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 provider responsible for non-provider-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 non-provider-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 non-provider-owned critical information infrastructure;

(*c*) information relating to the operation of the non-provider-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 non-provider-owned critical information infrastructure;

(*d*) any other information relating to the non-provider-owned critical information infrastructure that the Commissioner may require in order to ascertain the level of cybersecurity of the non-provider-owned critical information infrastructure.

(5) Any provider responsible for non-provider-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 provider responsible for non-provider-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 provider responsible for non-provider-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 non-provider-owned critical information infrastructure to the design, configuration, security or operation of the non-provider-owned critical information infrastructure after any information has been furnished to the Commissioner pursuant to a notice mentioned in subsection (4), the provider responsible for non-provider-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 non-provider-owned critical information infrastructure, or the ability of the owner of the non-provider-owned critical information infrastructure or the provider responsible for non-provider-owned critical information infrastructure, to respond to a cybersecurity threat or incident affecting the non-provider-owned critical information infrastructure.

(10) Any provider responsible for non-provider-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.

Codes of practice and standards of performance

18AF.—(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 providers responsible for non-provider-owned critical information infrastructure with respect to measures to be taken by them to ensure the cybersecurity of the non-provider-owned critical information infrastructure for which they are responsible;

(*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 provider responsible for non-provider-owned critical information infrastructure to which that code or standard applies.

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

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

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

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

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

(6) Subject to subsections (4) and (7), every provider responsible for non-provider-owned critical information infrastructure must comply with the codes of practice and standards of performance that apply to the provider.

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

Power of Commissioner to issue written directions

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

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

(*d*) any other matters that the Commissioner may consider necessary or expedient to ensure the cybersecurity of the non-provider-owned critical information infrastructure.

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

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

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

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

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

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

Change in ownership of non-provider-owned critical information infrastructure

18AH.—(1) A provider responsible for non-provider-owned critical information infrastructure must obtain a legally binding commitment from the owner of the non-provider-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 non-provider-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 provider responsible for non-provider-owned critical information infrastructure to cease using, directly or indirectly, the non-provider-owned critical information infrastructure for which it is responsible for the cybersecurity.

(3) Any provider responsible for non-provider-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 non-provider-owned critical information infrastructure, the provider responsible for non-provider-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 18AA(2) are no longer fulfilled, the provider responsible for non-provider-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 non-provider-owned critical information infrastructure, etc.

18AI.—(1) A provider responsible for non-provider-owned critical information infrastructure must obtain a legally binding commitment from the owner of the non-provider-owned critical information infrastructure for which the provider is responsible for its cybersecurity, that the owner of the non-provider-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 non-provider-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 non-provider-owned critical information infrastructure;

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

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

(3) Any provider responsible for non-provider-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 provider responsible for non-provider-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 non-provider-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 non-provider-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 non-provider-owned critical information infrastructure that the Commissioner has specified by written direction to the provider responsible for non-provider-owned critical information infrastructure.

(5) The provider responsible for non-provider-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 non-provider-owned critical information infrastructure, as set out any applicable code of practice.

(6) Any provider responsible for non-provider-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 non-provider-owned critical information infrastructure

18AJ.—(1) A provider responsible for non-provider-owned critical information infrastructure must obtain a legally binding commitment from the owner of the non-provider-owned critical information infrastructure for which the provider is responsible for its cybersecurity, that the owner of the non-provider-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 18AA(2), cause an audit of the adherence of the non-provider-owned critical information infrastructure with reference to the applicable codes of practice and standards of performance, 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 18AA(2), conduct a cybersecurity risk assessment of the non-provider-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 non-provider-owned critical information infrastructure to be carried out by an auditor approved by the Commissioner, as required by the provider pursuant to an order from the Commissioner under subsection (7);

(*f*) carry out further steps to evaluate the level of cybersecurity of the non-provider-owned critical information infrastructure, or cause another cybersecurity risk assessment of the non-provider-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 paragraph (*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 provider responsible for non-provider-owned critical information infrastructure to cease using, directly or indirectly, the non-provider-owned critical information infrastructure for which it is responsible for the cybersecurity.

(3) Any provider responsible for non-provider-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 provider responsible for non-provider-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 provider responsible for non-provider-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 provider responsible for non-provider-owned critical information infrastructure to require the owner of the non-provider-owned critical information infrastructure to carry out that aspect of the audit again.

