Cybersecurity | Third-Party-Owned Critical Information Infrastructure

Cybersecurity Regulations 2026: Key Obligations for Providers Responsible for Cybersecurity of Third-Party-Owned Critical Information Infrastructure

On 10 July 2026, the Cybersecurity (Providers of Essential Service Responsible for Cybersecurity of Third-Party-Owned Critical Information Infrastructure) Regulations 2026 (**Regulations**) were gazetted. The Regulations came into operation on **13 July 2026**.

The Regulations, made by the Minister for Digital Development and Information, prescribe certain timelines, forms and technical criteria for several obligations under Part 3A of the Cybersecurity Act 2018 (**Act**).

Part 3A of the Act, which came into force on 31 October 2025, sets out a framework for providers of essential services responsible for the cybersecurity of third-party-owned critical information infrastructure (**TPO-CII**). Under Part 3A, the Commissioner of Cybersecurity (**Commissioner**) may, by written notice, designate a provider as such (**Designated Provider**) if the Commissioner is satisfied that a computer or computer system (called a TPO-CII) (whether located in or outside Singapore): (a) is necessary for the continuous delivery of an essential service provided by the Designated Provider and its loss or compromise will have a debilitating effect on the availability of that service in Singapore; and (b) is not owned by the Designated Provider. Such a designation has effect for five years unless earlier withdrawn by the Commissioner.

The Regulations principally impose the following obligations on a Designated Provider: (a) reporting prescribed cybersecurity incidents to the Commissioner; and (b) obtaining a legally binding commitment from the owner of a TPO-CII (**Owner**) to conduct a cybersecurity risk assessment.

The key provisions of the Regulations are set out below.

Reporting of Cybersecurity Incidents

The Act sets out detailed requirements for cybersecurity incident reporting, structured around two separate notification obligations: a Designated Provider must obtain from the Owner a legally binding commitment that the Owner will notify the Designated Provider of specified cybersecurity incidents elaborated below (**Notification Commitment**); and the Designated Provider must separately report the above and other specified cybersecurity incidents (as elaborated below) to the Commissioner.

Reportable cybersecurity incidents and Owner's notification timeline

For the purposes of the Designated Provider's reporting obligation, the Regulations prescribe the following categories of cybersecurity incidents in respect of a relevant computer or computer system (**prescribed incidents**):

(a) **Unauthorised access**: 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) **Malicious code**: Any installation or execution of unauthorised software, or computer code, of a malicious nature on the relevant computer or computer system;

(c) **Interception**: 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) **Disruption**: Any denial-of-service attack or other unauthorised act(s) carried out through a computer or computer system that adversely affects the availability or operability of the relevant computer or computer system.

A relevant computer or computer system, in relation to a Designated Provider, means: (a) the TPO-CII; (b) a computer or computer system under the Owner's or Designated Provider's control, that is interconnected with or communicates with the TPO-CII; or (c) any other computer or computer system under the Designated Provider's control that does not fall within (b) above.

The Notification Commitment must require the Owner to notify the Designated Provider of a prescribed incident in respect of the TPO-CII and any computer or computer system under the Owner's control that is interconnected with or communicates with the TPO-CII as well as any other type of cybersecurity incident in respect of the TPO-CII that the Commissioner has specified by written direction to the Designated Provider. Under the Regulations, the Owner must do so within 72 hours after becoming aware of the incident.

Reporting to the Commissioner

The Designated Provider must notify the Commissioner of the following prescribed incidents (collectively, **Relevant Cybersecurity Incidents**) in the prescribed form and manner, within the prescribed period after becoming aware of such occurrence:

(a) A prescribed incident in respect of the TPO-CII;

(b) A prescribed incident in respect of any computer or computer system under the Owner's or the Designated Provider's control that is interconnected with or communicates with the TPO-CII;

(c) A prescribed incident in respect of any other computer or computer system under the Designated Provider's control that does not fall within paragraph (b) above which results in any disruption or degradation to the continuous delivery, in Singapore, of the essential service (where the TPO-CII is necessary for the continuous delivery); and

(d) Any other type of cybersecurity incident in respect of the TPO-CII that the Commissioner has specified by written direction to the Designated Provider.

