D.R. 8/2024

CYBER SECURITY BILL 2024

AMENDMENT IN COMMITTEE

ENGLISH LANGUAGE TEXT

Clause 58

Subparagraph 58*(b)*(i) of the Bill is amended by substituting for the word "and" at the end of the subparagraph the word "or".

EXPLANATORY STATEMENT

Clause 58 of the Bill is amended in subparagraph 58*(b)*(i) to further clarify the provision relating to the facts to be proven by a director, compliance officer, partner, manager, secretary or other similar officer of a company, limited liability partnership, firm, society or other body of persons in the case where the company, limited liability partnership, firm, society or other body of persons is found guilty of an offence under this Bill.

CYBER SECURITY BILL 2024

ARRANGEMENT OF CLAUSES

PART I

PRELIMINARY

Clause

1. Short title and commencement
2. This Act binds the Federal Government and State Governments
3. Extra-territorial application
4. Interpretation

PART II

NATIONAL CYBER SECURITY COMMITTEE

5. Establishment of Committee
6. Functions of Committee
7. Meetings of Committee
8. Committee may invite others to attend meetings
9. Committee may establish subcommittees

PART III

DUTIES AND POWERS OF CHIEF EXECUTIVE

10. Duties and powers of Chief Executive
11. National Cyber Coordination and Command Centre System
12. Appointment of cyber security expert
13. Directive of Chief Executive
14. Power to gather information

PART IV

NATIONAL CRITICAL INFORMATION INFRASTRUCTURE SECTOR LEAD AND NATIONAL CRITICAL INFORMATION INFRASTRUCTURE ENTITY

15. Appointment of national critical information infrastructure sector lead
16. Functions of national critical information infrastructure sector lead

Clause

17. Designation of national critical information infrastructure entity

18. Designation of national critical information infrastructure sector lead as national critical information infrastructure entity

19. Revocation of designation of national critical information infrastructure entity

20. Duty to provide information relating to national critical information infrastructure

21. Duty to implement code of practice

22. Duty to conduct cyber security risk assessment and audit

23. Duty to give notification on cyber security incident

24. Cyber security exercise

PART V

CODE OF PRACTICE

25. Code of practice

26. Directions under other written law shall be consistent with code of practice

PART VI

CYBER SECURITY SERVICE PROVIDER

27. Licensing of cyber security service provider

28. Qualifications for application of licence

29. Application for licence

30. Renewal of licence

31. Conditions of licence

32. Duty to keep and maintain record

33. Revocation or suspension of licence

34. Transfer or assignment of licence

PART VII

CYBER SECURITY INCIDENT

35. Cyber security incident

PART VIII

ENFORCEMENT

Clause

36. Authorization of public officer
37. Authority card
38. Power of investigation
39. Search and seizure with warrant
40. Search and seizure without warrant
41. List of seized objects, etc.
42. Cost of holding seized object, etc.
43. Release of seized object, etc.
44. Forfeiture of seized object, etc.
45. Property in forfeited object, etc.
46. Access to computerized data
47. No cost or damage arising from seizure to be recoverable
48. Power to require attendance of person acquainted with case
49. Examination of person acquainted with case
50. Admissibility of statement in evidence
51. Additional powers
52. Obstruction

PART IX

GENERAL

53. Appeal
54. Service of document
55. Obligation of secrecy
56. Protection against suit and legal proceedings
57. Prosecution
58. Liability of director, etc., of company, etc.
59. Liability of person for act, etc., of employee, etc.
60. Compounding of offences
61. Power to exempt

Clause

62. Power to amend Schedule
63. Power to make regulations
64. Saving

SCHEDULE

A BILL

intituled

An Act to enhance the national cyber security by providing for the establishment of the National Cyber Security Committee, duties and powers of the Chief Executive of the National Cyber Security Agency, functions and duties of the national critical information infrastructure sector leads and national critical information infrastructure entities and the management of cyber security threats and cyber security incidents to national critical information infrastructures, to regulate the cyber security service providers through licensing, and to provide for related matters.

[ ]

ENACTED by the Parliament of Malaysia as follows:

PART I

PRELIMINARY

Short title and commencement

1. (1) This Act may be cited as the Cyber Security Act 2024.

(2) This Act comes into operation on a date to be appointed by the Minister by notification in the *Gazette*.

This Act binds the Federal Government and State Governments

2. (1) This Act shall bind the Federal Government and State Governments.

(2) Nothing in this Act shall render the Federal Government and State Governments liable to prosecution for any offence under this Act.

Extra-territorial application

3. (1) This Act shall, in relation to any person, whatever his nationality or citizenship, have effect outside as well as within Malaysia, and where an offence under this Act is committed by any person in any place outside Malaysia, he may be dealt with in respect of such offence as if the offence was committed at any place within Malaysia.

(2) For the purposes of subsection (1), this Act shall apply if for the offence in question, the national critical information infrastructure is wholly or partly in Malaysia.

Interpretation

4. In this Act, unless the context otherwise requires—

"this Act" includes any subsidiary legislation made under this Act;

"cyber security threat" means an act or activity carried out on or through a computer or computer system, without lawful authority, that may imminently jeopardize or may adversely affect the cyber security of that computer or computer system or another computer or computer system;

"directive" means a directive issued by the Chief Executive under section 13;

"prescribed" means prescribed by Minister by regulations made under this Act;

"national critical information infrastructure entity" means any Government Entity or person designated as a national critical information infrastructure entity under section 17 or 18;

"Government Entity" means—

(a) any ministry, department, office, agency, authority, commission, committee, board, council or other body, of the Federal Government, or of any of the State Governments, established under any written law or otherwise; and

(b) any local authority;

"national critical information infrastructure" means 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;

"cyber security incident" means 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;

"Committee" means the National Cyber Security Committee established under section 5;

"cyber security" means the state in which a computer or computer system is protected from any attack or unauthorized access, and because of that state—

(a) the computer or computer system continues to be available and operational;

(b) the integrity of the computer or computer system is maintained; and

(c) the integrity and confidentiality of information stored in, processed by or transmitted through, the computer or computer system is maintained;

"Chief Executive" means the Chief Executive of the National Cyber Security Agency;

"national critical information infrastructure sector lead" means any Government Entity or person appointed as a national critical information infrastructure sector lead under section 15;

"computer" means an electronic, magnetic, optical, electrochemical, or other data processing device performing logical, arithmetic, storage or display function, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but does not include an automated typewriter or typesetter, or a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility;

"Minister" means the Minister charged with the responsibility for cyber security;

"authorized officer" means any police officer of whatever rank or any public officer authorized under section 36;

"cyber security service provider" means a person who provides a cyber security service;

"cyber security service" means the cyber security service as may be prescribed under subsection 27(2);

"national critical information infrastructure sector" means the national critical information infrastructure sector specified in the Schedule;

"computer system" means an arrangement of interconnected computers that is designed to perform one or more specific functions, and includes—

(a) an information technology system; and

(b) an operational technology system such as an industrial control system, a programmable logic controller, a supervisory control and data acquisition system, or a distributed control system;

"code of practice" means the code of practice referred to in section 25.

PART II

NATIONAL CYBER SECURITY COMMITTEE

Establishment of Committee

5. (1) A committee by the name of "National Cyber Security Committee" is established.

