First published in the Government *Gazette*, Electronic Edition, on 30 August 2018 at 5 pm.

**No. S 519**

# CYBERSECURITY ACT 2018
# (ACT 9 OF 2018)

# CYBERSECURITY (PROVIDER-OWNED CRITICAL INFORMATION INFRASTRUCTURE) REGULATIONS 2018

ARRANGEMENT OF REGULATIONS

PART 1

PRELIMINARY



In exercise of the powers conferred by sections 17(10) and 48 of the Cybersecurity Act 2018, Mr S Iswaran, who is charged with the responsibility for the portfolio of the Prime Minister as regards cybersecurity, makes the following Regulations:

PART 1

PRELIMINARY

## Citation and commencement

**1.** These Regulations are the Cybersecurity (Provider-Owned Critical Information Infrastructure) Regulations 2018 and come into operation on 31 August 2018.

*[S 678/2025 wef 31/10/2025]*

## Definitions

**2.** In these Regulations, unless the context otherwise requires —

[*Deleted by S 678/2025 wef 31/10/2025*]

[*Deleted by S 678/2025 wef 31/10/2025*]

"owner-controlled interconnected computer or computer system" means any computer or computer system under the control of the owner of a provider-owned critical information infrastructure, that is interconnected with or that communicates with the provider-owned critical information infrastructure;

*[S 678/2025 wef 31/10/2025]*

"owner-controlled non-interconnected computer or computer system" means any computer or computer system under the control of the owner of a provider-owned critical information infrastructure, that is not the provider-owned critical information infrastructure or an owner-controlled interconnected computer or computer system;

*[S 678/2025 wef 31/10/2025]*

"relevant computer or computer system" means —

(*a*) a provider-owned critical information infrastructure;

(*b*) an owner-controlled interconnected computer or computer system;

(*c*) an owner-controlled non-interconnected computer or computer system; or

(*d*) a supplier-controlled interconnected computer or computer system;

*[S 678/2025 wef 31/10/2025]*

"supplier-controlled interconnected computer or computer system" means any computer or computer system under the control of a supplier to the owner of a provider-owned critical information infrastructure, that is interconnected with or that communicates with the provider-owned critical information infrastructure;

*[S 678/2025 wef 31/10/2025]*

"working day" means any day except a Saturday, Sunday or public holiday.

## PART 2

## PROVIDING INFORMATION TO COMMISSIONER

### Information to ascertain if computer, etc., fulfils criteria of provider-owned critical information infrastructure

**3.**—(1) For the purposes of subsection 2 of section 8 of the Act, a notice to provide relevant information to the Commissioner under that subsection must be given in writing in the form set out on the Internet website at https://www.csa.gov.sg.

(2) The Commissioner may by notice under section 8(2) of the Act require a person who appears to be exercising control over a computer or computer system, to provide to the Commissioner the following information relating to that computer or computer system as is relevant for the purpose of ascertaining whether the computer or computer system fulfils the criteria of a provider-owned critical information infrastructure:

(*a*) name and location of the computer or computer system;

(*b*) the function that the computer or computer system is employed to serve;

(*c*) the type of essential service, if applicable, that the computer or computer system has a role in making

available in Singapore, and the role performed by the computer or computer system;

(*d*) the person or persons, or other computer or computer systems, that the computer or computer system mentioned in the notice serves;

(*e*) information relating to the design of the computer or computer system, including the parameters and key components of the computer system, as specified in the notice;

(*ea*) if the computer or computer system is a virtual computer or virtual computer system, information relating to the physical computing resources used for the simulation of the virtual computer or virtual computer system, including identifying information relating to the cloud computing service provider where the physical computing resources used for the simulation of the virtual computer or virtual computer system are provided by a cloud computing service provider;

*[S 678/2025 wef 31/10/2025]*

(*f*) the name, address, contact and business registration number (if applicable) of the person to whom the notice is given;

(*g*) if the person to whom the notice is given is not the owner of the computer or computer system, the name, address, contact and business registration number (if applicable) of the owner;

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

*[S 678/2025 wef 31/10/2025]*

(3) In this regulation, "location", in relation to a computer or computer system that is a virtual computer or virtual computer system, means the location of the physical computing resources

deployed for the simulation of the virtual computer or virtual computer system.

