No. S 490

CYBERSECURITY ACT 2018

CYBERSECURITY (PROVIDERS OF ESSENTIAL SERVICE RESPONSIBLE FOR CYBERSECURITY OF THIRD-PARTY-OWNED CRITICAL INFORMATION INFRASTRUCTURE) REGULATIONS 2026

ARRANGEMENT OF REGULATIONS

In exercise of the powers conferred by section 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 (Providers of Essential Service Responsible for Cybersecurity of Third-Party-Owned Critical Information Infrastructure) Regulations 2026 and come into operation on 13 July 2026.

Definitions

2. In these Regulations —

"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 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;

"quarter" means a period of 3 months beginning on 1 January, 1 April, 1 July or 1 October of any year;

"relevant computer or computer system", in relation to a designated provider responsible for third-party-owned critical information infrastructure, means a computer or computer system mentioned in section 16I(4)(*a*), (*b*) or (*c*) of the Act, being —

(*a*) the third-party-owned critical information infrastructure;

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

(*c*) any other computer or computer system under the provider's control that does not fall within section 16I(4)(*b*) of the Act;

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

"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 the 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.

Information to ascertain if provider of essential service fulfils criteria for designated provider responsible for cybersecurity of third-party-owned critical information infrastructure

3. For the purposes of section 16B(2) of the Act, a notice to provide relevant information to the Commissioner must be given in writing in the form set out on the Internet website at https://www.csa.gov.sg.

Information relating to third-party-owned critical information infrastructure

4. For the purposes of section 16E(4) of the Act, a notice to the designated provider responsible for third-party-owned critical information infrastructure to furnish information must be given in writing in the form set out on the Internet website at https://www.csa.gov.sg.

Prescribed period for purposes of section 16I(1) of Act

5. For the purposes of section 16I(1) of the Act, the prescribed period is 72 hours.

Prescribed cybersecurity incidents for purposes of section 16I(4) of Act

6. For the purposes of section 16I(4)(*a*), (*b*) and (*c*) of the Act, the following incidents 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.

Report of cybersecurity incident in respect of third-party-owned critical information infrastructure, etc.

7.—(1) Paragraph (2) applies to the following cybersecurity incidents:

(*a*) a prescribed cybersecurity incident mentioned in section 16I(4)(*a*) or (*b*) of the Act;

(*b*) a prescribed cybersecurity incident mentioned in section 16I(4)(*c*) of the Act which results in any disruption or degradation to the continuous delivery, in Singapore, of the essential service (where the third-party-owned critical information infrastructure is necessary for the continuous delivery);

(*c*) a cybersecurity incident mentioned in section 16I(4)(*d*) of the Act.

(2) For the purposes of section 16I(4) of the Act, if a cybersecurity incident mentioned in paragraph (1) occurs, the designated provider responsible for the third-party-owned critical information infrastructure in respect of which the incident occurred must notify the Commissioner of the occurrence of the cybersecurity incident within the following prescribed periods and in the following prescribed form and manner:

(*a*) within 2 hours after becoming aware of the occurrence — by submitting the following details in the manner mentioned in paragraph (6):

(i) the particulars of the third-party-owned critical information infrastructure;

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

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

(iv) if the relevant computer or computer system in respect of which the cybersecurity incident occurred is a computer or computer system under the provider's control that does not fall within section 16I(4)(*b*) of the Act — the purpose of the computer or computer system;

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

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

(*b*) within 72 hours after becoming aware of the occurrence — 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:

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

(ii) the cause of the cybersecurity incident;

(iii) the impact of the cybersecurity incident on the third-party-owned critical information infrastructure or any other relevant computer or computer system, or on the business operations of the designated provider responsible for the third-party-owned critical information infrastructure;

(iv) the remedial measures that have been taken;

(*c*) within 30 days (including any Saturday, Sunday and public holiday) after the submission mentioned in sub-paragraph (*b*) is made — 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:

(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*).