(2) The Committee shall consist of the following members:

(a) the Prime Minister who shall be the Chairman;

(b) the Minister charged with the responsibility for finance;

(c) the Minister charged with the responsibility for foreign affairs;

(d) the Minister charged with the responsibility for defence;

(e) the Minister charged with the responsibility for home affairs;

(f) the Minister charged with the responsibility for communications;

(g) the Minister charged with the responsibility for digital related matters;

(h) the Chief Secretary to the Government;

(i) the Chief of Defence Force;

(j) the Inspector General of Police;

(k) the Director General of National Security; and

(l) not more than two other persons who shall be appointed by the Committee from among persons of standing and experience in cyber security.

(3) The Chairman shall appoint from among the members of the Committee a Deputy Chairman.

(4) The Chief Executive shall be the secretary to the Committee.

Functions of Committee

6. (1) The Committee shall have the following functions:

(a) to plan, formulate and decide on policies relating to national cyber security;

(b) to decide on approaches and strategies in addressing matters relating to national cyber security;

(c) to monitor the implementation of policies and strategies relating to national cyber security;

(d) to advise and make recommendations to the Federal Government on policies and strategic measures to strengthen national cyber security;

(e) to give directions to the Chief Executive and national critical information infrastructure sector leads on matters relating to national cyber security;

(f) to oversee the effective implementation of this Act; and

(g) to do such other things arising out of or consequential to the functions of the Committee under this Act consistent with the purposes of this Act.

(2) The Committee shall have all such powers as may be necessary for, or in connection with, or reasonably incidental to, the performance of its functions under this Act.

Meetings of Committee

7. (1) The Committee shall convene its meeting as often as the Chairman may determine and the meeting shall be held at the time and place as determined by the Chairman.

(2) The Chairman shall preside at all meetings of the Committee.

(3) If the Chairman is absent from any meeting of the Committee, he may direct the Deputy Chairman to replace him as the chairman of the meeting.

(4) The quorum of the Committee shall be five.

(5) The Chairman may authorize the use of a live video link, live television link or any other electronic means of communication for the purposes of any meeting of the Committee.

(6) The Committee may determine its own procedure.

Committee may invite others to attend meetings

8. The Committee may invite any person to attend meetings of the Committee to advise the Committee on any matter under discussion.

Committee may establish subcommittees

9. (1) The Committee may establish any subcommittee as the Committee considers necessary or expedient to assist the Committee in the performance of its functions.

(2) The Committee may appoint any person to be a member of any subcommittee established under subsection (1).

(3) The Committee may appoint any of its members or any other person to be the chairman of the subcommittee established under subsection (1).

(4) The subcommittee shall be subject to and act in accordance with any directions given by the Committee.

(5) The subcommittee shall meet as often as may be necessary at the time and place as the chairman of the subcommittee may determine.

(6) The subcommittee may invite any person to attend meetings of the subcommittee to advise the subcommittee on any matter under discussion.

(7) The chairman of the subcommittee may authorize the use of a live video link, live television link or any other electronic means of communication for the purposes of any meeting of the subcommittee.

PART III

DUTIES AND POWERS OF CHIEF EXECUTIVE

Duties and powers of Chief Executive

10. (1) The Chief Executive shall have the following duties:

(a) to advise and make recommendations to the Committee on policies, strategies and strategic measures relating to national cyber security;

(b) to implement the policies, strategies and strategic measures made and directions given by the Committee or the Federal Government on matters relating to national cyber security;

(c) to coordinate and monitor the implementation of policies, strategies and strategic measures on national cyber security by the national critical information infrastructure sector leads, national critical information infrastructure entities, Government Entities or any other person;

(d) to collect and coordinate the data, information or intelligence relating to national cyber security received from the national critical information infrastructure sector leads, national critical information infrastructure entities, Government Entities or any other person, and to evaluate or correlate such data, information or intelligence;

(e) to disseminate the information and intelligence referred to in paragraph *(d)* to the national critical information infrastructure sector leads or national critical information infrastructure entities if the Chief Executive thinks it is essential to do so in the interest of national cyber security;

(f) to issue directives to the national critical information infrastructure sector leads, national critical information infrastructure entities, Government Entities or any person on matters relating to national cyber security; or

(g) to carry out any other duties imposed upon him under this Act or as directed by the Committee.

(2) The Chief Executive shall have all such powers as may be necessary for, or in connection with, or reasonably incidental to, the carrying out of his duties under this Act.

National Cyber Coordination and Command Centre System

11. (1) The Chief Executive shall establish and maintain 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.

(2) The National Cyber Coordination and Command Centre System may contain any data or information on cyber security obtained or kept by the Chief Executive in the course of carrying out his duties under this Act.

(3) The Chief Executive may, in the interest of national cyber security and subject to such terms and conditions as he thinks fit, authorize any person to have access to the National Cyber Coordination and Command Centre System.

Appointment of cyber security expert

12. The Chief Executive may in writing appoint any qualified expert in cyber security as a cyber security expert for a period as determined by the Chief Executive in the course of, or in connection with, or reasonably incidental to, the performance of the Chief Executive's duties under this Act.

Directive of Chief Executive

13. (1) The Chief Executive may issue such directive as the Chief Executive considers necessary for the purpose of ensuring compliance with this Act.

(2) The Chief Executive may revoke, vary, revise or amend the whole or any part of any directive issued under this section.

Power to gather information

14. (1) Notwithstanding any other written law, if the Chief Executive has reasonable grounds to believe that any person—

(a) has any information, particulars or document that is relevant to the performance of the Chief Executive's duties and powers under this Act; or

(b) is capable of giving any evidence which the Chief Executive has reasonable grounds to believe is relevant to the performance of the Chief Executive's duties and powers under this Act,

the Chief Executive may, by notice in writing, direct that person—

(A) to give any such information or particulars to the Chief Executive in the form and manner and within the period as specified in the notice or such extended period as the Chief Executive may grant;

(B) to produce any such document, whether in physical form or in electronic media, to the Chief Executive in the manner and within the period as specified in the notice or such extended period as the Chief Executive may grant;

(C) to make copies of any such document and to produce those copies to the Chief Executive in the manner and within the period as specified in the notice or such extended period as the Chief Executive may grant;

(D) if the person is an individual, to appear before an authorized officer at the time and place specified in the notice to give any evidence, either orally or in writing, and produce any document, whether in physical form or in electronic media, in the manner and within the period as specified in the notice or such extended period as the Chief Executive may grant;

(E) if the person is a body corporate or a public body, to cause a competent officer of the body corporate or public body to appear before an authorized officer at the time and place specified in the notice to give any evidence, either orally or in writing, and produce any document, whether in physical form or in electronic media, in the manner and within the period as specified in the notice or such extended period as the Chief Executive may grant; or

(F) if the person is a partnership, to cause an individual who is a partner in the partnership or an employee of the partnership to appear before an authorized officer at the time and place specified in the notice to give any evidence, either orally or in writing, and produce any document, whether in physical form or in electronic media, in the manner and within the period as specified in the notice or such extended period as the Chief Executive may grant.

(2) Where the Chief Executive directs any person to produce any document under subsection (1) and the document is not in the custody of that person, that person shall—

(a) state, to the best of his knowledge and belief, where the document may be found; and

(b) identify, to the best of his knowledge and belief, the last person who had custody of the document and to state, to the best of his knowledge and belief, where that last-mentioned person may be found.