*[S 678/2025 wef 31/10/2025]*

*[S 678/2025 wef 31/10/2025]*

**Information relating to provider-owned critical information infrastructure**

**4.**—(1) For the purposes of subsection (1) of section 10 of the Act, a notice to the owner of a provider-owned critical information infrastructure to furnish information required under that subsection must be given in writing in the form set out on the Internet website at https://www.csa.gov.sg.

*[S 678/2025 wef 31/10/2025]*

(2) The Commissioner may by notice under section 10(1) of the Act require the owner of the provider-owned critical information infrastructure to provide to the Commissioner —

(*a*) the following information on the design, configuration and security of the provider-owned critical information infrastructure:

(i) a network diagram depicting every key component and interconnection in the provider-owned critical information infrastructure, and any external connection and dependency that the provider-owned critical information infrastructure may have;

*[S 678/2025 wef 31/10/2025]*

(ii) for every key component in the provider-owned critical information infrastructure, the following details:

(A) its name and description;

(B) its physical location;

(C) any operating system and version;

(D) any key software and version;

(E) its internet protocol address and any open port, if the component is internet facing;

(F) the name and address of the operator, if the owner is not the operator;

*[S 678/2025 wef 31/10/2025]*

(iii) the types of data processed on or stored in the provider-owned critical information infrastructure;

*[S 678/2025 wef 31/10/2025]*

(iv) the name and contact of every individual having overall responsibility for the cybersecurity of the provider-owned critical information infrastructure;

*[S 678/2025 wef 31/10/2025]*

(*b*) the following 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 provider-owned critical information infrastructure:

(i) the name and description of that other computer or computer system;

(ii) the physical location of that other computer or computer system;

(iii) the name and address of its operator, if the owner is not the operator;

(iv) a description of any function provided by that other computer or computer system;

(v) the types of data exchanged with the provider-owned critical information infrastructure;

*[S 678/2025 wef 31/10/2025]*

(vi) the operating system and version;

(vii) the key software and version;

(viii) how that other computer or computer system is interconnected with or communicates with the provider-owned critical information infrastructure, including the communication protocol of that other computer or computer system with the provider-owned critical information infrastructure;

*[S 678/2025 wef 31/10/2025]*

(*c*) the name of any outsourced service provider supporting the provider-owned critical information infrastructure, and the nature of the outsourced service; and

*[S 678/2025 wef 31/10/2025]*

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

*[S 678/2025 wef 31/10/2025]*

(3) In this regulation, "physical location" —

(*a*) in relation to a key component of a provider-owned critical information infrastructure that is a virtual computer or virtual computer system, means the physical location of the physical computing resources deployed for the simulation of the key component of the virtual computer or virtual computer system; or

(*b*) in relation to a computer or computer system that is a virtual computer or virtual computer system, means the physical location of the physical computing resources deployed for the simulation of the virtual computer or virtual computer system.

*[S 678/2025 wef 31/10/2025]*

*[S 678/2025 wef 31/10/2025]*

**Report of cybersecurity incident in respect of provider-owned critical information infrastructure, etc.**

**5.**—(1) For the purposes of section 14(1) of the Act, where a cybersecurity incident mentioned in section 14(1)(*a*), (*b*), (*bb*) or (*c*) of the Act, or section 14(1)(*ba*) of the Act which is of the category mentioned in paragraph (1A) occurs, the owner of a provider-owned critical information infrastructure must notify the Commissioner of the occurrence of the cybersecurity incident in the following form and manner:

(*a*) by submitting the following details in the manner specified in paragraph (2), within 2 hours after becoming aware of the occurrence:

(i) the provider-owned critical information infrastructure which the cybersecurity incident relates to;

*[S 678/2025 wef 31/10/2025]*

(ii) the name and contact number of the owner of the provider-owned critical information infrastructure;

*[S 678/2025 wef 31/10/2025]*

(iii) the nature of the cybersecurity incident, whether it was in respect of the provider-owned critical information infrastructure or any other relevant computer or computer system, and when and how it occurred;

*[S 678/2025 wef 31/10/2025]*

(iii*a*) where the relevant computer or computer system the cybersecurity incident was in respect of is an owner-controlled non-interconnected computer or computer system — the purpose of the computer or computer system;

*[S 678/2025 wef 31/10/2025]*

(iv) the resulting effect that has been observed, including how the provider-owned critical information infrastructure or any other relevant computer or computer system has been affected;

*[S 678/2025 wef 31/10/2025]*

(v) the name, designation, organisation and contact number of the individual submitting the notification;

(*b*) by providing to the fullest extent practicable the following supplementary details in writing in the form set out on the Internet website at https://www.csa.gov.sg within 72 hours after becoming aware of the occurrence:

(i*a*) any updates and supplementary details in respect of the details submitted under sub-paragraph (*a*);

*[S 678/2025 wef 31/10/2025]*

(i) the cause of the cybersecurity incident;

(ii) the impact of the cybersecurity incident on the provider-owned critical information infrastructure or

any other relevant computer or computer system, or on the business operations of the owner of the provider-owned critical information infrastructure;

*[S 678/2025 wef 31/10/2025]*

(iii) what remedial measures have been taken;

*[S 678/2025 wef 31/10/2025]*

*[S 678/2025 wef 31/10/2025]*

(*c*) by providing a final incident report containing the following details in writing in the form set out on the Internet website at https://www.csa.gov.sg within 30 days (including any Sunday and public holiday) after the submission mentioned in sub-paragraph (*b*) is made:

(i) the details submitted under sub-paragraphs (*a*) and (*b*);

(ii) to the fullest extent practicable, any updates and supplementary details in respect of the details submitted under sub-paragraphs (*a*) and (*b*).

*[S 678/2025 wef 31/10/2025]*

*[S 678/2025 wef 31/10/2025]*

(1A) The category of cybersecurity incident mentioned in paragraph (1) is a cybersecurity incident mentioned in section 14(1)(*ba*) of the Act which results in any disruption or degradation to the continuous delivery, in Singapore, of the essential service for which the provider-owned critical information infrastructure is designated.

*[S 678/2025 wef 31/10/2025]*

(2) The details mentioned in paragraphs (1)(*a*) and (2C) must be submitted —

(*a*) by calling the telephone number specified by the Commissioner; or

(*b*) if the owner is unable to submit the details in the manner set out in sub-paragraph (*a*) within a reasonable time —

(i) by text message to the telephone number specified by the Commissioner; or

(ii) in writing, in the form set out on the Internet website at https://www.csa.gov.sg, to the electronic address specified by the Commissioner.

*[S 678/2025 wef 31/10/2025]*

(2A) For the purposes of section 14(1) of the Act, where a cybersecurity incident mentioned in section 14(1)(*ba*) of the Act which is not of the category mentioned in paragraph (1A) occurs, the owner of a provider-owned critical information infrastructure must notify the Commissioner of the occurrence of the cybersecurity incident in accordance with paragraphs (2B) and (2C).

