Shearn Delamore &co.

Malaysia's Cyber Security Bill 2024 Passed: Navigating Malaysia's New Compliance Standards and Licensing Framework

Introduction

In Malaysia, the Cyber Security Bill 2024 (the "**Proposed Act**") was passed in Parliament, after the third reading by Digital Minister Gobind Singh Deo on 3 April 2024. The primary objective of the Proposed Act is to establish an overarching regulatory framework designed to fortify national cyber security by requiring compliance with specific measures, standards and processes in the management of the cyber security threats. For these purposes, the regulatory framework introduces various provisions relating to, among others, the establishment of the National Cyber Security Committee, the duties and powers of the Chief Executive of the National Cyber Security Agency ("**NACSA**"), national critical information infrastructure sectors ("**NCII Sectors**"), the appointment of sector leads to regulate each national critical information infrastructure sectors ("**NCII Sector Leads**"), the designation of national critical information infrastructure entities ("**NCII Entities**") as well as licensing requirements for cyber security service providers[1].

Will my business or organisation be subject to the new law?

Private and public entities (i.e. including private businesses) that are designated as NCII Entities and cyber security service providers (as will be discussed below) will be expected to comply with the regulatory requirements under the Proposed Act once it comes into force.

Therefore, this article aims to offer an overview of these key provisions of the Proposed Act which businesses and relevant sectors should consider in preparation for the enactment of the forthcoming legislation although the Proposed Act will still be subject to royal assent by the Yang di-Pertuan Agong.

Technology, Media & Telco Update

APRIL 2024

Shearn Delamore & Co
7th Floor
Wisma Hamzah Kwong-Hing,
No 1, Leboh Ampang
50100, Kuala Lumpur, Malaysia
T: 603 2027 2727
F: 603 2078 5625
info@shearndelamore.com
www.shearndelamore.com
www.linkedin.com/company/shearn-delamore-&-co

Extra-territorial application

Further, the Proposed Act is intended to have extra-territorial application. It shall apply to any person, irrespective of nationality or citizenship, and shall have effect outside as well as within Malaysia if the offence committed under the Proposed Act pertains to a national critical information infrastructure ("**NCII**") that is wholly or partly in Malaysia[2].

It should therefore be noted that foreign businesses may potentially be subject to the Proposed Act where it relates to NCIIs that are wholly or partly in Malaysia.

What are my next steps before the legislation comes into force?

In anticipation of the Proposed Act coming into force, potential entities mentioned above that may be subject to the Proposed Act should adopt proactive measures such as commencing reviews and audits of their cyber security-related policies, procedures and operations including with their third-party service providers to enable them to be better prepared for compliance with the Proposed Act.

(a) Definition of "national critical information infrastructure"

One of the main focuses of the Proposed Act is the regulation of NCII Entities. The definition of NCII is a "*computer or computer system which the disruption to or destruction of the computer or computer system would have a detrimental impact on the delivery of any service essential to the security, defence, foreign relations, economy, public health, public safety or public order of Malaysia, or on the ability of the Federal Government or any of the State Governments to carry out its functions effectively*"[3].

The NCII Sectors identified under the Schedule of the Proposed Act are:

- government;
- banking and finance;
- transportation;
- defence and national security;
- information, communication and digital;
- healthcare services;
- water sewerage and waste management;
- energy;
- agriculture and plantation;
- trade, industry and economy; and
- science, technology and innovation.

(b) Appointment of NCII Sector Leads and designation of NCII Entities

Each NCII Sector may have one or more NCII Sector Leads which will be appointed by the Minister responsible for cyber security at the recommendation of the Chief Executive. The NCII Sector Leads will be responsible for, among others, (i) designating any government entity or person as an NCII Entity which owns or operates an NCII in respect of its appointed sector, (ii) preparing a code of practice containing measures, standards and processes in ensuring the cyber security of an NCII within the NCII Sector for which it is appointed ("**Code of Practice**"), and (iii) monitoring and ensuring that actions required of and duties imposed on the NCII Entities under the Proposed Act are carried out by the NCII Entities.

Businesses or stakeholders operating within an NCII Sector designated as an NCII Entity will be obligated to adhere to certain duties (covered in more detail below). Notably, an NCII Sector Lead itself may also be designated as an NCII Entity by the Chief Executive of NACSA in a similar manner as businesses operating in NCII Sectors.

(c) Governing authorities

National Cyber Security Committee

The National Cyber Security Committee ("**Committee**") will be established under the Proposed Act. The Committee will consist of 14 members across various ministries, including the Prime Minister of Malaysia who shall be the chairman[4], and the Chief Executive of NACSA ("**Chief Executive**") who shall be the secretary to the Committee[5].

The Committee's main function will include, but not be limited to, overseeing the effective implementation of the Proposed Act when it comes into force, advising and making recommendations to the Federal Government on policies and measures to strengthen national cyber security and giving directions to the Chief Executive and NCII Sector Leads on matters relating to national cyber security[6].