(3) Any person directed to give or produce any information, particulars or documents or copies of any document under subsection (1), shall ensure that the information, particulars or documents or copies of the document given or produced are true, accurate and complete and such person shall provide an express

representation to that effect, including a declaration that he is not aware of any other information, particulars or document which would make the information, particulars or document given or produced untrue or misleading.

(4) Where any person discloses any information or particulars or produces any document in response to a notice in writing under this section, such person, his agent or employee, or any other person acting on his behalf or under his directions, shall not, by reason only of such disclosure or production, be liable to prosecution for any offence under any written law, or to any proceedings or claim by any person under any law or under any contract, agreement or arrangement, or otherwise.

(5) Subsection (4) shall not bar, prevent or prohibit the institution of any prosecution for any offence as provided by this section or the disclosure or production of false information or document in relation to a notice in writing under this section furnished to the Chief Executive pursuant to this section.

(6) Any person who fails to comply with the directions of the Chief Executive under subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding three years or to both.

(7) Any person who contravenes subsection (2) or (3) commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding three years or to both.

PART IV

NATIONAL CRITICAL INFORMATION INFRASTRUCTURE SECTOR LEAD AND NATIONAL CRITICAL INFORMATION INFRASTRUCTURE ENTITY

Appointment of national critical information infrastructure sector lead

15. (1) The Minister may, upon the recommendation of the Chief Executive, appoint any Government Entity or person to be the national critical information infrastructure sector lead for each of the national critical information infrastructure sectors.

(2) The Minister may appoint more than one national critical information infrastructure sector lead for any of the national critical information infrastructure sectors.

(3) The names of the national critical information infrastructure sector leads appointed under this section shall be published in the official website of the National Cyber Security Agency.

Functions of national critical information infrastructure sector lead

16. The national critical information infrastructure sector lead shall, in respect of the national critical information infrastructure sector for which it is appointed, have the following functions:

(a) to designate a national critical information infrastructure entity under section 17;

(b) to prepare a code of practice as required under section 25;

(c) to implement the decisions of the Committee and directives under this Act;

(d) to monitor and ensure that actions required of and duties imposed on the national critical information infrastructure entities under this Act are carried out by the national critical information infrastructure entities;

(e) to prepare and maintain guidelines on best practices in relation to cyber security management;

(f) to prepare and submit to the Chief Executive a situational report whether on its own initiative or as required by the Chief Executive where a cyber security threat or cyber security incident has affected a national critical information infrastructure within its national critical information infrastructure sector; and

(g) to carry out such other functions under this Act.

Designation of national critical information infrastructure entity

17. (1) A national critical information infrastructure sector lead may, in respect of the national critical information infrastructure sector for which it is appointed, designate in such manner as may

be determined by the Chief Executive, any Government Entity or person as a national critical information infrastructure entity if the national critical information infrastructure sector lead is satisfied that the Government Entity or person owns or operates a national critical information infrastructure.

(2) For the purpose of subsection (1), the national critical information infrastructure sector lead may require the Government Entity or person to produce any information, particulars or document as may be determined by the national critical information infrastructure sector lead including information relating to the function and design of the computer or computer system owned or operated by the Government Entity or person.

(3) No Government Entity shall be designated as a national critical information infrastructure entity by a national critical information infrastructure sector lead which is not a Government Entity.

(4) The national critical information infrastructure sector lead shall notify the Chief Executive of the designation of the national critical information infrastructure entity made under subsection (1) together with particulars relating to the national critical information infrastructure owned or operated by the national critical information infrastructure entity in the manner as may be determined by the Chief Executive.

(5) The national critical information infrastructure sector lead shall keep and maintain a register of the national critical information infrastructure entities which have been designated under this section in such manner as may be determined by the Chief Executive.

(6) The national critical information infrastructure entity which has been designated under this section shall by notice in writing notify its national critical information infrastructure sector lead without delay if—

(a) the national critical information infrastructure entity is of the opinion that the computer or computer system owned or operated by the national critical information infrastructure entity has ceased to be a national critical information infrastructure; or

(b) the national critical information infrastructure entity no longer owns or operates any national critical information infrastructure.

Designation of national critical information infrastructure sector lead as national critical information infrastructure entity

18. (1) The Chief Executive may designate a national critical information infrastructure sector lead as a national critical information infrastructure entity in such manner as he may determine if the Chief Executive is satisfied that the national critical information infrastructure sector lead owns or operates a national critical information infrastructure.

(2) For the purpose of subsection (1), the Chief Executive may require the national critical information infrastructure sector lead to produce any information, particulars or document as may be determined by the Chief Executive including information relating to the function and design of the computer or computer system owned or operated by the national critical information infrastructure sector lead.

(3) The Chief Executive shall keep and maintain a register of the national critical information infrastructure sector leads which have been designated as national critical information infrastructure entities under this section in such manner as may be determined by the Chief Executive.

(4) The national critical information infrastructure sector lead which has been designated as a national critical information infrastructure entity under this section shall by notice in writing notify the Chief Executive without delay if—

(a) the national critical information infrastructure sector lead is of the opinion that the computer or computer system owned or operated by the national critical information infrastructure sector lead has ceased to be a national critical information infrastructure; or

(b) the national critical information infrastructure sector lead no longer owns or operates any national critical information infrastructure.

Revocation of designation of national critical information infrastructure entity

19. (1) A national critical information infrastructure sector lead may by notice in writing to the national critical information infrastructure entity, revoke the designation of the national critical information infrastructure entity made under section 17, if the national critical information infrastructure sector lead is satisfied that the national critical information infrastructure entity no longer owns or operates any national critical information infrastructure.

(2) The revocation of the designation made under subsection (1) shall take effect from the date specified in the notice.

(3) The national critical information infrastructure sector lead shall notify the Chief Executive of the revocation made under subsection (1).

(4) The Chief Executive may by notice in writing to the national critical information infrastructure sector lead which has been designated as a national critical information infrastructure entity under section 18, revoke the designation of the national critical information infrastructure sector lead if the Chief Executive is satisfied that the national critical information infrastructure sector lead no longer owns or operates any national critical information infrastructure.

(5) The revocation of the designation made under subsection (4) shall take effect from the date specified in the notice and shall not affect the appointment of the national critical information infrastructure sector lead under section 15.

Duty to provide information relating to national critical information infrastructure

20. (1) The national critical information infrastructure sector lead may request a national critical information infrastructure entity in respect of the national critical information infrastructure sector for which it is appointed to provide information relating to the national critical information infrastructure owned or operated by the national critical information infrastructure entity in such manner as may be determined by the national critical information infrastructure sector lead and the national critical information infrastructure entity shall comply with the request.

(2) Where the national critical information infrastructure entity procures or has come into possession or control of any additional computer or computer system which in the opinion of the national critical information infrastructure entity that the computer or computer system is a national critical information infrastructure, the national critical information infrastructure entity shall provide such information to its national critical information infrastructure sector lead regardless whether there is a request under subsection (1).

(3) If a material change is made to the design, configuration, security or operation of the national critical information infrastructure owned or operated by the national critical information infrastructure entity after the information on such national critical information infrastructure has been provided under subsection (1), the national critical information infrastructure entity shall notify its national critical information infrastructure sector lead of the material change within thirty days from the date the change was completed.