(7) Where it appears to the Commissioner that —

(*a*) the non-provider-owned critical information infrastructure is not in conformity with reference to an applicable code of practice or standard of performance; or

(*b*) any information furnished by the provider responsible for non-provider-owned critical information infrastructure under section 18AE is false, misleading, inaccurate, or incomplete,

the Commissioner may for the purpose of ascertaining the non-provider-owned critical information infrastructure's conformity with reference to an applicable code of practice or standard of performance, or the accuracy or completeness of the information (as the case may be), by order direct the provider to require the owner of the non-provider-owned critical information infrastructure to cause an audit in respect of the non-provider-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 (6), that the assessment was not carried out satisfactorily, the

Commissioner may direct the provider responsible for non-provider-owned critical information infrastructure to require the owner of the non-provider-owned critical information infrastructure to either —

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

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

(9) Where the provider responsible for non-provider-owned critical information infrastructure has notified the Commissioner under section 18AE(8) of a material change made to the design, configuration, security or operation of the non-provider-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 non-provider-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 provider responsible for non-provider-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 or order 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 provider responsible for non-provider-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

18AK.—(1) If a material change is made to a legally binding commitment that was obtained by a provider responsible for non-provider-owned critical information infrastructure for the purpose of meeting a requirement under section 18AE(1), 18AH(1), 18AI(1) or 18AJ(1), the provider responsible for non-provider-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 provider responsible for non-provider-owned critical information infrastructure to obtain the performance, by the owner of the non-provider-owned critical information infrastructure, of the actions committed in accordance with the legally binding commitment.

(3) Any provider responsible for non-provider-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

18AL.—(1) The Commissioner may conduct cybersecurity exercises for the purpose of testing the state of readiness of providers responsible for different non-provider-owned critical information infrastructure in responding to significant cybersecurity incidents.

(2) A provider responsible for non-provider-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.

Appeal to Minister

18AM.—(1) The provider responsible for non-provider-owned critical information infrastructure who is aggrieved by —

(*a*) the decision of the Commissioner to issue the notice under section 18AA(2) designating the provider as such;

(*b*) the decision of the Commissioner to issue the notice under section 18AD(1) extending the designation of the provider as such;

(*c*) an order of the Commissioner under section 18AB(5), 18AE(2), 18AH(2), 18AI(2) or 18AJ(2);

(*d*) a written direction of the Commissioner under section 18AG or 18AL(2); or

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

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

(2) An appeal under subsection (1) must be made within 30 days after the date of the notice, 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).

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

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

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

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

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

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

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

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

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

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

(*a*) by confirming, varying or reversing a decision, notice, 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.

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

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

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

Appeals Advisory Panel

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

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

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

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

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

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

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

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

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

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

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

New Part 3B

14. In the principal Act, after Part 3A, insert —

"PART 3B

MAJOR FOUNDATIONAL DIGITAL INFRASTRUCTURE SERVICE

Application and interpretation of this Part

18BA.—(1) This Part does not apply to any provider of a foundational digital infrastructure service in relation to any computer or computer system for which a designation under section 7 or 18AA is in effect.

(2) In this Part, unless the context otherwise requires —

"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;

"foundational digital infrastructure" means the computer or computer system (or class of computers or computer systems) that are necessary for the continuous delivery of a foundational digital infrastructure service;

Designation of major foundational digital infrastructure service provider

18BB.—(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 Part, 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) to one or more persons in Singapore, and the loss or impairment of the provision of that foundational digital infrastructure service will lead to or cause disruption to 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 will lead to or cause disruption to 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 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;

(*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 major foundational digital infrastructure service provider may appoint a person in Singapore to accept service of notices or directions under this Act.

(6) In this section —

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

(i) from 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 which is incorporated under any written law, or is 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

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

(4) [See note at end of Part 3B for considerations in relation to penalties to be imposed on major foundational digital infrastructure service providers which fail to comply with subsection (2).]

(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 a major foundational digital infrastructure service provider

18BD. 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 criteria in section 18BB(1) are no longer fulfilled.

Extension of designation of a major foundational digital infrastructure service provider

18BE.—(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 criteria in section 18BB(1) continue to be fulfilled.

(2) Any extension of a designation under section 18BB(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 a major foundational digital infrastructure service provider

18BF.—(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) [See note at end of Part 3B for considerations in relation to penalties to be imposed on major foundational digital infrastructure service providers which fail to comply with subsection (1).]

(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).

Codes of practice and standards of performance

18BG.—(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 major foundational digital infrastructure service providers with respect to measures to be taken by them to ensure the cybersecurity of the major foundational digital infrastructure; or

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

(2) If any provision in any code of practice or standard of performance is inconsistent with this Act, 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 the major foundational digital infrastructure service provider to which that code or standard applies.

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

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

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

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

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

(6) Subject to subsections (4) and (7), every major foundational digital infrastructure service provider must comply with the codes of practice and standards of performance that apply to the major foundational digital infrastructure.

(7) The Commissioner may, either generally or for such time as the Commissioner may specify, waive the application to the major foundational digital infrastructure service provider of any code of practice or standard of performance, or any part of it.