The prescribed periods, form and manner are as follows:

(a) **Initial notification (within 2 hours)**: Notify the Commissioner within two hours after becoming aware of the occurrence of a Relevant Cybersecurity Incident, initially by calling the telephone number specified by the Commissioner or, if the Designated Provider is unable to do so within a reasonable time, by text message to that telephone number; or in writing, in the form on the Cyber Security Agency of Singapore (**CSA**)'s website, to the electronic address specified by the Commissioner. The initial notification must set out: (i) the particulars of the TPO-CII; (ii) the name and contact number of the Owner; (iii) the nature of the Relevant Cybersecurity Incident, whether it occurred in respect of the TPO-CII or any other relevant computer or computer system, and when and how it occurred; (iv) if the relevant computer or computer system is under the Designated Provider's control that is not interconnected with or does not communicate with the TPO-CII, the purpose of the computer or computer system; (v) the resulting effect that has been observed, including how the TPO-CII or any other relevant computer or computer system has been affected; and (vi) the name, designation, organisation and contact number of the individual submitting the notification;

(b) **Supplementary report (within 72 hours)**: Provide, to the fullest extent practicable, the following supplementary details in the form on CSA's website within 72 hours after becoming aware of the occurrence of the Relevant Cybersecurity Incident : (i) any updates and supplementary details in respect of the details submitted under paragraph (a) above; (ii) the cause of the incident; (iii) the impact on the TPO-CII or any other relevant computer or computer system, or on the business operations of the Designated Provider; and (iv) the remedial measures that have been taken; and

(c) **Final report (within 30 days after submission of the supplementary report)**: Provide a final incident report in the form on CSA's website within 30 days (including any Saturday, Sunday and public holiday) after the supplementary report is submitted containing: (i) the details submitted in the initial notification and supplementary report; and (ii) to the fullest extent practicable, any updates and supplementary details.

Quarterly consolidated reporting for non-disruptive incidents

For a prescribed incident on any other computer or computer system under the Designated Provider's control (that is not interconnected with or does not communicate with the TPO-CII) which does not result in any disruption or degradation to the continuous delivery, in Singapore, of the essential service (where the TPO-CII is necessary for the continuous delivery), the Designated Provider must

notify the Commissioner of the occurrence of such prescribed incident in the following prescribed form and manner and prescribed periods:

(a) **Consolidated quarterly report**: To the fullest extent practicable, details in a consolidated quarterly report in writing in the form set out on CSA's website, no later than the end of the third working day following the end of the quarter in which the Designated Provider became aware of such prescribed incident. For this purpose, a quarter is a three-month period beginning on 1 January, 1 April, 1 July or 1 October of any year; and a working day means any day except a Saturday, Sunday or public holiday.

(b) **Required details**: The consolidated quarterly report must include: (i) the date and time of such prescribed incident; (ii) the particulars of the TPO-CII; (iii) the name and contact number of the Owner; (iv) the computer or computer system in respect of which such prescribed incident occurred, and its purpose; (v) the nature of such prescribed incident, and when and how it occurred; (vi) its cause; (vii) the resulting effect; (viii) the impact on the computer or computer system, the TPO-CII, or the business operations of the Designated Provider; and (ix) the remedial measures that have been taken.

A Designated Provider must, however, revert to the 2-hour, 72-hour and 30-day timeline with requisite details for such prescribed incident if it becomes aware that: (a) the incident has any effect observable by any member of the public; (b) the incident was caused by or related to the exploitation of a zero-day vulnerability, being 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 was not previously known to the cybersecurity industry, at the time of the exploit; or (c) any indicator of compromise 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 incident. A Designated Provider must also revert to that timeline if it suspects that the incident may have been caused by an advanced persistent threat.

Cybersecurity Risk Assessments

A Designated Provider must obtain from the Owner a legally binding commitment that a cybersecurity risk assessment of the TPO-CII (**Assessment**) will be conducted at least once a year (**Risk Assessment Commitment**) and that the Assessment will: (a) identify, as far as is reasonably practicable, every cybersecurity risk to the TPO-CII; (b) evaluate the likelihood of the occurrence, and possible consequences, of the materialisation of each identified cybersecurity risk; and (c) identify the actions that will be taken in respect of each identified cybersecurity risk by the Designated Provider or the Owner.