(4) For the purpose of subsection (3), a change is a material change if the change affects or may affect the cyber security of the national critical information infrastructure or the ability of the national critical information infrastructure entity to respond to a cyber security threat or cyber security incident.

(5) The national critical information infrastructure sector lead shall notify the Chief Executive of any information received under subsections (2) and (3) in the manner as may be determined by the Chief Executive.

(6) Any national critical information infrastructure entity which contravenes subsection (1), (2) or (3) commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

(7) Any national critical information infrastructure sector lead which contravenes subsection (5) commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit.

Duty to implement code of practice

21. (1) A national critical information infrastructure entity shall implement the measures, standards and processes as specified in the code of practice to ensure the cyber security of the national critical information infrastructure owned or operated by the national critical information infrastructure entity.

(2) Notwithstanding subsection (1), the national critical information infrastructure entity may implement any alternative measures, standards and processes if the national critical information infrastructure entity proves to the satisfaction of the Chief Executive that the alternative measures, standards and processes provide equal or higher level of protection to the national critical information infrastructure owned or operated by the national critical information infrastructure entity.

(3) A national critical information infrastructure entity may, in addition to the measures, standards and processes referred to in subsection (1) or (2), establish and implement the measures, standards and processes on cyber security based on internationally recognized standards or framework.

(4) Where a national critical information infrastructure entity implements measures, standards and processes to ensure the cyber security of the national critical information infrastructure owned or operated by the national critical information infrastructure entity as required under any other written law, the national critical information infrastructure entity shall be deemed to have complied with this section provided that such measures, standards and processes are not in contravention with the code of practice.

(5) Any national critical information infrastructure entity which contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding ten years or to both.

Duty to conduct cyber security risk assessment and audit

22. (1) A national critical information infrastructure entity shall within the period as may be prescribed—

(a) conduct a cyber security risk assessment in respect of the national critical information infrastructure owned or operated by the national critical information infrastructure entity in accordance with the code of practice and directive; and

(b) cause to be carried out an audit by an auditor approved by the Chief Executive to determine the compliance of the national critical information infrastructure entity with this Act.

(2) The national critical information infrastructure entity shall, within the period of thirty days after the completion of the cyber security risk assessment or audit under subsection (1), submit the cyber security risk assessment report or audit report to the Chief Executive.

(3) Where it appears to the Chief Executive from the cyber security risk assessment report submitted under subsection (2) that the result of the cyber security risk assessment is not satisfactory, the Chief Executive may direct the national critical information infrastructure entity to take further initiatives to re-evaluate the cyber security risk to such national critical information infrastructure within the period as may be determined by the Chief Executive.

(4) Where the Chief Executive finds that the audit report submitted under subsection (2) is insufficient, the Chief Executive may direct the national critical information infrastructure entity to rectify the audit report within the period as may be determined by the Chief Executive.

(5) Upon receipt of the information from the national critical information infrastructure sector lead under subsection 20(5) on the material change made to the design, configuration, security or operation of a national critical information infrastructure, the Chief Executive may by notice in writing direct the national critical information infrastructure entity which owns or operates the national critical information infrastructure to conduct a cyber security risk assessment or cause to be carried out an audit in respect of the national critical information infrastructure regardless whether a cyber security risk assessment or audit has been conducted or carried out under subsection (1) in respect of such national critical information infrastructure.

(6) The Chief Executive may direct a national critical information infrastructure entity to conduct a cyber security risk assessment or cause to be carried out an audit in addition to the cyber security risk assessment or audit under subsection (1) or (5).

(7) Any national critical information infrastructure entity which contravenes subsection (1) or (2) commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding three years or to both.

(8) Any national critical information infrastructure entity which fails to comply with the directions of the Chief Executive under subsection (3), (4), (5) or (6) commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit.

Duty to give notification on cyber security incident

23. (1) If it comes to the knowledge of a national critical information infrastructure entity that a cyber security incident has or might have occurred in respect of the national critical information infrastructure owned or operated by the national critical information infrastructure entity, the national critical information infrastructure entity shall notify the Chief Executive and its national critical information infrastructure sector lead on such information within the period and in such manner as may be prescribed.

(2) Any national critical information infrastructure entity which contravenes this section commits an offence and shall, on conviction, be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding ten years or to both.

Cyber security exercise

24. (1) The Chief Executive may conduct a cyber security exercise for the purpose of assessing the readiness of any national critical information infrastructure entity in responding to any cyber security threat or cyber security incident.

(2) The Chief Executive shall, before carrying out any cyber security exercise under subsection (1), issue a notice in writing to the national critical information infrastructure entity concerned notifying his intention to carry out such cyber security exercise in respect of the national critical information infrastructure entity.

(3) The Chief Executive may give any directions to the national critical information infrastructure entity as the Chief Executive thinks fit for the purpose of the cyber security exercise carried out under this section.

(4) Any national critical information infrastructure entity which fails to comply with the directions of the Chief Executive under subsection (3) commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit.

PART V

CODE OF PRACTICE

Code of practice

25. (1) A national critical information infrastructure sector lead shall prepare a code of practice to be endorsed by the Chief Executive containing measures, standards and processes in ensuring the cyber security of a national critical information infrastructure within the national critical information infrastructure sector for which it is appointed.

(2) The national critical information infrastructure sector lead shall, in preparing the code of practice under subsection (1), consider among others the following matters:

(a) the functions of the relevant national critical information infrastructure entities;

(b) provisions relating to cyber security under any other written law applicable to the national critical information infrastructure sector lead;

(c) the views of the relevant national critical information infrastructure entities; and

(d) the views of the relevant regulatory authority, if any, of which the national critical information infrastructure entity is subject to.

(3) The Chief Executive may endorse the code of practice prepared under subsection (1) if the Chief Executive is satisfied that—

(a) the measures, standards and processes specified in the code of practice are consistent with or above the minimum requirements specified in the directive;

(b) the matters as set out in subsection (2) have been given due consideration; and

(c) the code of practice is consistent with the provisions of this Act.

(4) The code of practice under this section shall take effect on the date of the endorsement of the code of practice by the Chief Executive.

(5) If the Chief Executive refuses to endorse the code of practice, the Chief Executive shall notify the national critical information infrastructure sector lead concerned of his decision in writing and provide the reasons for it.

(6) Any national critical information infrastructure sector lead which contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit.

Directions under other written law shall be consistent with code of practice

26. Where a national critical information infrastructure sector lead directs any national critical information infrastructure entity to implement measures, standards and processes to ensure the cyber security of the national critical information infrastructure owned or operated by the national critical information infrastructure entity under any other written law, the national critical information infrastructure sector lead shall ensure that the directions given are consistent with the code of practice.

PART VI

CYBER SECURITY SERVICE PROVIDER

Licensing of cyber security service provider

27. (1) No person shall—

(a) provide any cyber security service; or

(b) advertise, or in any way hold himself out as a provider of a cyber security service,

unless he holds a licence to provide a cyber security service issued under this Part.

(2) The Minister may prescribe any cyber security service in respect of which a license shall be obtained under this Part.

(3) This Part shall not apply in the case where the cyber security service is provided by a company to its related company.

