Allen&Gledhill

Publication Date:
31 January 2018

Main Contact:
Dr Stanley Lai, SC
+65 6890 7883
stanley.lai@allenandgledhill.com

Parliament introduces Cybersecurity Bill to protect critical information infrastructure against cybersecurity threats

On 8 January 2018, the Cybersecurity Bill ("**Bill**") was tabled in Parliament for first reading. The Bill seeks to establish a framework for the protection of critical information infrastructure ("**CII**") against cybersecurity threats, the taking of measures to prevent, manage and respond to cybersecurity threats and incidents in Singapore, and the regulation of providers of licensable cybersecurity services.

Key features of the Cybersecurity Bill

- Commissioner of Cybersecurity administers the Bill
- Commissioner designates CII for five years
- Essential services defined and include services relating to banking and finance, energy and info-communications
- CII owner refers to legal owner and includes joint owner
- Permanent Secretary is owner of CII owned by the Government
- Notice of designation sent to person with effective control of the CII
- CII owners have various statutory duties which include notifying change in ownership, conducting audits and cybersecurity risk assessment
- Commissioner determines appropriate response to cybersecurity threats and incidents based on level of severity
- Only managed security operations centre (SOC) monitoring service and penetration testing service are prescribed as licensable cybersecurity services

Set out below are the key features proposed in the Bill.

1. Commissioner of Cybersecurity administers the Bill

The powers of the Bill will be vested in a Commissioner of Cybersecurity ("**Commissioner**") to be appointed by the Minister-in-charge of Cybersecurity ("**Minister**"). The Minister may appoint a Deputy Commissioner, as well as a number of Assistant Commissioners to assist the Commissioner in the discharge of his duties and functions. An Assistant Commissioner may be a public officer of another Ministry or employee of a statutory board under the charge of another Ministry where that other Ministry or statutory board has supervisory or regulatory responsibility over an industry or a sector to which the owner of the CII belongs. The Commissioner may also appoint public officers as cybersecurity officers.

Allen & Gledhill LLP
One Marina Boulevard #28-00
Singapore 018989
T +65 6890 7188
F +65 6327 3800
E enquiries@allenandgledhill.com

2. Commissioner designates CII for five years

The Commissioner is empowered to designate a computer or computer system as a CII if the Commissioner is satisfied that the computer or computer system is:

a. located wholly or partly in Singapore; and

b. necessary for the continuous delivery of an essential service and its loss or compromise will have a debilitating effect on the availability of the essential service in Singapore.

The designation has effect for a period of five years unless it is withdrawn by the Commissioner before the expiry of the period.

3. Essential services defined and include services relating to banking and finance, energy and info-communications

An essential service means any service essential to the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore, and specified in the First Schedule to the Bill. The list of essential services in the First Schedule includes services relating to banking and finance, energy, info-communications, water, healthcare, security and emergency services, aviation, land transport, maritime and media.

4. CII owner refers to legal owner and includes joint owner

An "owner" in relation to a CII means the legal owner of the CII and, where the CII is jointly owned by more than one person, includes every joint owner.

5. Permanent Secretary is owner of CII owned by the Government

Where a CII is owned by the Government and operated by a Ministry, the Permanent Secretary allocated to the Ministry who has responsibility for the CII is treated as the owner of the CII.

6. Notice of designation sent to person with effective control of the CII

Under the Bill, the Commissioner designates a computer or computer system as a CII via written notice to the owner of the computer or computer system.

However, the person who receives such notice of designation ("**Recipient**") may request the Commissioner to amend the notice and address it to another person who has effective control over the CII ("**Controller**"), by showing proof that the Recipient is not able to comply with the relevant requirements under the Bill because the Recipient has neither effective control over the operations of the computer or computer system nor the ability or right to carry out changes to the same, and the Controller has such effective control and ability and right. If the Commissioner addresses and sends an amended notice to the Controller, the Controller will be subject to the requirements under Part 3 of the Bill during the period when the notice is in effect, as if the Controller were the owner.

7. CII owners have various statutory duties which include notifying change in ownership, conducting audits and cybersecurity risk assessment

CII owners have various statutory duties under Part 3 of the Bill which include:

- providing the Commissioner with information relating to the CII;
- complying with codes of practice, standards of performance or written directions in relation to the CII as may be issued by the Commissioner;
- notifying the Commissioner of any change in ownership of the CII not later than seven days after the change in ownership;
- notifying the Commissioner of any prescribed cybersecurity incidents relating to the CII;
- conducting regular audits of the compliance of the CII by an auditor approved or appointed by the Commissioner at least once every two years (or more frequently as directed by the Commissioner in any particular case);
- conducting a cybersecurity risk assessment of the CII at least once a year; and
- participating in cybersecurity exercises if so directed by the Commissioner.

Generally, non-compliance with the statutory duties without reasonable excuse is a criminal offence which attracts a fine and/or imprisonment.

8. Commissioner determines appropriate response to cybersecurity threats and incidents based on level of severity

The Bill empowers the Commissioner to respond to a cybersecurity threat or incident by exercising, or authorising the exercise of investigatory powers depending on the severity of the cybersecurity threat or incident. The Bill also empowers the Minister to authorise the taking of emergency cybersecurity measures.

9. Only managed security operations centre (SOC) monitoring service and penetration testing service are prescribed as licensable cybersecurity services

The Bill prescribes two licensable cybersecurity services for the purposes of the Bill:

- managed security operations centre (SOC) monitoring service; and
- penetration testing service.

Background

On 13 November 2017, the Ministry of Communications and Information ("**MCI**") and the Cyber Security Agency of Singapore ("**CSA**") released a joint press release and a full report setting out their response in specific areas following feedback received from a six-week joint public consultation exercise on the proposed Bill in July and August 2017. An article about the response issued by MCI and CSA was featured in a previous issue of the Allen & Gledhill Legal Bulletin (November 2017). To read the article entitled "*MCI and CSA respond to feedback received on proposed Cybersecurity Bill*", please click **here**.

Reference materials

The Cybersecurity Bill is available from the Parliament website www.parliament.gov.sg. To access the Cybersecurity Bill, please click **here**.

For further information, please contact:

Dr Stanley Lai, SC
+65 6890 7883
stanley.lai@allenandgledhill.com

Adrian Ang
+65 6890 7710
adrian.ang@allenandgledhill.com

Aaron Lee
+65 6890 7852
aaron.lee@allenandgledhill.com

Tan Wee Meng
+65 6890 7518
tan.weemeng@allenandgledhill.com

Tham Kok Leong
+65 6890 7526
tham.kokleong@allenandgledhill.com

Alexander Yap
+65 6890 7627
alexander.yap@allenandgledhill.com