In this context, "cybersecurity risk", in relation to the TPO-CII, means the risk that a vulnerability in the cybersecurity of the TPO-CII may be exploited by a cybersecurity threat or incident. The report of the Assessment must include: (a) the methodology used in the Assessment; (b) a description of every identified risk to the TPO-CII; (c) the evaluated likelihood and possible consequences of the materialisation of each identified cybersecurity risk; and (d) the identified action that will be taken in respect of each identified cybersecurity risk by the Designated Provider or Owner. The Risk

Assessment Commitment must require the Owner to furnish the report to the Designated Provider no later than 30 days after the Assessment is completed, and the Designated Provider must furnish a copy to the Commissioner no later than 14 days after receiving it from the Owner. Additionally, the Designated Provider must obtain a legally binding commitment from the Owner that the first Assessment will be completed within six months after the date on which the Commissioner, by written notice, designates the Designated Provider as such, or any longer period that the Commissioner may allow.

Offences and Enforcement

Under the Act, a Designated Provider who, without reasonable excuse, fails to report a Relevant Cybersecurity Incident to the Commissioner as required is liable to a fine of not more than S$100,000, or imprisonment for a term of not more than 2 years, or both. Where a Designated Provider fails to obtain a required Notification Commitment or Risk Assessment Commitment from the Owner, the Commissioner may order the Designated Provider to stop using, directly or indirectly, the TPO-CII; a Designated Provider who, without reasonable excuse, fails to comply with such an order is liable to the same maximum penalty, together with a further fine not exceeding S$5,000 for every day or part of a day during which the offence continues after conviction. A Designated Provider who, without reasonable excuse, fails to notify the Commissioner of a material change to a Notification Commitment or Risk Assessment Commitment no later than 14 days after the change is made is liable to a fine not exceeding S$25,000, or imprisonment for a term not exceeding 12 months, or both.

If you would like information and/or assistance on the above or any other area of law, you may wish to contact the Partner at WongPartnership whom you normally work with or any of the following Partners:

LAM Chung Nian
Head – Intellectual Property, Technology & Data

Kylie PEH
Partner – Intellectual Property, Technology & Data

Connect with WongPartnership.

WPG MEMBERS AND OFFICES

- contactus@wongpartnership.com

SINGAPORE

-
WongPartnership LLP
12 Marina Boulevard Level 28
Marina Bay Financial Centre Tower 3
Singapore 018982
t +65 6416 8000
f +65 6532 5711/5722

CHINA

-
WongPartnership LLP
Shanghai Representative Office
Unit 1015 Link Square 1
222 Hubin Road
Shanghai 200021, PRC
t +86 21 6340 3131
f +86 21 6340 3315

INDONESIA

-
Makes & Partners Law Firm
Menara Batavia, 7th Floor
Jl. KH. Mas Mansyur Kav. 126
Jakarta 10220, Indonesia
t +62 21 574 7181
f +62 21 574 7180
w makeslaw.com

MALAYSIA

-
Cheang & Ariff
Advocates & Solicitors
Loke Mansion
273A, Jalan Medan Tuanku
50300 Kuala Lumpur
t +60 3 2691 0803
f +60 3 2693 4475
w cheangariff.com
-
Foong & Partners
Advocates & Solicitors
13-1, Menara 1MK, Kompleks 1 Mont' Kiara
No 1 Jalan Kiara, Mont' Kiara
50480 Kuala Lumpur, Malaysia
t +60 3 6419 0822
f +60 3 6419 0823
w foongpartners.com

MIDDLE EAST

-
Al Aidarous Advocates and Legal Consultants
Abdullah Al Mulla Building, Mezzanine Suite 02
39 Hameem Street (side street of Al Murroor Street)
Al Nahyan Camp Area
P.O. Box No. 71284
Abu Dhabi, UAE
t +971 2 6439 222
f +971 2 6349 229
w aidarous.com
-
Al Aidarous Advocates and Legal Consultants
Oberoi Centre, 13th Floor, Marasi Drive, Business Bay
P.O. Box No. 33299
Dubai, UAE
t +971 4 2828 000
f +971 4 2828 011

PHILIPPINES

-
Gruba Law
27/F 88 Corporate Center
141 Valero St., Salcedo Village
Makati City 1227, Philippines
t +63 2 889 6060
f +63 2 889 6066
w grubalaw.com