SINGAPORE'S CYBERSECURITY BILL – RESPONSE TO PUBLIC FEEDBACK

On 10 July 2017, the Singapore Ministry of Communications and Information (MCI) and the Cyber Security Agency of Singapore (CSA) jointly released a draft Cybersecurity Bill (Bill) for public consultation and feedback. A report summarising industry feedback on the Bill and providing clarification and proposed changes was released on 13 November 2017.

Key highlights

- The MCI/CSA have clarified and changed areas of the Bill.
- Potential CII owners will be engaged before formal designation.
- CII designations will not be official secrets.
- CII owners must inform the cybersecurity Commissioner of any ownership change within seven days.
- The scope of licensing for cybersecurity service providers will be narrow. The focus will be on providers of penetration testing and managed security operations centre monitoring services. In-house provision of cybersecurity services will be exempted.

BACKGROUND

On 10 July 2017, the MCI and CSA released the Bill for public consultation. Due to public requests, the consultation period was extended. As we have previously discussed in our client briefing of July 2017, this Bill seeks to establish an omnibus cybersecurity law in Singapore.

Ninety-two submissions were received by the MCI/CSA. This includes a joint submission – by Clifford Chance, the International Swaps and Derivatives Association, the Asia Securities Industry & Financial Markets Association and the Futures Industry Association – covering a number of issues, many of which appear to have been taken up, in varying degrees, by the MCI/CSA.

The report provides welcome clarification on a number of issues and directly addresses the view that the proposed requirements could be onerous. The clarifications are clearly geared towards assuring organisations that the costs of compliance would be kept to a minimum.

Although the form and scheme of the original proposal are largely intact, the key clarifications and changes include:

- confirmation that owners of any potential critical information infrastructure (CII) will be approached before they are formally designated;
- removal of the classification of CII designation as an official secret;
- streamlining and harmonising the Bill with respective sectoral requirements;
- revision of the Bill to make clear that CII owners will be required to establish reasonable mechanisms and processes to detect cyber threats; and
- keeping the scope of the licencing framework for cybersecurity providers narrow.

DESIGNATION AND IDENTIFICATION OF CIIs

The MCI/CSA stated that they have already approached potential CII owners and that it will be the MCI/CSA's policy to engage with any new potential CII owners before they are formally designated. The MCI/CSA also clarified that computers and computer systems located wholly overseas will not be designated as CIIs and that CII designations will no longer be official secrets under the Official Secrets Act.

In addition, the MCI/SCA highlighted that the CII owner will be the entity (or entities) which has effective control over or is responsible for the CII, which would usually be the legal owner of the CII asset.

What are the critical information infrastructure sectors?

Aviation
Banking and finance
Energy
Government
Healthcare
Land transport
Media
Maritime
Security and emergency
Infocomms
Water

COMPLIANCE AND DISCLOSURE

Recognising the time required to comply with the Bill, the MCI/CSA will provide a grace period which will be determined in consultation with the Assistant Commissioners appointed by the sector regulators. The CSA will also implement on-boarding programmes to assist CII owners.

Other initiatives to help with compliance, include:

- streamlining and harmonising obligations of CII owners with their respective sectoral obligations;
- revising the standard in the Bill to require instead "reasonable" mechanisms and processes for cyber risks detection; and
- introducing additional guidelines on the reporting of cybersecurity incidents for CII owners, including specific reporting thresholds.

The consultation draft had included a requirement for audit and risk assessments at least every three years. In response to comments that this was inadequate given the pace of technological change, the MCI/CSA are considering increasing the frequency and providing flexibility in requirements based on sector needs.

CONTROL AND OWNERSHIP OF CII

Market participants should also be aware of the change of control reporting requirements of the Bill. The consultation draft required a CII owner to give the cybersecurity Commissioner notice of an intended change of control 90 days in advance. Noting the practical issues this might cause, the new requirement is that, not later than seven days after the change of control, the CII owner(s) must inform the Commission.

