Baker McKenzie Wong & Leow.

Intellectual Property & Technology
Client Alert

March 2022

Singapore: New initiatives to ensure digital security and enhanced cyber resilience

The government announces legislative, regulatory and economic measures to build a digitally secure, economically vibrant, and socially stable Singapore

In brief

The Ministry of Communications and Information announced plans to build a digitally secure, economically vibrant, and socially stable Singapore during the Committee of Supply 2022 debate on 4 March 2022.

The new initiatives will enhance the cyber resilience of Critical Information Infrastructure (CII) sectors and better secure Singapore's cyberspace. Of particular note, the Cyber Security Agency of Singapore (CSA) will update and expand the Cybersecurity Act to also cover virtual assets (such as cloud-hosted systems), foundational digital infrastructure and key digital services.

Other initiatives include:

- Updating the Cybersecurity Code of Practice (CCoP) for the 11 CII sectors
- Introducing new Internet Codes of Practice ("**New Codes**") to raise the baseline standard for online safety to create a safer online environment
- A new Alternative Dispute Resolution (ADR) scheme
- A new Data Protection Essentials (DPE) programme
- Sustainable development of data centres

We summarise these developments and the extent of these changes below.

In addition, the government will support small and medium enterprises (SMEs) to digitally transform and internationalise through the Advanced Digital Solutions scheme, which will provide more AI-enabled and cloud-based integrated solutions. The government will also introduce a broader suite of e-commerce platforms under the Grow Digital scheme, to help SMEs access international markets without the need for physical presence overseas.

In this issue

Key takeaways

Please refer to the table below for the proposed changes and timelines:

Review of the Cybersecurity Act	The provisions currently focused on securing and protecting CII, i.e. computer systems delivering water, power and other essential services in the physical world, will be expanded to: • Require awareness of cyberspace threats, possibly to require patches to known software vulnerabilities, before malicious actors compromise the systems or exfiltrate data • Recognise and protect those virtual assets supporting essential services (e.g. systems hosted on the cloud) as CII, in addition to securing physical networks and systems • Apply a risk-based approach to protect those foundational digital infrastructure and key digital services, e.g. apps, important to enable our

	digital economy and sustain our digital way of life, and for them to recover quickly when attacked
Timeline	After stakeholder and public consultations planned for early 2023, the Ministry of Communications and Information and the CSA intend to complete the review in 2023 and thereafter update the Cybersecurity Act.
Update to the Cybersecurity Code of Practice	The CCoP currently comprises foundational cyber hygiene practices set out in: • The list of Codes of Practice issued by the Commissioner of Cybersecurity for the regulation of those critical sectors designated as CII • The mandatory Operational Technology (OT)-specific cybersecurity practices to elevate the state of cybersecurity for OT CII Recognising these foundational cyber hygiene practices may be insufficient to counter evolving, and increasingly sophisticated, cyber threats, as well as CII cybersecurity risks specific to their digital terrains, the CSA proposes to enhance the CCoP to achieve the following objectives: • To help CIIs improve their odds of defending against cyber threat actors using sophisticated threats • To allow CIIs to be more agile to respond to emerging risks in specific domains • To enhance coordinated defences between the Government and private sectors to identify, discover and respond to cyber threats and/or attacks in a timely manner The CSA suggests more advanced cyber hygiene practices such as: • Adopting a threat-based approach to identify threat actors' common tactics and techniques used in a cyber-attack lifecycle, allowing the CSA to identify actions, develop new practices and enhance existing practices to counter and impede the threat actors' activities in a cyber attack • Incorporating the flexibility to add domain-specific practices, e.g. use of 5G technologies, on an *ad-hoc* basis to the relevant CII sectors for specific CII owners to implement, to increase sectors' agility in addressing emerging risks
Timeline	The CSA has briefed and consulted key CII stakeholders, sector leads and owners, and will factor in their feedback before the enhanced CCoP is issued to CII owners in Q2 2022.