(4) In this section, "related company" has the meaning assigned to it in the Companies Act 2016 [*Act 777*].

(5) Any person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding ten years or to both.

Qualifications for application of licence

28. Any person may apply for a licence under this Part if the person—

(a) fulfils prerequisite requirements as may be determined by the Chief Executive; and

(b) has not been convicted of an offence involving fraud, dishonesty or moral turpitude.

Application for licence

29. (1) An application for a licence to provide cyber security service shall be made to the Chief Executive in such manner as may be prescribed.

(2) The application under subsection (1) shall be accompanied by payment of the prescribed fee and such information, particulars or document as may be determined by the Chief Executive.

(3) After considering the application, the Chief Executive may—

(a) approve the application and issue to the applicant upon payment of the prescribed fee a licence in such form as may be determined by the Chief Executive; or

(b) refuse the application, stating the grounds for refusal.

(4) A licence issued under this section shall be valid for a period as specified in the licence.

Renewal of licence

30. (1) A licensee may apply to renew its licence issued under section 29 at least thirty days before the date of expiration of the licence in such manner as may be prescribed.

(2) The application under subsection (1) shall be accompanied by payment of the prescribed fee and such information, particulars or document as may be determined by the Chief Executive.

(3) After considering the application, the Chief Executive may—

(a) approve the application and renew the licence upon payment of the prescribed fee; or

(b) refuse the application, stating the grounds for refusal.

Conditions of licence

31. (1) A licence to provide a cyber security service may be issued subject to such conditions as the Chief Executive thinks fit to impose.

(2) The Chief Executive may at any time vary or revoke the conditions imposed on a license under subsection (1).

(3) Any person who contravenes any conditions of a licence imposed under subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

Duty to keep and maintain record

32. (1) A licensee shall, on each occasion where the licensee is engaged to provide cyber security service, keep and maintain the following records:

(a) the name and address of the person engaging the licensee for the cyber security service;

(b) the name of the person providing the cyber security service on behalf of the licensee, if any;

(c) the date and time of cyber security service that was provided by the licensee or other person on behalf of the licensee;

(d) details of the type of cyber security service provided; and

(e) such other particulars as may be determined by the Chief Executive.

(2) The information referred to in subsection (1) shall be—

(a) kept and maintained in the manner as may be determined by the Chief Executive;

(b) retained for a period of not less than six years from the date the cyber security service was provided; and

(c) produced to the Chief Executive at any time as the Chief Executive may direct.

(3) Any person who contravenes subsection (1) or (2) commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

Revocation or suspension of licence

33. The Chief Executive may revoke or suspend the licence issued under section 29 if the Chief Executive is satisfied that—

(a) the licensee has failed to comply with any conditions of the licence;

(b) the licence has been obtained by fraud or misrepresentation;

(c) a circumstance existed at the time the licence was issued or renewed that the Chief Executive was unaware of, which would have caused the Chief Executive to refuse to issue or renew the licence if the Chief Executive had been aware of the circumstance at that time;

(d) the licensee has ceased to carry on the business in respect of which he is licenced under this Act;

(e) the licensee has been adjudged a bankrupt or has gone into liquidation or is being wound up;

(f) the licensee has been convicted of an offence under this Act or an offence involving fraud, dishonesty or moral turpitude; or

(g) the revocation or suspension is in the interest of the public or national security.

Transfer or assignment of licence

34. (1) A licence shall not be transferred or assigned to any other person.

(2) Any person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding three years or to both.

(3) Notwithstanding subsection (1), a licence may be transferred to any other person with the approval of the Chief Executive—

(a) if an application in writing is made to the Chief Executive by the licensee; and

(b) if the Chief Executive is satisfied that the person to whom the licence is to be transferred has the necessary financial and technical resources to comply with the conditions of the licence.

PART VII

CYBER SECURITY INCIDENT

Cyber security incident

35. (1) Upon receipt of the notification on cyber security incident from a national critical information infrastructure entity under section 23 or if it comes to the knowledge of the Chief Executive that a cyber security incident in respect of a national critical information infrastructure has or might have occurred, the Chief Executive shall instruct an authorized officer to investigate into the matter.

(2) The investigation carried out under this Part shall be for the purposes of—

(a) ascertaining whether a cyber security incident has occurred; or

(b) in the case where a cyber security incident has occurred, determining the measures necessary to respond to or recover from the cyber security incident and preventing such cyber security incident from occurring in the future.

(3) Upon completion of the investigation by the authorized officer under this Part—

(a) if the authorized officer finds that no cyber security incident has occurred, the authorized officer shall notify the Chief Executive about such findings and the Chief Executive shall notify the national critical information infrastructure entity which owns or operates the national critical information infrastructure referred to in subsection (1) accordingly and dismiss the matter; or

(b) if the authorized officer finds that a cyber security incident has occurred, the authorized officer shall notify the Chief Executive about such findings and the Chief Executive shall notify the national critical information infrastructure entity which owns or operates the national critical information infrastructure referred to in subsection (1) accordingly.

(4) Upon being notified by the authorized officer under paragraph (3)*(b)* that a cyber security incident has occurred, the Chief Executive may issue a directive to the national critical information infrastructure entity which owns or operates the national critical information infrastructure concerned on the measures necessary to respond to or recover from the cyber security incident and to prevent such cyber security incident from occurring in the future.

(5) Any national critical information infrastructure entity which fails to comply with the directive of the Chief Executive under subsection (4) commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding three years or to both.

PART VIII

ENFORCEMENT

Authorization of public officer

36. The Minister may, in writing, authorize any public officer to exercise the powers of enforcement under this Act.

Authority card

37. (1) There shall be issued to each authorized officer an authority card to be signed by the Minister.

(2) Whenever such authorized officer exercises any of the powers under this Act, he shall, on demand, produce to the person against whom the power is being exercised the authority card issued to him under subsection (1).

Power of investigation

38. (1) An authorized officer shall have all the powers necessary to carry out an investigation in relation to any cyber security incident under this Act.

(2) An authorized officer shall have the powers of a police officer of whatever rank as provided for under the Criminal Procedure Code [*Act 593*] in relation to investigation into any offence under this Act, and such powers shall be in addition to and not in derogation of, the powers provided for under this Act.

Search and seizure with warrant

39. (1) Where it appears to a Magistrate, upon written information on oath from an authorized officer and after such inquiry as the Magistrate considers necessary, that there is reasonable cause to believe that—

(a) any premises have been used in; or

(b) there is in any premises evidence necessary to the carrying out of an investigation into,

the commission of an offence under this Act, the Magistrate may issue a warrant authorizing the authorized officer named in the warrant, at any reasonable time by day or by night and with or without assistance, to enter the premises and if need be by force.

(2) Without affecting the generality of subsection (1), the warrant issued by the Magistrate may authorize the search and seizure of—

(a) copies of any book, account or other document, including computerized data, which contain or are reasonably suspected to contain information as to any offence so suspected to have been committed;

(b) any signboard, card, letter, pamphlet, leaflet or notice representing or implying that the person has a licence issued under this Act; or

(c) any other document, facility, apparatus, vehicle, equipment, device or matter that is reasonably believed to furnish evidence of the commission of the offence.