*[S 678/2025 wef 31/10/2025]*

(2B) Subject to paragraph (2C), the owner of the provider-owned critical information infrastructure must provide to the fullest extent practicable the following details in a consolidated quarterly report in writing in the form set out on the Internet website at https://www.csa.gov.sg, no later than the end of the third working day following the end of the quarter in which the owner became aware of the cybersecurity incident mentioned in paragraph (2A):

(*a*) the date and time of the cybersecurity incident;

(*b*) the provider-owned critical information infrastructure which the cybersecurity incident relates to;

(*c*) the name and contact number of the owner of the provider-owned critical information infrastructure;

(*d*) the computer or computer system the incident was in respect of, and the purpose of that computer or computer system;

(*e*) the nature of the cybersecurity incident, and when and how it occurred;

(*f*) the cause of the cybersecurity incident;

(*g*) the resulting effect of the cybersecurity incident;

(*h*) the impact of the cybersecurity incident on the computer or computer system mentioned in sub-paragraph (*d*), on the provider-owned critical information infrastructure which the cybersecurity incident relates to, or on the business

operations of the owner of the provider-owned critical information infrastructure;

(*i*) what remedial measures have been taken.

*[S 678/2025 wef 31/10/2025]*

(2C) In addition to notifying the Commissioner of the occurrence of the cybersecurity incident in accordance with paragraph (2B), the owner must, upon the occurrence of any of the circumstances mentioned in paragraph (2D), submit to the Commissioner —

(*a*) within 2 hours after the occurrence of the circumstance, the following details in the manner specified in paragraph (2):

(i) the details set out in paragraph (1)(*a*);

(ii) the circumstance or circumstances mentioned in paragraph (2D) which has or have occurred;

(*b*) within 72 hours after the occurrence of the circumstance, the supplementary details set out in paragraph (1)(*b*) (to the fullest extent practicable) in the form set out on the Internet website at https://www.csa.gov.sg; and

(*c*) within 30 days (including any Sunday and public holiday) after the submission mentioned in sub-paragraph (*b*) is made, a final incident report containing the details set out in paragraph (1)(*c*).

*[S 678/2025 wef 31/10/2025]*

(2D) The circumstances mentioned in paragraph (2C) are as follows:

(*a*) the owner becomes aware that the cybersecurity incident has any effect which is observable by any member of the public;

(*b*) the owner becomes aware that the cybersecurity incident was caused by or related to an exploitation of a vulnerability which was a zero-day vulnerability at the time of the exploit;

(*c*) the owner becomes aware that any indicator of compromise that is associated with an advanced persistent threat and was previously notified in writing to

the owner by the Commissioner was detected in relation to the cybersecurity incident;

(*d*) the owner suspects that the cybersecurity incident may have been caused by an advanced persistent threat.

*[S 678/2025 wef 31/10/2025]*

(2E) In paragraph (2B), "quarter" means a period of 3 months beginning on 1 January, 1 April, 1 July or 1 October of any year.

*[S 678/2025 wef 31/10/2025]*

(3) For the purposes of section 14(1)(*a*), (*b*), (*ba*) and (*bb*) of the Act, the following are prescribed cybersecurity incidents in respect of a relevant computer or computer system:

(*a*) any unauthorised hacking of the relevant computer or computer system to gain unauthorised access to or control of the relevant computer or computer system;

(*b*) any installation or execution of unauthorised software, or computer code, of a malicious nature on the relevant computer or computer system;

(*c*) any man-in-the-middle attack, session hijack or other unauthorised interception by means of a computer or computer system of communication between the relevant computer or computer system, and an authorised user of the relevant computer or computer system;

(*d*) any denial of service attack or other unauthorised act or acts carried out through a computer or computer system that adversely affects the availability or operability of the relevant computer or computer system.

*[S 678/2025 wef 31/10/2025]*

(4) In this regulation —

"advanced persistent threat" means an adversary, possessing sophisticated levels of expertise, that —

(*a*) employs advanced techniques; and

(*b*) demonstrates persistence (for example, by pursuing its objectives repeatedly and over an extended period of time while taking measures to stay undetected),

in an effort to jeopardise or adversely affect the cybersecurity of the computer or computer system which it is targeting, for a purpose such as espionage, deception or disruption;

*Examples*

Examples of advanced techniques are techniques which involve time-stomping, chaining exploits, attacking system memory, the bypassing or disarming of protective measures or the use of fileless malware.