New Codes	The Ministry requires online platforms accessible by users in Singapore to take greater responsibility for user safety by endeavouring to keep online spaces free from harmful content, including age-inappropriate content, such as violent and graphic content, and content that promotes sexual violence.
	The Ministry will raise the baseline standard for online safety by introducing codes of practice in three new areas.
	• **Child safety**: Platforms will be required to have robust systems in place, such as content filters for child accounts and online parental supervision mechanisms, to minimise exposure of children and young persons to harmful content
	• **User reporting**: To address feedback from social media platforms that they cannot be fully aware of all the voluminous content that needs moderation, platforms will be required to:
	  ○ Set up easy-to-access mechanisms to empower users to report harmful content
	  ○ Be responsive in evaluating and acting on these reports
	  ○ Apprise users in a timely manner of the actions taken
	• **Platform accountability**: Platforms will be required to provide information on measures undertaken to keep users safe, including:
	  ○ Information on the prevalence of harmful online content on the platforms
	  ○ The user reports received and acted upon
	  ○ The systems and processes in place to address harmful online content,
	so as to allow users to make informed decisions about which platforms to engage with or disengage from.

	These New Codes will have the force of law, similar to existing Codes of Practice administered by the Infocomm Media Development Authority (IMDA).
Timeline	The Ministry has not released any dates but is presently studying how to effectively enforce the New Codes, including through appropriate legislative updates.
ADR scheme	IMDA will provide an affordable and effective alternative to existing contractual dispute resolution options between consumers and small business and their telecommunication and media services providers, administered by the Singapore Mediation Centre The ADR scheme will primarily cover disputes relating to billing and unsolicited charges (such as excess data or Value Added Service charges) up to a maximum dispute value of SGD10,000. However, the ADR scheme will not include cases relating to litigation, regulatory policies, service providers' commercial decisions including their range of services offered and pricing of services. Services covered by the ADR scheme include mobile services, fibre connection services, subscription TV services. Participation in the ADR scheme will be mandatory for such providers. However, the ADR scheme excludes services that are: • Less pervasive • Infrequently used • Not licensed by IMDA such as billing on behalf of services, App store purchases and Over the Top media streaming services.
Timeline	ADR scheme expected to be launched in April 2022.
DPE programme	The Personal Data Protection Commission and IMDA will commence the DPE programming comprising: • Security solutions • DPE checklists • A one-time set-up service to assist SMEs in acquiring basic level data protection and security practices to protect their customers' personal data and recover quickly in the event of a data breach through service providers registered with IMDA. Businesses that have good cybersecurity practices will also be recognised through the Cyber Trust Mark and Cyber Essentials Mark
Timeline	Available from 1 April 2022.
Sustainable data centres	Recognising the continued need to build sustainable digital infrastructure for the next wave of digitalisation, IMDA and the Economic Development Board will pilot a Call for Application to construct 'green' data centres that also fulfil Singapore's environmental obligations under the 2015 Paris Agreement. Applications will be assessed based on the use of best-in-class techniques, technologies and practices for energy efficiency and decarbonisation.
Timeline	The Call for Application will be launched by the second quarter of 2022.

Sources:

Speech by Josephine Teo, Minister of Communications and Information, at the Ministry of Communications and Information Committee of Supply Debate on 4 March 2022

Speech by Tan Kiat How, Minister of State, Ministry of Communications and Information, at the Ministry of Communications and Information Committee of Supply Debate on 4 March 2022

Speech by Janil Puthucheary, Senior Minister of State, Ministry of Communications and Information, at the Ministry of Communications and Information Committee of Supply Debate on 4 March 2022

The Ministry of Communications and Information (MCI) unveils initiatives to help Singaporeans and businesses thrive securely in an increasingly digital world

CSA Media Factsheet: Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CIIs

Contact Us

Andy Leck
Principal
Andy.Leck@bakermckenzie.com

Ken Chia
Principal
Ken.Chia@bakermckenzie.com