First published in the Government *Gazette*, www.egazette.gov.sg, on 15 October 2025 at 7 pm.

No. S 678

CYBERSECURITY ACT 2018

CYBERSECURITY
(CRITICAL INFORMATION INFRASTRUCTURE)
(AMENDMENT) REGULATIONS 2025

In exercise of the powers conferred by sections 17(10) and 48 of the Cybersecurity Act 2018, the Minister for Digital Development and Information, Josephine Teo, who is charged with the responsibility for cybersecurity, makes the following Regulations:

Citation and commencement

1. These Regulations are the Cybersecurity (Critical Information Infrastructure) (Amendment) Regulations 2025 and come into operation on 31 October 2025.

Amendment of regulation 1

2. In the Cybersecurity (Critical Information Infrastructure) Regulations 2018 (G.N. No. S 519/2018) (called in these Regulations the principal Regulations), in regulation 1, before "Critical Information Infrastructure", insert "Provider-Owned".

Amendment of regulation 2

3. In the principal Regulations, in regulation 2, replace the definitions of "Appeals Secretary" and "appellant" with —

> "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;

"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;

"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;

"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;".

Amendment of regulation 3

4. In the principal Regulations, in regulation 3 —

(*a*) in paragraph (2), after sub-paragraph (*e*), insert —

"(*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;"; and

(*b*) after paragraph (2), insert —

"(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.".

Amendment of regulation 4

5. In the principal Regulations, in regulation 4, after paragraph (2), insert —

"(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.".

Amendment of regulation 5

6. In the principal Regulations, in regulation 5 —

(*a*) in paragraph (1), replace "section 14(1)(*a*), (*b*) or (*c*) of the Act" with "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)";

(*b*) in paragraph (1)(*a*)(i), replace "affected" with "which the cybersecurity incident relates to";

(*c*) in paragraph (1)(*a*)(iii), replace "critical information infrastructure or an interconnected" with "provider-owned critical information infrastructure or any other relevant";

(*d*) in paragraph (1)(*a*), after sub-paragraph (iii), insert —

"(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;";

(*e*) in paragraph (1)(*a*)(iv), replace "critical information infrastructure or any interconnected" with "provider-owned critical information infrastructure or any other relevant";

(*f*) in paragraph (1)(*b*), replace "14 days after the submission mentioned in sub-paragraph (*a*)" with "72 hours after becoming aware of the occurrence";

(*g*) in paragraph (1)(*b*), before sub-paragraph (i), insert —

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

(*h*) in paragraph (1)(*b*), replace sub-paragraph (ii) with —

"(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;";

(*i*) in paragraph (1)(*b*)(iii), replace the full-stop at the end with a semi-colon;

(*j*) in paragraph (1), after sub-paragraph (*b*), insert —

"(*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*).";

(*k*) after paragraph (1), insert —

"(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.";

(*l*) in paragraph (2), replace "paragraph (1)(*a*)" with "paragraphs (1)(*a*) and (2C)"; and

(*m*) replace paragraphs (3) and (4) with —

"(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).

(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.

(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*).

(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.

(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.

(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.

(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.".

Amendment of regulation 6

7. In the principal Regulations, in regulation 6, replace paragraph (2) with —

"(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.

(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.".

Deletion of Parts 3 and 4

8. In the principal Regulations, delete Parts 3 and 4.

Miscellaneous amendments

9. In the principal Regulations —

(*a*) in the following regulations, in the regulation heading, replace "**critical information infrastructure**" with "**provider-owned critical information infrastructure**":

Regulation 3

Regulation 4

Regulation 5; and

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

Regulation 3(2)

Regulation 4(1) and (2)

Regulation 5(1)

Regulation 6(1) and (3).

Saving and transitional provision

10. Despite regulation 6, regulation 5 of the principal Regulations as in force immediately before 31 October 2025 continues to apply to and in relation to a cybersecurity incident for which a report mentioned in regulation 5(1)(*a*) of those principal Regulations had been submitted before that date.

Made on 15 October 2025.

JOSEPH LEONG WENG KEONG
Permanent Secretary
(Cybersecurity),
Prime Minister's Office,
Singapore.

[CSA.0007.200003; 2020-1629; AG/LEGIS/SL/70A/2020/8]