Chief Executive

The Proposed Act empowers the Chief Executive to among others, advise and make recommendations to the Committee[7], implement policies made and directions given by the Committee or the Federal Government[8], coordinate and monitor the implementation of such policies by the NCII Sector Leads and NCII Entities[9], collect and evaluate data, information or intelligence relating to national cyber security and to disseminate them if it thinks it is essential to do so in the interests of national cyber security[10], and issue directives which it considers necessary for the purposes of ensuring compliance with the Proposed Act ("**Directives**")[11]. The Chief Executive is also responsible for maintaining a national cyber security system known as the "*National Cyber Coordination and Command Centre System*" for the purpose of dealing with cyber security threats and cyber security incidents[12].

(d) Duties of NCII Entities

The Proposed Act imposes various duties on public and private entities that own or operate NCIIs, including:

(i) implementing the measures, standards and processes as specified in the Code of Practice for the purpose of ensuring the cyber security of its NCII. There are two notable points regarding this:

- notwithstanding this duty, any alternative and additional measures, standards and processes may be implemented if the NCII Entity may prove to the satisfaction of the Chief Executive that they can provide equal or higher level of protection to its NCII; and

- NCII Entities may, in addition to the aforementioned measures, standards and processes, establish and implement measures, standards and processes based on internationally recognised standards or framework[13];

(ii) providing information relating to its NCII requested by its NCII Sector Lead[14];

(iii) conducting cyber security risk assessments in accordance with the Code of Practice and Directives[15];

(iv) causing to be carried out a cyber security audit by an auditor approved by the Chief Executive to determine the compliance of the NCII Entity with the Proposed Act[16];

(v) notifying the Chief Executive and its NCII Sector Lead of any cyber security incident which has or might have occurred in respect of its NCII[17]. The Proposed Act defines a cyber security incident as "*an act or activity carried out on or through a computer or computer system, without lawful authority, that jeopardizes or adversely affects the cyber security of that computer or computer system or another computer or computer system*" (emphasis added); and

(vi) carrying out the directions given by the Chief Executive for cyber security exercises conducted by the Chief Executive for the purpose of assessing the readiness of an NCII Entity in responding to any cyber security threat or cyber security incident[18].

Non-compliance with the aforementioned duties will constitute offences under the Proposed Act which may result in fines or imprisonment, or both.

(e) Licensing of cyber security service providers

Aside from the regulation of NCII Entities, the Proposed Act provides for the licensing of cyber security service providers. However, the types of services constituting "*cyber security services*" that are subject to this requirement have not been defined and are left to be prescribed by the Minister. Similarly, matters such as the prerequisites for licence application, manner in which the application for licence is to be made as well as information, particulars or documents needed for the licence have not been prescribed by the Proposed Act yet. We anticipate that these will be determined by subsidiary legislation once the Proposed Act comes into force.

Non-compliance could see offenders hit with a fine of up to RM100,000 (approximately USD21,000 as at the date of writing) and/or two years imprisonment.

(f) Government bound by the Proposed Act

For completeness, the Proposed Act shall bind the Federal Government and State Governments, albeit nothing in the Proposed Act shall render them liable to prosecution for any offence under the Proposed Act.

Conclusion

The passing of a legislation to regulate cyber security matters has been a long time coming. Businesses and relevant sectors falling under the NCII Sectors are advised to keep watch for the legal developments, particularly the issuance of regulations or directives addressing the licensing requirements and be ready to take proactive steps in implementing necessary measures required by the Proposed Act to ensure regulatory compliance.

For further enquiries, please contact:

Janet Toh Yoong San
Head, Personal Data Protection & Privacy
Co-Head, Technology, Media & Telco
E: janet.toh@shearndelamore.com
T: +603 2027 2978

Boo Cheng Xuan
Associate, Personal Data Protection & Privacy
Associate, Technology, Media & Telco
E: boo.chengxuan@shearndelamore.com
T: +603 2027 2662

This article was written with the assistance of Ng Ying Chia (Pupil-in-Chambers).

[1] See Explanatory Statement of the Bill.
[2] Clause 3 of the Bill.
[3] Clause 4 of the Bill.
[4] Clause 5(2) of the Bill.
[5] Clause 5(4) of the Bill.
[6] Clause 6(1) of the Bill.
[7] Clause 10(1)(a) of the Bill.
[8] Clause 10(1)(b) of the Bill.
[9] Clause 10(1)(c) of the Bill.
[10] Clauses 10(1)(d) and (e) of the Bill.
[11] Clause 13 of the Bill.
[12] Clause 11 of the Bill.
[13] Clause 21 of the Bill.
[14] Clause 20 of the Bill.
[15] Clause 22 of the Bill.
[16] Clause 22 of the Bill.
[17] Clause 23 of the Bill.
[18] Clause 24 of the Bill.