(3) An authorized officer conducting a search under subsection (1) may, for the purpose of investigating into the offence, search any person who is in or on the premises.

(4) An authorized officer making a search of a person under subsection (3) may seize or take possession of, and place in safe custody all things, other than the necessary clothing, found upon the person, and any other things, for which there is a reason to believe that they are the instruments or other evidence of the crime, and they may be detained until the discharge or acquittal of the person.

(5) No person shall be searched except by another person of the same gender, and such search shall be conducted with strict regard to decency.

(6) If, by reason of its nature, size and amount, it is not practicable to remove any object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter seized under this section, the authorized officer shall, by any means, seal such object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter in or on the premises in which it is found.

(7) Any person who, without lawful authority, breaks, tampers with or damages the seals referred to in subsection (6) or removes any object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter under seals or attempts to do so commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

Search and seizure without warrant

40. If an authorized officer is satisfied upon information received that he has reasonable cause to believe that by reason of delay in obtaining a search warrant under section 39 the investigation would be adversely affected or evidence of the commission of an offence is likely to be tampered with, removed, damaged or destroyed, the authorized officer may enter the premises and exercise in, upon and in respect of the premises all the powers referred to in section 39 in as full and ample manner as if he were authorized to do so by a warrant issued under that section.

List of seized objects, etc.

41. (1) Where any seizure is made under this Act, an authorized officer making the seizure shall prepare a list of the object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter seized and shall sign the list.

(2) The list prepared in accordance with subsection (1) shall be delivered immediately to the owner or person in control or in charge of the premises which has been searched, or to such owner's or person's agent or employee, at that premises.

Cost of holding seized object, etc.

42. Where any object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter seized under this Act is held in the custody of the Federal Government

pending completion of any proceedings in respect of an offence under this Act, the cost of holding it in custody shall, in the event of any person being convicted of such offence, be a debt due to the Federal Government by such person and shall be recoverable accordingly.

Release of seized object, etc.

43. (1) Where any object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter has been seized under this Act, any authorized officer, may at any time, after referring to the Deputy Public Prosecutor, release the object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter to the person as he determines to be lawfully entitled to the object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter if he is satisfied that the object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter is not liable to forfeiture under this Act and is not otherwise required for the purposes of any proceedings under this Act, or for the purposes of any prosecution under any other written law, and in such event neither the authorized officer effecting the seizure, nor the Federal Government or any person acting on behalf of the Federal Government, shall be liable to any proceedings by any person if the seizure and the release of the object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter had been effected in good faith.

(2) A record in writing shall be made by the authorized officer effecting the release of the object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter under subsection (1) specifying in detail the circumstances of and the reason for the release, and he shall send a copy of the record to the Deputy Public Prosecutor as soon as practicable.

Forfeiture of seized object, etc.

44. (1) Any object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter seized in exercise of any power conferred under this Act shall be liable to forfeiture.

(2) An order for the forfeiture of any object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter shall be made if it is proved to the satisfaction of the court that an offence under this Act has been committed and that the object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter was the subject matter of or was used in the commission of the offence, even though no person has been convicted of such offence.

(3) Where there is no prosecution with regard to any object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter seized under this Act, such object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter shall be taken and deemed to be forfeited at the expiration of a period of one calendar month from the date of service of a notice to the last known address of the person from whom the object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter was seized indicating that there is no prosecution in respect of such object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter unless before the expiration of that period a claim thereto is made in the manner set out in subsections (4), (5), (6) and (7).

(4) Any person asserting that he is the owner of the object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter referred to in subsection (3) and that it is

not liable to forfeiture may personally or by his agent authorized in writing, give written notice to the authorized officer in whose possession such object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter is held that he claims the object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter.

(5) On receipt of the notice referred to in subsection (4), the authorized officer shall refer the claim to a Magistrate for his decision.

(6) The Magistrate to whom a matter is referred under subsection (5) shall issue a summons requiring the person asserting that he is the owner of the object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter and the person from whom it was seized to appear before him, and when they appear or they fail to appear, due service of the summons having been proved, the Magistrate shall proceed to the examination of the matter.

(7) If it is proved that an offence under this Act has been committed and that the object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter referred to in subsection (6) was the subject matter of or was used in the commission of such offence, the Magistrate shall order the object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter to be forfeited, and shall, in the absence of such proof, order its release.

(8) Any object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter forfeited or deemed to be forfeited shall be delivered to the Chief Executive and shall be disposed of in such manner as the Chief Executive thinks fit.

Property in forfeited object, etc.

45. Any object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter forfeited or deemed to be forfeited under this Act shall be the property of the Federal Government.

Access to computerized data

46. (1) Any authorized officer conducting a search under this Act shall be given access to computerized data whether stored in computer or otherwise.

(2) For the purposes of this section, an authorized officer shall be provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of the computerized data.

No cost or damage arising from seizure to be recoverable

47. No person shall, in any proceedings before any court in respect of any object, book, account, document, computerized data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter seized in the exercise or the purported exercise of any power conferred under this Act, be entitled to the costs of such proceedings or to any damages or other relief unless such seizure was made without reasonable cause.

Power to require attendance of person acquainted with case

48. (1) An authorized officer making an investigation under this Part may, by order in writing, require the attendance before himself of any person who appears to him to be acquainted with the facts and circumstances of the case, and such person shall attend as so required.

(2) If any such person refuses or fails to attend as required by an order made under subsection (1), the authorized officer may report such refusal or failure to a Magistrate who shall issue a warrant to secure the attendance of such person as may be required by the order.

Examination of person acquainted with case

49. (1) An authorized officer making an investigation under this Act may examine orally any person supposed to be acquainted with the facts and circumstances of the case.

(2) Such person shall be bound to answer all questions relating to the case put to him by the authorized officer, but he may refuse to answer any question the answer which would have a tendency to expose him to a criminal charge or penalty or forfeiture.

(3) A person making a statement under this section shall be legally bound to state the truth, whether or not such statement is made wholly or partly in answer to questions.

(4) The authorized officer examining a person under subsection (1) shall first inform that person of the provision of subsections (2) and (3).

(5) A statement made by any person under this section shall, whenever possible, be reduced into writing and signed by the person making it or affixed with his thumbprint, as the case may be—

(a) after it has been read to him in the language in which he made it; and

(b) after he has been given an opportunity to make any correction he may wish.

Admissibility of statement in evidence

50. (1) Except as provided in this section, no statement made by any person to an authorized officer in the course of an investigation made under this Act shall be used in evidence.

(2) When any witness is called for the prosecution or for the defence, other than the accused, the court shall, on the request of the accused or the prosecutor, refer to any statement made by that witness to an authorized officer in the course of an investigation under this Act and may then, if the court thinks fit in the interest of justice, direct the accused to be furnished with a copy of the statement and the statement may be used to impeach the credit of the witness in the manner provided by the Evidence Act 1950 [*Act 56*].

(3) Where the accused had made a statement during the course of an investigation, such statement may be admitted in evidence in support of his defence during the course of the trial.

(4) Nothing in this section shall be deemed to apply to any statement made in the course of an identification parade or falling within section 27 or paragraphs 32(1)*(a)*, *(i)* and *(j)* of the Evidence Act 1950.