"indicator of compromise" means a technical artifact or event on a network or system that suggests a cybersecurity incident is imminent or is currently underway, or that a cybersecurity incident may have already occurred;

"interception", in relation to a communication to or from a relevant computer or computer system, includes —

(*a*) listening to or the recording of the communication; and

(*b*) acquiring the substance, meaning or purport of that communication;

"zero-day vulnerability" means a hardware, firmware or software weakness, susceptibility or flaw, which can be exploited to jeopardise or adversely affect the cybersecurity of a computer or computer system, that is not previously known to the cybersecurity industry at a relevant point in time, as evidenced by such weakness, susceptibility or flaw not being included in any of the following:

(*a*) the Common Vulnerabilities and Exposures List published on the Common Vulnerabilities and Exposures Program's website at https://www.cve.org;

(*b*) the National Vulnerability Database published on the United States National Institute of Standards and Technology's website at https://nvd.nist.gov;

(*c*) the Known Exploited Vulnerabilities Catalog published on the United States Cybersecurity and Infrastructure Security Agency's website at

https://www.cisa.gov/known-exploited-vulnerabilities-catalog;

(*d*) the European Union Vulnerability Database published on the European Union Agency for Cybersecurity's website at https://euvd.enisa.europa.eu.

*[S 678/2025 wef 31/10/2025]*

*[S 678/2025 wef 31/10/2025]*

**Cybersecurity risk assessment**

**6.**—(1) For the purposes of section 15(1)(*b*) of the Act, a cybersecurity risk assessment of a provider-owned critical information infrastructure must be conducted in the following form and manner:

(*a*) the assessment must —

(i) identify, as far as is reasonably practicable, every cybersecurity risk to the provider-owned critical information infrastructure;

(ii) evaluate the likelihood of the occurrence, and the possible consequences, of the materialisation of each identified cybersecurity risk; and

(iii) identify the action that the owner of the provider-owned critical information infrastructure will take in respect of each identified cybersecurity risk;

(*b*) the report of the assessment must cover the following:

(i) the methodology used in the cybersecurity risk assessment;

(ii) a description of every identified cybersecurity risk to the provider-owned critical information infrastructure;

(iii) the evaluated likelihood and possible consequences of the materialisation of each identified cybersecurity risk;

(iv) the identified action that the owner of the provider-owned critical information infrastructure will take in respect of each identified cybersecurity risk.

*[S 678/2025 wef 31/10/2025]*

(2) The first cybersecurity risk assessment of a provider-owned critical information infrastructure must be completed within 6 months after the date of the notice issued under section 7(1) or (1A) of the Act or, subject to section 15(1)(*b*) of the Act, any longer period that the Commissioner may allow in a particular case.

*[S 678/2025 wef 31/10/2025]*

(2A) To avoid doubt, where the designation of a provider-owned critical information infrastructure is extended under section 9A of the Act, the reckoning of time for the performance of the duty of the owner of the provider-owned critical information infrastructure to conduct a cybersecurity risk assessment of the provider-owned critical information infrastructure at least once a year in accordance with section 15(1)(*b*) of the Act, starts from the date of the notice issued under section 7(1) or (1A) of the Act.

*[S 678/2025 wef 31/10/2025]*

(3) In this regulation, "cybersecurity risk", in relation to a provider-owned critical information infrastructure, means the risk that a vulnerability in the cybersecurity of the provider-owned critical information infrastructure may be exploited by a cybersecurity threat or incident.

*[S 678/2025 wef 31/10/2025]*

## PART 3

[*Deleted by S 678/2025 wef 31/10/2025*]

## PART 4

[*Deleted by S 678/2025 wef 31/10/2025*]

Made on 30 August 2018.

GABRIEL LIM
*Permanent Secretary*
*(Cybersecurity),*
*Prime Minister's Office,*
*Singapore.*

[AK02.001.001; AG/LEGIS/SL/70A/2015/2 Vol. 1]