Power of Commissioner to issue written directions

18BH.—(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 code of practice or standard of performance applicable to the provider;

(*c*) 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

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

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

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

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

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

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

(6) [See note at end of Part 3B for considerations in relation to penalties to be imposed on major foundational digital infrastructure service providers which fail to comply with subsection (1).]

Duty to report cybersecurity incident in respect of major foundational digital infrastructure service provider, etc.

18BI.—(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 any 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 any 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) [See note at end of Part 3B for considerations in relation to penalties to be imposed on major foundational digital infrastructure service providers which fail to comply with subsection (1).]

Appeal to Minister

18BJ.—(1) The major foundational digital infrastructure service provider who is aggrieved by —

(*a*) the decision of the Commissioner to issue the notice under section 18BB(1) designating the major foundational digital infrastructure service provider as such;

(*b*) the decision of the Commissioner to issue the notice under section 18BE(1) extending the designation of the provider as such;

(*c*) a written direction of the Commissioner under section 18BH; or

(*d*) any provision in any code of practice or standard of performance issued or approved by the Commissioner

that applies to the provider, or any amendment made to it,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Appeals Advisory Panel

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

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

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

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

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

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

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

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

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

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

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

Note: CSA's policy intent is to prescribe financial penalties that are (a) commensurate with the risks resulting from non-compliance; and (b) an effective deterrent effect against non-compliance. CSA is studying comparable laws in other jurisdictions that purport to regulate companies that would likely qualify as major foundational digital infrastructure service providers, as well as comparable statutes under Singapore law, and will set out the proposed penalty provisions in a future version of the Bill.

New Part 3C

15. In the principal Act, after Part 3B, insert —

"PART 3C

ENTITIES OF SPECIAL CYBERSECURITY INTEREST

Application and interpretation of this Part

18CA.—(1) This Part does not apply to any entity in relation to any computer or computer system for which a designation under section 7 or 18AA is in effect.

(2) In this Part —

"entity" means —

(*a*) a body corporate (including a limited liability partnership);

(*b*) an unincorporated association;

(*c*) a partnership; or

(*d*) a person other than an individual;

Designation of entity of special cybersecurity interest

18CB.—(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 stores sensitive information in a computer or computer system (or class of computers or computer systems), or the entity uses a 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; and

(*b*) the entity is incorporated 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, "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

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

(3) Without limiting subsection (2), for the purpose of ascertaining whether an entity fulfils the criteria of 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 of an entity of special cybersecurity interest.

(4) [See note at end of Part 3C for considerations in relation to penalties to be imposed on entities of special cybersecurity interest which fail to comply with subsection (2).]

(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 an entity of special cybersecurity interest

18CD. 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 criteria in section 18CB(1) is no longer fulfilled.

Extension of designation of an entity of special cybersecurity interest

18CE.—(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 criteria in section 18CB(1) continues to be fulfilled.

(2) Any extension of a designation under section 18CB(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 an entity of special cybersecurity interest

18CF.—(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) [See note at end of Part 3C for considerations in relation to penalties to be imposed on entities of special cybersecurity interest which fail to comply with subsection (1).]

(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).

Codes of practice and standards of performance

18CG.—(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 entities of special cybersecurity interest with respect to measures to be taken by them to ensure the

cybersecurity of the system of special cybersecurity interest; or

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

(2) If any provision in any code of practice or standard of performance is inconsistent with this Act, 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 the entity of special cybersecurity interest to which that code or standard applies.

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

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

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

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

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

(6) Subject to subsections (4) and (7), every entity of special cybersecurity interest must comply with the codes of practice

and standards of performance that apply to the system of special cybersecurity interest.

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

Power of Commissioner to issue written directions

18CH.—(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 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 code of practice or standard of performance applicable to the entity;

(*c*) 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

(*d*) any other matters 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) may be revoked at any time by the Commissioner.

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

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

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

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

(6) [See note at end of Part 3C for considerations in relation to penalties to be imposed on entities of special cybersecurity interest which fail to comply with subsection (1).]

Duty to report cybersecurity incident in respect of entity of special cybersecurity interest, etc.

18CI.—(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 any 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 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) [See note at end of Part 3C for considerations in relation to penalties to be imposed on entities of special cybersecurity interest which fail to comply with subsection (1).]

Appeal to Minister

18CJ.—(1) The entity of special cybersecurity interest who is aggrieved by —

(*a*) the decision of the Commissioner to issue the notice under section 18CB(1) designating the entity of special cybersecurity interest as such;

(*b*) the decision of the Commissioner to issue the notice under section 18CE(1) extending the designation of the entity as such;

(*c*) a written direction of the Commissioner under section 18CH; or

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Appeals Advisory Panel

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

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

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

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

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

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

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

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

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

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

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

Note: CSA's policy intent is to prescribe financial penalties that are (a) commensurate with the risks resulting from non-compliance; and (b) an effective deterrent effect against non-compliance. CSA is studying comparable laws in other jurisdictions that purport to regulate companies that would likely qualify as entities of special cybersecurity interest, as well as comparable statutes under Singapore law, and will set out the proposed penalty provisions in a future version of the Bill.