(5) When any person is charged with any offence in relation to the making or the contents of any statement made by him to an authorized officer in the course of an investigation made under this Act, that statement may be used as evidence in the prosecution's case.

Additional powers

51. (1) An authorized officer shall, for the purposes of the execution of this Act, have the powers to do all or any of the following:

(a) to require the production of any computer, book, record, computerized data, document or other article and to inspect, examine and make copy of any of them;

(b) to require the production of any identification document from any person in relation to any act or offence under this Act; and

(c) to make such inquiries as may be necessary to ascertain whether the provisions of this Act have been complied with.

(2) Any person who fails to comply with the requirement made under subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

Obstruction

52. Any person who assaults, impedes, obstructs or interferes with, or refuses access to any premises or computerized data to, the Chief Executive or authorized officer in the performance of his duties under this Act commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

PART IX

GENERAL

Appeal

53. (1) Any person aggrieved—

(a) by the refusal of the Chief Executive to issue to him a licence under this Act; or

(b) by the revocation or suspension of his licence,

may, within thirty days after being informed in writing of the refusal, suspension or revocation, appeal in writing against such decision to the Minister.

(2) The Minister may, after considering the appeal made under subsection (1), confirm or set aside the decision appealed against.

Service of document

54. (1) Subject to subsection (2), the Chief Executive may allow any information, particulars or document required to be submitted or furnished under this Act to be submitted or furnished by an electronic medium or by way of an electronic transmission.

(2) The conditions and specifications under which the information, particulars or document referred to in subsection (1) are to be submitted or furnished shall be as determined by the Chief Executive.

(3) The information, particulars or document referred to in subsection (1) shall be deemed to have been submitted or furnished by a person to the Chief Executive on the date the acknowledgement of receipt of such documents is transmitted electronically by the Chief Executive to the person.

(4) The acknowledgment of receipt by the Chief Executive of that information, particulars or document submitted or furnished pursuant to subsection (3) shall be admissible as evidence in any proceedings.

Obligation of secrecy

55. (1) Except for any of the purposes of this Act or for the purposes of any civil or criminal proceedings under any written law or where otherwise authorized by the Committee, any member of the Committee, the Chief Executive or any authorized officer, whether during or after his tenure of office or employment, shall not disclose any information obtained by him in the course of his duties.

(2) Any person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

Protection against suit and legal proceedings

56. No action, suit, prosecution or other proceedings shall be brought, instituted or maintained in any court against the Minister, any member of the Committee, the Chief Executive or any authorized officer on account of or in respect of any act, neglect or default done or omitted by him in the course of carrying out his duties under this Act unless it can be proven that the act, neglect or default was done or omitted in bad faith and without reasonable cause.

Prosecution

57. No prosecution for an offence under this Act shall be instituted except by or with the written consent of the Public Prosecutor.

Liability of director, etc., of company, etc.

58. Where any person who commits an offence under this Act is a company, limited liability partnership, firm, society or other body of persons, a person who at the time of the commission of the offence was a director, compliance officer, partner, manager, secretary or other similar officer of the company, limited liability partnership, firm, society or other body of persons or was purporting to act in the capacity or was in any manner or to any extent responsible for the management of any of the affairs of the company, limited liability partnership, firm, society or other body of persons or was assisting in its management—

(a) may be charged severally or jointly in the same proceedings with the company, limited liability partnership, firm, society or other body of persons; and

(b) if the company, limited liability partnership, firm, society or other body of persons is found guilty of the offence, shall be deemed to be guilty of the offence and shall be liable to the same punishment or penalty as an individual unless, having regard to the nature of his functions in that capacity and to all circumstances, he proves—

(i) that the offence was committed without his knowledge; and

(ii) that the offence was committed without his consent or connivance and that he had taken all reasonable precautions and exercised due diligence to prevent the commission of the offence.

Liability of person for act, etc., of employee, etc.

59. Where any person would be liable to any punishment or penalty under this Act for any act, omission, neglect or default committed—

(a) by that person's employee in the course of his employment;

(b) by that person's agent when acting on behalf of that person; or

(c) by the employee of that person's agent when acting in the course of his employment with that person's agent or otherwise on behalf that person's agent acting on behalf of that person,

that person shall be liable to the same punishment or penalty for every such act, omission, neglect or default of that person's employee or agent, or of the employee of that person's agent.

Compounding of offences

60. (1) The Minister may, with the approval of the Public Prosecutor, make regulations prescribing—

(a) any offence under this Act as an offence which may be compounded; and

(b) the method and procedure for compounding such offence.

(2) The Chief Executive may, with the consent in writing of the Public Prosecutor, compound any offence committed by any person under this Act prescribed to be a compoundable offence by making a written offer to the person suspected to have committed the offence to compound the offence upon payment to the Chief Executive of an amount of money not exceeding fifty per centum of the amount of maximum fine for that offence within such time as may be specified in his written offer.

(3) An offer under subsection (2) may be made at any time after the offence has been committed but before any prosecution for it has been instituted.

(4) If the amount specified in the offer is not paid within the time specified in the offer, or such extended time as the Chief Executive may grant, prosecution for the offence may be instituted at any time after that against the person to whom the offer was made.

(5) Where an offence has been compounded under this section—

(a) no prosecution shall be instituted in respect of the offence against the person to whom the offer to compound was made; and

(b) any document or thing seized in connection with the offence may be released by the Chief Executive, subject to such terms as the Chief Executive thinks fit.

(6) All sums of money received by the Chief Executive under this section shall be paid into and form part of the Federal Consolidated Fund.

Power to exempt

61. The Minister may, by order published in the *Gazette*, subject to such conditions or restrictions as he may consider necessary or expedient to impose, exempt any person or class of persons from any or all of the provisions of this Act.

Power to amend Schedule

62. The Minister may, upon recommendation of the Chief Executive, by order published in the *Gazette*, amend the Schedule to this Act.

Power to make regulations

63. (1) The Minister may make regulations as may be necessary or expedient for the purpose of carrying into effect the provisions of this Act.

(2) Without prejudice to the generality of subsection (1), the Minister may make regulations to prescribe—

(a) the period for the conduct of a cyber security risk assessment and the carrying out of audit;

(b) the period and manner in which the information relating to a cyber security incident shall be notified to the Chief Executive and the national critical information sector lead;

(c) the cyber security service in respect of which a licence shall be obtained under this Act before it can be provided;

(d) the manner for the application of licence and renewal of licence under this Act;

(e) the fees payable under this Act;

(f) the offences which may be compounded and the forms to be used and the method and procedure for compounding the offences under this Act;

(g) any other matters required by this Act to be prescribed.

(3) The regulations made under this Act may prescribe an act or omission in contravention of the regulations to be an offence and may prescribe penalties of a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding three years or to both.

Saving

64. On the date of the coming into operation of this Act, any measures, standards and processes which have been implemented to ensure the cyber security of a national critical information infrastructure and imposed on any Government Entity or person under Directive of the National Security Council No. 26 shall, so long as it is consistent with the provisions of this Act, continue to remain in force until it is revoked under the National Security Council Act 2017 [*Act 776*].