With CII assets often being under the control of third party vendors, CII owners need to review carefully their contractual arrangements. The Bill does not extend direct responsibility to third party vendors, and makes CII owners ultimately responsible. CII owners should therefore ensure that appropriate cybersecurity requirements are imposed on third party vendors. In some situations there may be more than one legal owner of the CII asset – CII owners should be aware that all legal owners need to be identified to the Commissioner.

LICENCE FRAMEWORK

The initial licence framework proposed by the MCI/CSA captured both penetration testing and managed security operations centre (SOC) monitoring services providers, while exempting in-house providers of those services. A number of respondents expressed reservations about licensing in any form, particularly how it might affect the broader pool of cybersecurity service providers, such as cybersecurity risk assessment and audit services.

The MCI/CSA, taking those views on board, will keep the licence framework narrowly scoped to penetration testing and managed SOC monitoring service providers only whilst promoting a voluntary accreditation scheme for other cybersecurity service providers.

This is positive news for other cybersecurity service providers seeking to grow their businesses and for the industry at large. For users of these services, given the mainstream adoption of the services to be licensed, the new framework will provide helpful certainty of quality and reliability while voluntary accreditation schemes provide companies with a useful barometer for assessing newer cybersecurity products and services.

RESPONSE TO CYBERSECURITY THREATS AND INCIDENTS

In direct response to comments that there should be safeguards to the powers of the cybersecurity Commissioner to investigate cybersecurity threats, the MCI/CSA have stated that such powers are calibrated depending on the severity of the threat or incident.

Assurances were also provided for cooperation, including that (i) information provided would be marked as confidential and treated with care and (ii) indemnities will be provided for compliance with information disclosure obligations. Notably, the MCI/CSA have stated that their intention is to indemnify persons who, in good faith as required under the Bill, disclose information.

WHAT NEXT?

The final Cybersecurity Bill will not be introduced to Parliament until early 2018 and will continue to be refined. The Bill, if passed, will come into force a few months after its passage so as to allow time for subsidiary legislation to be finalised.

However, the licence framework will not take immediate effect after the Bill's enactment. The CSA intends to undertake further consultation on the detailed requirements before putting the framework in place.

With the clarifications and proposed revisions to the Bill, the MCI/CSA have struck a sound balance between safeguarding national cybersecurity and associated compliance costs.

Clifford Chance will be holding a series of closed door sector roundtables in the first quarter of 2018 in Singapore. Please reach out to your usual Clifford Chance contacts if you or your Chief Information Security Officer is interested in joining us.

Read our other publications

- Talking Tech – the new Clifford Chance technology website.
- New Singapore Cybersecurity Bill released for public consultation (July 2017)
- New PRC cyber-security law comes into force (July 2017)
- NY DFS Cybersecurity Rules Take Effect (July 2017)
- The fintech market in Asia Pacific (September 2017)

CONTACTS

Paul Landless
Partner

T + 65 6410 2235
M + 65 9126 8871
E paul.landless
@cliffordchance.com

Luke Grubb
Partner

T + 65 6506 2780
M + 65 8233 2954
E luke.grubb
@cliffordchance.com

Lena Ng
Partner

T + 65 6410 2215
M + 65 8126 0729
E lena.ng
@cliffordchance.com

Nish Shetty
Partner

T + 65 6410 2285
M + 65 8128 7412
E nish.shetty
@cliffordchance.com

Lijun Chui
Senior Associate

T + 65 6506 2752
M + 65 9128 4122
E lijun.chui
@cliffordchance.com

James Kwong
Trainee Solicitor

T + 65 6506 1984
M + 65 9620 5743
E james.kwong
@cliffordchance.com

www.cliffordchance.com

Clifford Chance Pte Ltd, 12 Marina Boulevard, 25th Floor Tower 3,

Marina Bay Financial Centre, Singapore 018982