(3) Paragraph (4) applies to a prescribed cybersecurity incident mentioned in section 16I(4)(*c*) of the Act which does not result in any disruption or degradation to the continuous delivery, in Singapore, of the essential service (where the third-party-owned critical information infrastructure is necessary for the continuous delivery).

(4) For the purposes of section 16I(4) of the Act, if a prescribed cybersecurity incident mentioned in paragraph (3) occurs, the designated provider responsible for the third-party-owned critical information infrastructure in respect of which the incident occurred must notify the Commissioner of the occurrence of the cybersecurity incident in the following prescribed form and manner and within the following prescribed periods:

(*a*) by providing to the Commissioner, 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 designated provider became aware of the cybersecurity incident:

(i) the date and time of the cybersecurity incident;

(ii) the particulars of the third-party-owned critical information infrastructure;

(iii) the name and contact number of the owner of the third-party-owned critical information infrastructure;

(iv) the computer or computer system in respect of which the cybersecurity incident occurred, and the purpose of that computer or computer system;

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

(vi) the cause of the cybersecurity incident;

(vii) the resulting effect of the cybersecurity incident;

(viii) the impact of the cybersecurity incident on the computer or computer system mentioned in sub-paragraph (iv), on the third-party-owned critical information infrastructure, or on the business operations of the designated provider responsible for the third-party-owned critical information infrastructure;

(ix) the remedial measures that have been taken;

(*b*) if any of the circumstances mentioned in paragraph (5) occurs — by submitting to the Commissioner —

(i) within 2 hours after the occurrence of the circumstance — the following details in the manner mentioned in paragraph (6):

(A) the details set out in paragraph (2)(*a*);

(B) the circumstance mentioned in paragraph (5) that has occurred;

(ii) within 72 hours after the occurrence of the circumstance — the supplementary details set out in paragraph (2)(*b*) (to the fullest extent practicable) in the form set out on the Internet website at https://www.csa.gov.sg; and

(iii) within 30 days (including any Sunday and public holiday) after the submission mentioned in sub-paragraph (ii) is made — a final incident report containing the details set out in paragraph (2)(*c*).

(5) The circumstances mentioned in paragraph (4)(*b*) are as follows:

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

(*b*) the designated provider 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 designated provider becomes aware that any indicator of compromise that is associated with an advanced persistent threat and that was previously notified in writing to the designated provider by the Commissioner was detected in relation to the cybersecurity incident;

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

(6) The manner of submission mentioned in paragraphs (2)(*a*) and (4)(*b*)(i) is submission —

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

(*b*) if the designated provider 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.

Cybersecurity risk assessment

8.—(1) For the purposes of section 16J(1)(*b*) of the Act, a designated provider responsible for third-party-owned critical information infrastructure must obtain from the owner of the

third-party-owned critical information structure a legally binding commitment that a cybersecurity risk assessment will be conducted in the following form and manner:

(*a*) that the assessment will —

(i) identify, as far as is reasonably practicable, every cybersecurity risk to the third-party-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 actions that will be taken in respect of each identified cybersecurity risk by any of the following:

(A) the designated provider of the third-party-owned critical information infrastructure;

(B) the owner of the third-party-owned critical information infrastructure;

(*b*) that the report of the assessment will include the following:

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

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

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

(iv) the identified action that will be taken in respect of each identified cybersecurity risk by the designated provider, or owner, of the third-party-owned critical information infrastructure, as the case may be.

(2) A designated provider responsible for third-party-owned critical information infrastructure must obtain from the owner of the

third-party-owned critical information structure a legally binding commitment that the first cybersecurity risk assessment of the third-party-owned critical information infrastructure will be completed within 6 months after the date of the notice issued under section 16A(1) of the Act or, subject to section 16J(1)(*b*) of the Act, any longer period that the Commissioner may allow in a particular case.

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

Made on 6 July 2026.

CHNG KAI FONG
Permanent Secretary
(Cybersecurity),
Prime Minister's Office,
Singapore.

[CSA.0007.200003; 2020-1629; AG/LEGIS/SL/70A/2025/4]