New Part 3D

16. In the principal Act, after Part 3C, insert —

"PART 3D

SYSTEM OF TEMPORARY CYBERSECURITY CONCERN

Application of this Part

18DA. This Part does not apply to any computer or computer system for which a designation under section 7 or 18AA is in effect.

Designation of system of temporary cybersecurity concern

18DB.—(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 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;

(*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;

(*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

18DC.—(1) This section applies where the Commissioner has reason to believe that a computer or computer system may fulfil the criteria of 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 of 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 of 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 of 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 a system of temporary cybersecurity concern

18DD. 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 criteria in section 18DB(1) is no longer fulfilled.

Extension of designation of a system of temporary cybersecurity concern

18DE.—(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 criteria in section 18DB(1) continues to be fulfilled.

(2) Any extension of a designation under s18DB(1) has effect for the period stated in the notice in subsection (1) (which must not exceed 1 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 a system of temporary cybersecurity concern

18DF.—(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).

Codes of practice and standards of performance

18DG.—(1) The Commissioner may, from time to time —

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

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

(2) If any provision in any code of practice or standard of performance is inconsistent with this Act, 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 the owner of a system of temporary cybersecurity concern to which that code or standard applies.

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

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

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

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

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

(6) Subject to subsections (4) and (7), every owner of a system of temporary cybersecurity concern must comply with the codes of practice and standards of performance that apply to the system of temporary cybersecurity concern.

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

Power of Commissioner to issue written directions

18DH.—(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 code of practice or standard of performance applicable to the owner;

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

(*d*) any other matters 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) may be revoked at any time by the Commissioner.

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

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

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

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

(6) Any person who, without reasonable excuse, fails to comply with a direction under subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000

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

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

18DI.—(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.

Appeal to Minister

18DJ.—(1) The owner of a system of temporary cybersecurity concern who is aggrieved by —

(*a*) the decision of the Commissioner to issue the notice under section 18DB(1) designating the system of temporary cybersecurity concern as such;

(*b*) the decision of the Commissioner to issue the notice under section 18DE(1) extending the designation of the system of temporary cybersecurity concern as such;

(*c*) a written direction of the Commissioner under section 18DH; or

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Appeals Advisory Panel

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

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

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

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

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

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

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

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

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

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

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

New section 29A

17. 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 such 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 such records, accounts and documents as are mentioned in subsection (1) are kept in electronic form, then —

(*a*) the power of the licensing officer in subsection (1)(*b*) to require any such records, accounts or documents to be produced for inspection includes 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 such records, accounts or documents includes power to require any person on the premises in question to give him or her 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) A 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.".

Amendment of section 48

18. In the principal Act, in section 48(2) —

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

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

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

(*d*) replace paragraph (*e*) with —

"(*e*) the type of cybersecurity incidents in respect of a provider-owned critical information infrastructure, major foundational digital infrastructure, system of special cybersecurity interest, system of temporary cybersecurity concern or non-provider-owned critical information infrastructure that are required to be reported by the owner of the provider-owned critical information infrastructure or system of temporary cybersecurity concern, provider responsible for non-provider-owned critical information infrastructure, major foundational digital infrastructure service provider or entity of special cybersecurity interest;";

(*e*) in paragraph (*f*), replace "critical information infrastructure" with "provider-owned critical information infrastructure or the owner of a non-provider-owned critical information infrastructure"; and

(*f*) after paragraph (*i*), insert —

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

New Third Schedule

19. In the principal Act, after the second Schedule, insert —

"THIRD SCHEDULE

Section 18BA(2)

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 that other person's 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

20. In the principal Act —

(*a*) in the following sections, replace "critical information infrastructure" in every case with "provider-owned critical information infrastructure":

Sections 3(1), 7(1), (2)(a), (b) and (d), (6), (7) and (8), 8(1), (2) and (3)(c), 9, 10(1), (2), (3), (4), (5), (6) and (7), 11(1)(a), (3)(c), (6) and (7), 12(1) and (2)(d), 13(1) and (3)(a) and (b), 14(1), (2) and (3), 15(1), (2), (3), (5)(a) and (b), (6), (7) and (8), 16(1) and (2), 17(1), 20(3);

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

(*c*) in the section headings of the following sections, insert "provider-owned" before "critical":

Sections 7, 8, 9, 10, 13, 14, 15.