Baker McKenzie Wong & Leow.

Information Technology & Communications
Singapore

Client Alert
July 2017

# Singapore Government issues Public Consultation on draft Cybersecurity Bill


**For more information, please contact:**

Ken Chia
Principal
+65 6434 2558
Ken.Chia
@bakermckenzie.com

Seng Yi Lin
Local Principal
+65 6434 2713
YiLin.Seng
@bakermckenzie.com


## Executive summary

The long-awaited draft Cybersecurity Bill ("**draft Bill**") has been issued for public consultation by the Ministry of Communications and Information (MCI) and the Cyber Security Agency of Singapore (CSA) on 10 July 2017. The draft Bill and the public consultation document are available here.

In light of the growing cybersecurity threats globally, the draft Bill seeks to, amongst others, provide and maintain a framework for national cybersecurity as well as ensure that critical information infrastructure is protected against such threats. The provision of certain investigative and non-investigative cybersecurity services will also now be regulated under the draft Bill.

We explore some of the key highlights of the draft Bill below.

## Highlights of draft Bill

- Commissioner of Cybersecurity to be appointed

The Commissioner of Cybersecurity (the "**Commissioner**") may be appointed by the Minister of Communications and Information (the "**Minister**"), along with a Deputy Commissioner and Assistant Commissioners of Cybersecurity as may be deemed fit by the Minister. Apart from advising the Government in respect of cybersecurity matters as well as monitoring cybersecurity threats or cybersecurity incidents that may threaten Singapore's national security, the Commissioner is also responsible for identifying and designating Critical Information Infrastructure ("**CII**") and establishing cybersecurity codes of practice and standards of performance for CII owners to comply with. The Commissioner is also to cooperate with Computer Emergency Response Teams ("**CERTs**") internationally on cybersecurity incidents.

- Designating critical information infrastructure

The draft Bill provides that the Commissioner may, by written notice, designate a computer or computer system as a CII[1] if it fulfils the relevant criteria and the computer or computer system is located wholly or partly in Singapore.

[1] The term CII is defined as a computer or computer system that is necessary for the continuous delivery of essential services which Singapore relies on, the loss or compromise of which will lead to a debilitating impact on the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore. The term "essential services" is set out in the First Schedule covering forty [one] services relating to key sectors such as energy, info-communications, water, healthcare, banking and finance, security and emergency services, aviation, land transport, maritime, media and the Government.

This requires the Commissioner to, amongst others, identify the specific computer or computer system that is being designated as CII, as well as identify the owner of the CII regarding his duties and responsibilities under the proposed Cybersecurity Act that arise from the designation. Such designation will take effect of 5 years unless withdrawn earlier by the Commissioner. Such withdrawal may take place if the Commissioner is of the opinion that the computer or computer system no longer fulfils the criteria of a CII.

If an owner of a CII is aggrieved by such decision of the Commissioner to designate a computer or computer system as CII, the owner may appeal to the Minister within 30 days of such decision.

Critically, where the Commissioner has reason to suspect that a computer or computer system may fulfil the criteria of a CII, the Commissioner has the power to obtain information from any person who appears to be operating the computer or computer system information to such computer or computer system. Such information request may include information relating to the persons who are served by the computer or computer system as well as technical information and specific functions of the computer or computer system.

- Duties imposed on owners of CII

The draft Bill imposes certain duties on owners of CII. The Commissioner has the power to request the owner of CII to provide information on the design, configuration and security of the CII as well as any other computer or computer system that it communicates with. Further, if material changes are made to the design, configuration or operation of the CII after such information has been furnished, the owner must notify the Commissioner of such changes within 30 days of the change. The term "material change" refers to a change which affects or may potentially affect the cybersecurity of the CII or the ability of the owner to respond to a cybersecurity incident affecting the CII.

An owner of CII must also comply with relevant codes of practice and standards of performance as may be issued by the Commissioner. However such code or standard is not intended to have any legislative effect.

An owner of CII must also notify the Commissioner of certain cybersecurity incidents. This includes any significant cybersecurity incident that occurs in respect of the CII or any computer or computer system under the owner's control that is interconnected with or communicates with the CII. A CII owner must therefore establish mechanisms and processes in order to detect any cybersecurity threat in respect of its CII.

Further, regular risk assessments and audits are expected to be undertaken every 3 years, with such audit or assessment report to be furnished to the Commissioner within 30 days of the completion of the audit or risk assessment.

An owner of CII is also expected to participate in national cybersecurity exercises.

