CYBERSECURITY ACT

EXPLANATORY STATEMENT

Explanations of each Part and Section of the Cybersecurity Act

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

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

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

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

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

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

Part 6 contains general provisions.

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

PART 1

PRELIMINARY

Section 1 relates to the short title and commencement.

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

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

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

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

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

PART 2

ADMINISTRATION

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

The Commissioner may appoint public officers as cybersecurity officers.

The Commissioner is responsible for the administration of the Act.

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

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

PART 3

CRITICAL INFORMATION INFRASTRUCTURE

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

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

The person who receives a notice of designation may request the Commissioner to amend the notice by addressing it to another person who has effective control of the CII (controller), by showing proof that the person who received the notice is not able to comply with the requirements in Part 3 because that person has neither effective control over the CII's operations nor the ability or right to carry out changes to the CII, whilst the controller has both. If the Commissioner addresses and sends

an amended notice to the controller, the controller will be subject to all the requirements under Part 3 during the period when the notice is in effect, as if the controller were the owner.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PART 4

RESPONSES TO CYBERSECURITY THREATS AND INCIDENTS

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

Section 19 empowers the Commissioner to exercise or authorise the exercise by an incident response officer of information and record gathering powers as necessary to investigate a cybersecurity threat or incident for the purpose of assessing its impact, preventing harm arising from the cybersecurity incident or preventing a further cybersecurity incident from arising. The powers which are to be exercised against persons affected by the cybersecurity threat or incident, typically the victims, are the following:

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

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

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

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

Section 19(6) provides that any person examined or who receives a notice under Section 19(2) or an order of a Magistrate under Section 19(5) is not obliged to disclose any information that is subject to any right, privilege or immunity conferred, or obligation or limitation imposed, by or under any law or rules of professional

conduct in relation to the disclosure of such information, except that the performance of a contractual obligation is not an excuse for not disclosing the information. For example, the person is not obliged to produce to the incident response officer an email infected by a malicious program if that email contains information that is subject to legal privilege. However, the person is not entitled to withhold an infected email that is subject to a contractual obligation of confidentiality, and the person is not treated as in breach of that contractual obligation if the person produces that email with reasonable care and in good faith for the purpose of complying with a requirement made under Section 19.

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

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

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

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

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

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

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

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

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

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

(ii) monitoring the affected computer or computer system;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Section 23 re-enacts with slight modifications section 15A of the Computer Misuse and Cybersecurity Act (Cap. 50A), which will be repealed by Section 49. Section 23 empowers the Minister to authorise or direct any person or organisation to take emergency cybersecurity measures and comply with necessary requirements, for the

purposes of preventing, detecting or countering any serious and imminent threat to the provision of any essential service, or to the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore.

PART 5

CYBERSECURITY SERVICE PROVIDERS

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

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

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

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

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

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

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

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

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

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

Section 30 empowers the licensing officer to revoke or suspend a licence, censure the licensee or impose other conditions on the licensee, if prescribed conditions are satisfied and after giving the licensee an opportunity to be heard. An order of revocation or suspension takes effect at the end of 14 days after service of the notice of the order, unless the licensing officer states in the order that it is undesirable in the public interest for the licensee to continue to carry on the licensee's business as a licensee, in which case the order takes effect immediately upon service of the notice of the order.

Section 31 provides that a provider of a licensable cybersecurity service is not entitled to bring any proceeding to recover any commission, fee, gain or reward unless the provider held a valid licence at the time of providing the service.

Section 32 provides that a licensing officer may, in addition to or instead of taking action under Section 30(1) or (2), order a licensee to pay a financial penalty for a contravention of a provision of Part 5 that is not an offence or for failure to comply with a licence condition.

Section 33 relates to the process that must be observed by the licensing officer before making an order for a licensee to pay any financial penalty. The licensee may make representations before the date on which the order is intended to be made.

Section 34 provides for the recovery of any financial penalty as a debt due to the Government. The licensing officer is empowered to waive, remit or refund in whole or in part any financial penalty imposed, or any interest due on any financial penalty.

Section 35 provides for an avenue of appeal to the Minister against decisions made by the licensing officer.

PART 6

GENERAL

Sections 36 and 37 are standard provisions for the liability of officers of offenders which are corporations or unincorporated bodies like partnerships and associations.

Section 38 confers various powers for investigating an offence under the Act (except an offence under Section 23).

Section 39 allows an investigation officer to enter premises under a Magistrate's warrant, for the purposes of an investigation under Section 38.

Section 40 confers jurisdiction on a District Court to try any offence under the Act and to impose the full punishment for any such offence.

Section 41 provides powers of composition that may be exercised by the Commissioner or any Assistant Commissioner authorised by the Commissioner.

Section 42 deals with the service of documents permitted or required by the Act to be served on a person. The Section does not deal with service of court documents, as these are regulated by other written laws.

Section 43 is a confidentiality provision which provides that a person who is or has been the Commissioner, the Deputy Commissioner, an Assistant Commissioner, a cybersecurity officer, an authorised officer, a member of an Appeals Advisory Panel, a cybersecurity technical expert or an assistant licensing officer, or the Minister or a person assisting the Minister, must not disclose certain information which has come to the person's knowledge in the performance of his or her functions, or the discharge of his or her duties, under the Act, except in the circumstances specified in the Section.

Section 44(1) is a standard provision providing immunity from suits for any act of the Commissioner, the Deputy Commissioner, an Assistant Commissioner, a cybersecurity officer, an authorised officer, an assistant licensing officer, a member of an Appeals Advisory Panel or any other person acting under the direction of the Commissioner, who, acting in good faith and with reasonable care, does or omits to do anything in the exercise or purported exercise of any power under the Act or the performance or purported performance of any function or duty under the Act.

Section 44(2) confers upon the Commissioner, and any person acting under the Commissioner's direction, protection from liability for any error or omission appearing in any information supplied to the public under a service pursuant to any written law, if made in good faith and despite the exercise of reasonable care in the discharge of the duties of the Commissioner or such person.

Section 45 relates to the protection of the identity of informers of offences under Part 3.

Section 46 confers on the Minister power to exempt, by order in the *Gazette*, any person or any class of persons from all or any of the provisions of the Act.

Section 47 empowers the Minister to amend the First or Second Schedule by order in the *Gazette*, and to make transitional, incidental, consequential or supplementary provision as necessary or expedient.

Section 48 confers on the Minister the power to make regulations for the purposes of the Act.

Section 49 provides for related amendments to the Computer Misuse and Cybersecurity Act.

Section 50 provides for consequential amendments to certain Acts.

Section 51 contains saving and transitional provisions. The Section also confers on the Minister the power to make regulations of a saving or transitional nature, in the 2 years after the date of commencement of any provision of the Act.

The First Schedule sets out a list of essential services.

The Second Schedule sets out the licensable cybersecurity services for the purposes of the Act. Two cybersecurity services — managed security operations centre (SOC) monitoring service and penetration testing service — are prescribed as licensable cybersecurity services.