Singapore: The latest step in cyber security strategy

On 5 February 2018, Singapore passed the Cybersecurity Bill No. 2/2018 (‘the Bill’), a draft of which had previously been issued for public consultation on 10 July 2017. The Bill, which was sponsored by the Cyber Security Agency of Singapore (‘CSA’) and the Singapore Ministry of Communications and Information (‘MCI’), significantly strengthens the regulation of critical information infrastructure (‘CII’) in Singapore and creates a new Commissioner of Cybersecurity (‘the Commissioner’) with significant authority to investigate cyber security incidents in Singapore. In this article, Yuet Ming Tham, Partner at Sidley Austin LLP, analyses the progression and implications of the Bill, in terms of its focus on CII and duties of the new Commissioner.

The Bill is only the latest step in the evolution of Singapore’s cyber security strategy. In April 2015, Singapore established the CSA. In October 2016, the Government issued a report on Singapore’s cyber security strategy (‘the Report’), which emphasised the need to safeguard CII, noting that attacks on CII could not only disrupt essential services for the country’s own residents, but also have significant spillover effects regionally and globally.

The Report further underscored the need for close cooperation between the Government, CII operators, and the cyber security community in order to effectively prepare for and address such threats. Before the passage of the Bill, the Government noted that although existing laws guarded against certain cyber security threats, and certain sectors already had their own regulations in place, Singapore did not have a harmonised national framework that would provide generalised protections across all CII sectors. The Bill:

• addresses the regulation of CII;
• creates the Commissioner, which has with significant powers to prevent and respond to cyber security incidents in Singapore, not only those related to CII; and
• sets up a licensing scheme for providers of certain cyber security services.

Regulation of CII

CII is defined as computer systems, located at least partly within Singapore, that are necessary for the continuous delivery of an essential service such that the loss of a system would have a debilitating effect on the availability of the essential service in Singapore\(^2\). Essential services are defined as services in the following 11 sectors: government, security and emergency services, healthcare, telecommunications, banking and finance, energy, water, media, land transport, aviation, and maritime\(^2\), however, the MCI may amend the list of sectors at a later date.

The Bill does not require systems operators to determine for themselves whether their systems qualify as CII. Rather, the Commissioner will designate those systems that qualify as CII. In aid of such determinations, the Commissioner may request any person exercising control over a computer system to provide it with information necessary for the Commissioner to determine whether the system qualifies as CII.

When the Commissioner designates a system as CII, it will notify the legal owner(s) of the system, in writing, of their duties to comply with the Bill’s requirements governing CII, and such designation will be effective for five years unless withdrawn by the Commissioner. The legal owner of a system receiving such notification may inform the Commissioner if the owner is not in actual control of the system or is otherwise unable to ensure compliance, in which case the Commissioner may amend its notice to specify the party that is in a position to comply. Furthermore, a CII owner that believes its system has been inappropriately designated as CII may appeal against the Commissioner’s designation.

An owner/operator of a system that has been designated as CII must:

• comply with any codes of practice and standards of performance promulgated by the Commissioner;
• comply with written directions of the Commissioner;
• report to the Commissioner certain prescribed incidents in respect of the CII or any system under the owner’s control that is interconnected or communicates with the CII;
• establish mechanisms and processes for detecting cyber security threats and incidents as set out in any applicable code of practice;
• report any material change to the design, configuration, security, or operation of the CII within 30 days after the change is made;
• inform the Commissioner of any change in the beneficial or legal ownership (including any share in such ownership) of the CII;
A significant area of uncertainty is how broadly the Commissioner will seek to apply the CII provisions. If the Commissioner defines CII too broadly, that may impose needless burdens on system owners without a significant offsetting benefit to cyber security in Singapore.
A cyber security incident or threat, an

Furthermore, in the case of a serious

•

may, among other things:

its authority, the Commissioner

CSA in investigation of cyber security

operator CII, must cooperate with the

organisation, even if it does not own or

broad authority to monitor and respond

The Bill grants the Commissioner

Beyond CII operators

The Bill grants the Commissioner

organisation, even if it does not own or

operate CII, must cooperate with the

CSA in investigation of cyber security

threats and incidents. In exercising

its authority, the Commissioner

may, among other things:

A person who receives a notice

from the Commissioner and fails to

respond, or who fails to make a

required report to the Commissioner,

may be guilty of an offence.

Beyond CII operators

The Bill grants the Commissioner

broad authority to monitor and respond
to cyber security incidents. Any

organisation, even if it does not own or

operate CII, must cooperate with the

CSA in investigation of cyber security

threats and incidents. In exercising

its authority, the Commissioner

may, among other things:

• require any person to attend

a meeting to answer any

questions, or to provide a signed

statement, concerning a cyber

security threat or incident;

• require any person to produce

any physical or electronic record

or document, or provide any

information, related to any matter

relevant to an investigation; and

• orally examine any person who

appears to be acquainted with facts

and circumstances relating to a

cyber security threat or incident.

Furthermore, in the case of a serious

cyber security incident or threat, an

organisation may be required to:

• carry out such remedial measures,

or cease carrying on such activities,

as the Commissioner may direct

in relation to a system that may be

affected by the cyber security incident;

• preserve the state of a

system by not using it;

• monitor a computer system for

a specified period of time;

• perform a scan of a computer system

to detect cyber security vulnerabilities;

• allow the investigating officer to

connect any equipment to a system

or install any software program as

is necessary for the investigation;

• allow an investigating officer to enter

any premises that the investigating

officer suspects may contain a system

affected by the cyber security incident;

• take a copy of, or extracts from, any

electronic record or program contained

in a computer that the investigating

officer has reasonable cause to suspect

is impacted by the incident; and

• with the consent of the owner, take

possession of any computer or other

equipment for the purpose of carrying

out further examination and analysis.

Finally, the Cybersecurity Bill

establishes a licensing regime for
certain providers of cyber security

services, even if they do not themselves

maintain CII. The licensable cyber

security services, set forth in the

Second Schedule to the Bill, are:

1. services that monitor the cyber

security level of other persons’

computers or systems, and

2. services that assess, test or evaluate

the cyber security level of other

persons’ computers or systems

by searching for vulnerabilities

in, and compromising, the

defences of such systems.

Any person who provides a licensable

cyber security service without a

license is guilty of an offense, and an

unlicensed person may not bring any

proceeding to recover any unpaid fees

from its customers in connection with

such service. Furthermore, licensees

must keep records of information

concerning their engagements to

provide cyber security services,

including the names and addresses

of persons who engage the service

provider to provide cyber security

services, the names of the persons who

provided the services, and details of

the services provided. The licensing

requirements do not apply, however, to

companies that provide cyber security

services to their related companies,
as defined under the Companies

Act (Chapter 50), Act 42 of 1967.

A significant area of uncertainty is how

broadly the Commissioner will seek

to apply the Bill’s CII provisions. If the

Commissioner defines CII too broadly,

that may impose needless burdens on

system owners without a significant

offsetting benefit to cyber security in

Singapore. Additionally, the contours of

what the Commissioner may consider

“serious” cyber security incidents

justifying the exercise of its broad

investigative powers remain unclear.

Given these uncertainties, all companies—

not just potential CII operators—should

closely monitor any implementing

regulations, codes and standards that

the Commissioner may promulgate,
as these will hopefully provide further

guidance on the Government’s

enforcement priorities going forward.

This article has been prepared for

informational purposes only and
does not constitute legal advice. This

information is not intended to create,

and the receipt of it does not constitute,
a lawyer-client relationship. Readers

should not act upon this without

seeking advice from professional

advisers. The content therein does

not reflect the views of the firm.