

Cybersecurity | Critical Information Infrastructure

Cybersecurity Code of Practice for Critical Information Infrastructure to Be Updated to Address APT and AI-enabled Threats

On 22 July 2026, the Cyber Security Agency of Singapore (**CSA**) issued a [press release](#) announcing that it will, in the later part of this year, release the updated Cybersecurity Code of Practice (**CCoP**) for Critical Information Infrastructure (**CII**), and a new CCoP for Cloud Services (**CCoP (Cloud)**).

Since the last update of the CCoP in 2022, the cyber threat landscape has shifted with new artificial intelligence (**AI**)-enabled threats, allowing threat actors to launch attacks faster and at a greater scale. With the emergence of Frontier AI, threat actors can now discover vulnerabilities faster, thus shortening the window period for exploitation. As part of Singapore's efforts to deal with Advanced Persistent Threats (**APTs**) and AI-enabled threats, the Government is working together with CII owners to raise their cybersecurity posture.

The updates to the CCoP focus on strengthening CII governance, visibility, detection and readiness, and broader enterprise networks that are interconnected with the CIIs, to align with the amendments made to the Cybersecurity Act 2018 (**Act**). The CCoP is intended to specify the minimum requirements that the CII owner shall implement to ensure the cybersecurity of its CII in accordance with the Act, which establishes a legal framework for the oversight and maintenance of national cybersecurity in Singapore. The Act has been amended to ensure that CII owners remain responsible for the cybersecurity and cyber resilience of the CII, even as they embrace new technological and business models, like the use of cloud computing.

The new CCoP (Cloud) aims to establish cybersecurity requirements governing the secure deployment, operation, and management of CII systems hosted on the cloud.

We highlight below the key features of the press release.

Upcoming Launch of CCoP 2026

The key changes to the CCoP are:

- (a) **Board and senior management accountability:** CII owners are required to strengthen Board and senior management accountability and oversight for cybersecurity. Boards must maintain a documented cyber resilience framework covering risk tolerance, mitigation, transfer, and recovery, reviewed at least annually.
- (b) **Cyber Trust Mark Level 5 certification:** CII owners are required to attain Cyber Trust Mark Level 5 certification to elevate the cybersecurity posture of CIIs.

- (c) **Oversight of interconnected systems:** CII owners are required to maintain oversight of interconnected systems that connect and communicate with CII to strengthen visibility of the broader network architecture and improve cybersecurity risk management.
- (d) **Threat detection systems:** CSA will work with CII owners to deploy threat detection systems across CII owners' network segments to detect malicious activities.
- (e) **Cybersecurity exercise plan:** CII owners are required to develop a comprehensive cybersecurity exercise plan, to ensure coordinated and effective response to cyber incidents.
- (f) **Network architecture management:** CII owners are required to have robust management measures to maintain network architecture, for example, in the areas of network management, monitoring, and detection management.

The CCoP will be further updated later this year with technical guidance covering adversarial attack simulation, penetration testing, and threat hunting.

Planned Launch of the CCoP (Cloud) in 2H 2026

With CII owners increasingly adopting cloud technologies to support their operations, there is a need to ensure that these environments are secured against evolving cyber threats. The CCoP (Cloud) aims to establish cybersecurity requirements governing the secure deployment, operation, and management of CII systems hosted on the cloud.

CSA conducted a series of closed-door consultations with key stakeholders, including auditors as well as CII owners that have or are exploring the adoption of cloud services, to understand the operating environment and ensure that the proposed controls are practical and implementable. Feedback gathered through these engagements was incorporated into the refinement of both the controls and the accompanying guidance statements, resulting in a more robust, practical, and operationally applicable set of requirements.

CSA has partnered with leading Cloud Service Providers (**CSPs**), namely, Amazon Web Services, Google Cloud and Microsoft Azure, to jointly develop CSP-specific Companion Guides, which will be published alongside the CCoP (Cloud). The Companion Guides will provide practical guidance on how the CCoP (Cloud) controls can be implemented within their respective cloud environments through appropriate configurations and the effective use of cloud-native services and security capabilities.

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