- Notification of change in ownership of CII

An owner of CII must inform the Commissioner of any intended change in ownership of the CII not later than 90 days before the date of the intended change in ownership.

- Powers of investigation and emergency cybersecurity measures

The Commissioner has broad powers of investigation in the event it receives information regarding a cybersecurity threat. Where such incident or threat satisfies a specified severity threshold (e.g. where it creates a real risk of significant harm to CII), the Commissioner may direct any person to carry out certain remedial measures (e.g. installation of software updates or temporarily disconnect infected computers from a network) in relation to a computer or computer system in order to minimize cybersecurity vulnerabilities. Notably, this includes "allowing the investigating officer to install on the computer or computer system any software program, or interconnect any equipment to the computer or computer system, for the purpose of the investigation".

In the case of emergency cybersecurity incidents, for example to counter any threat to national security, the Minister may take any relevant measures necessary to prevent, detect or counter any threat to a computer or computer system.

- Regulation of licensable cybersecurity services

Persons carrying out any licensable cybersecurity services for reward (i.e. any licensable investigative cybersecurity service or licensable non-investigative cybersecurity service) will need to obtain a licence under the draft Bill. Such licensable cybersecurity services have been specified in the Second Schedule, with the following being designated: penetration testing service as a licensable investigative cybersecurity service; and managed security operations centre (SOC) monitoring service as a licensable non-investigative cybersecurity service. There will be new record keeping obligations imposed on such licensed cybersecurity service providers.

## What is not known

There are crucial pieces which are yet to be known, in particular what will be "significant cybersecurity incidents" which need to be reported, the technical standards expected to be maintained, and what the threshold for a "debilitating impact" will be. The draft Bill provides that the Minister may issue regulations ("**Regulations**") covering, *inter alia*:

a) the process for the designation of a CII;

b) the technical or other standards to be maintained by an owner of a CII;

c) the responsibilities and duties of an owner of a CII;

d) the type of changes that are considered material changes to the design, configuration, security or operations of a CII to be reported by an owner of a CII;

e) the type of cybersecurity incidents that are considered significant cybersecurity incidents in respect of a CII to be reported by an owner of a CII;

f) the requirements and manner of cybersecurity audits and cybersecurity risk assessments to be conducted by an owner of a CII; and

g) the form and nature of cybersecurity exercises that may be conducted.

It would be helpful if the draft Regulations could be issued in the next round of public consultations as these would be important to fully understand how the new Cybersecurity Act would impact organisations.

Further, any owners of CII will need to notify the Commissioner in respect of any potential ownership change at least 90 days prior to the date of intended change in ownership. As there is no definition of "ownership", it is not clear what would amount to a "change of ownership" requiring such notification. Clarity may be required as to how this provision may apply to, for example, publicly-listed companies which have been designated as CII. Nonetheless, whilst this is not an approval requirement, such organisations will need to keep this notification requirement in mind for any potential mergers, acquisitions or shareholder changes.

Interestingly, it does not appear that privacy breaches which cause "serious harm to any of the individuals to whom the information relates" (as in Australia) is likely to be one of the criteria to determine whether a cybersecurity incident is serious enough to warrant an investigation unless it can be considered in assessing the "value of information put at risk" under Section 21(2) of the draft Bill. The overlap between this cybersecurity regime and the Protection Obligation under the Personal Data Protection Act will also need to be examined further.

## How this may affect you

Organisations which have computers or computer systems necessary for the continuous delivery of essential services which Singapore relies on may potentially be designated as CII. The Bill covers not only traditional IT systems but also "an operational technology system such as an industrial control system (ICS), a programmable logic controller (PLC), a supervisory control and data acquisition (SCADA) system, or a distributed control system (DCS)", which could cover new "Internet of Things" technology.

If designated as CII, there are a number of duties imposed on owners of such CII which organisations would need to be prepared to comply with, as highlighted above. For example, organisations providing licensable cybersecurity services as specified under the Second Schedule will need to be prepared to comply with the new licensing regime instituted under the draft Bill. This includes ensuring that relevant employees hired as investigative cybersecurity service practitioners are also licensed accordingly.

The above measures are part of the draft Bill which is open to public consultation. Should you wish to provide feedback to the consultation, this should be done by 3 August 2017 in accordance with the submission instructions provided.

**www.bakermckenzie.com**

Baker McKenzie Wong & Leow
8 Marina Boulevard
#05-01 Marina Bay Financial Centre
Tower 1
Singapore 018981

Tel: +65 6338 1888
Fax: +65 6337 5100