SCHEDULE

[Section 4]

CRITICAL NATIONAL INFORMATION INFRASTRUCTURE SECTOR

1. Government
2. Banking and finance
3. Transportation
4. Defence and national security
5. Information, communication and digital
6. Healthcare services
7. Water, sewerage and waste management
8. Energy
9. Agriculture and plantation
10. Trade, industry and economy
11. Science, technology and innovation

EXPLANATORY STATEMENT

This Bill ("the proposed Act") seeks to enhance the national cyber security by requiring compliance of certain measures, standards and processes in the management of the cyber security threats and cyber security incidents to national critical information infrastructures. This is due to the extensive use of information and communications technology systems and devices in executing various functions and businesses of the public sectors and private sectors. For these purposes, the proposed Act provides, among others, for the establishment of the National Cyber Security Committee, the duties and powers of the Chief Executive of the National Cyber Security Agency, the appointment of the national critical information infrastructure sector leads and the designation of national critical information infrastructure entities as well as licensing of cyber security service providers.

PART I

2. Part I of the proposed Act deals with preliminary matters.

3. *Clause 1* contains the short title of the proposed Act and provision on the commencement of the proposed Act.

4. *Clause 2* seeks to provide that the proposed Act shall bind the Federal Government and State Governments. However, no prosecution shall be instituted against the Federal Government or any of the State Governments for any offence under the proposed Act.

5. *Clause 3* seeks to provide for the extra-territorial application of the proposed Act.

6. *Clause 4* contains the definitions of certain words and expressions used in the proposed Act.

PART II

7. Part II of the proposed Act deals with the establishment of the National Cyber Security Committee ("Committee").

8. *Clause 5* seeks to provide for the establishment and membership of the Committee.

9. *Clause 6* seeks to provide for the functions of the Committee.

10. *Clause 7* seeks to provide for meetings of the Committee. This *clause* also provides that the Committee may determine its own procedure.

11. *Clause 8* seeks to provide that the Committee may invite any person to attend meetings of the Committee for the purpose of advising the Committee on any matter under discussion.

12. *Clause 9* seeks to provide that the Committee may appoint subcommittees to assist the Committee in the performance of its functions under the proposed Act.

PART III

13. Part III of the proposed Act deals with the duties and powers of the Chief Executive of National Cyber Security Agency ("Chief Executive").

14. *Clause 10* seeks to provide for the duties and powers of the Chief Executive under the proposed Act.

15. *Clause 11* seeks to provide for the establishment and maintenance of the National Cyber Coordination and Command Centre System by the Chief Executive for the purpose of dealing with cyber security threats and cyber security incidents.

16. *Clause 12* seeks to empower the Chief Executive to appoint any qualified expert in cyber security as a cyber security expert in the course of or in connection with, or reasonably incidental to, the performance of the Chief Executive duties under the proposed Act. Among the main purposes of the appointment of a cyber security expert under the proposed Act is to assist the Chief Executive in carrying out his duties in relation to cyber security incidents.

17. *Clause 13* seeks to provide that the Chief Executive may issue such directive for the purpose of ensuring compliance with the proposed Act. This directive shall include among others the minimum requirement for measures, standards and processes relating to cyber security.

18. *Clause 14* seeks to require any person to provide information, particulars or document to the Chief Executive if the Chief Executive has reasonable grounds to believe that such person has any information, particulars or document that is relevant to the performance of the Chief Executive's duties and powers under the proposed Act or that such person is capable of giving any evidence which the Chief Executive has reasonable grounds to believe is relevant to the performance of the Chief Executive's duties and powers under the proposed Act. Any person who discloses any information or produces any document under this *clause* shall not, by reason only of such disclosure or production, be liable to prosecution for any offence under any written law, or to any proceedings or claim by any person under any law or under any contract, agreement or arrangement, or otherwise.

PART IV

19. Part IV of the proposed Act deals with the national critical information infrastructure sector leads and national critical information infrastructure entities.

20. *Clause 15* seeks to provide for the appointment of a national critical information infrastructure sector lead.

21. *Clause 16* seeks to provide for the functions of a national critical information infrastructure sector lead.

22. *Clause 17* seeks to provide for the designation of any Government Entity or person as a national critical information infrastructure entity by a national critical information infrastructure sector lead if the national critical information infrastructure sector lead is satisfied that the national critical information infrastructure entity owns or operates a national critical information infrastructure. This *clause* also provides for the keeping of the register of national critical information infrastructure entities so designated.

23. *Clause 18* seeks to provide for the designation of the national critical information infrastructure sector lead as a national critical information infrastructure entity by the Chief Executive and the keeping of a register of such designation made by the Chief Executive.

24. *Clause 19* seeks to provide for the revocation of the designation of a national critical information infrastructure entity if the entity no longer owns or operates any national critical information infrastructure.

25. *Clause 20* seeks to provide for the duty of a national critical information infrastructure entity to provide information relating to its national critical information infrastructure to the national critical information infrastructure sector lead. A national critical information infrastructure entity is also required to provide information under this *clause* when it procures or has come into possession or control of any additional computer or computer system which in its opinion is a national critical information infrastructure, or when any material change is made to the design, configuration, security or operation of its existing national critical information infrastructure.

26. *Clause 21* seeks to provide for the duty of a national critical information infrastructure entity to implement measures, standards and processes as specified in the code of practice or any alternative and additional measures, standards and processes for the purpose of ensuring the cyber security of its national critical information infrastructure. Implementation of measures, standards and processes under any other written law for the purpose of ensuring the cyber security of the national critical information infrastructure which is not in contravention with the code of practice shall be deemed to be in compliance with this *clause*.

27. *Clause 22* seeks to provide for the duty of a national critical information infrastructure entity to conduct a cyber security risk assessment and cause to be carried out an audit and to submit the cyber security risk assessment report or audit report to the Chief Executive.

28. *Clause 23* seeks to provide for the duty of a national critical information infrastructure entity to notify the Chief Executive and its national critical information infrastructure sector lead of any cyber security incident which has or might have occurred in respect of its national critical information infrastructure.

29. *Clause 24* seeks to empower the Chief Executive to carry out a cyber security exercise for the purpose of assessing the readiness of any national critical information infrastructure entity in responding to any cyber security threat or cyber security incident.

PART V

30. Part V of the proposed Act deals with code of practice.

31. *Clause 25* seeks to provide for the preparation and endorsement of the code of practice.

32. *Clause 26* seeks to clarify that when a national critical information infrastructure sector lead directs a national critical information infrastructure entity to implement measures, standards and processes to ensure the cyber security of its national critical information infrastructure under any other written law, the national critical information infrastructure sector lead shall ensure that the directions given are consistent with the code of practice prepared under *clause 25*.

PART VI

33. Part VI of the proposed Act deals with the licensing of cyber security service provider.

34. *Clause 27* seeks to provide for the requirement of licence in relation to cyber security service provider. For this purpose, the cyber security service shall be as prescribed by the Minister.

35. *Clause 28* seeks to provide for the qualifications for an application for a licence under this Part.

36. *Clause 29* seeks to provide that an application for a licence shall be made to the Chief Executive and the Chief Executive may approve or refuse the application.

37. *Clause 30* seeks to provide for the renewal of a licence.

38. *Clause 31* seeks to provide for the power of the Chief Executive to impose conditions on a licence.

39. *Clause 32* seeks to provide for the duty of a licensee to keep and maintain records relating to the cyber security service provided by the licensee.

40. *Clause 33* seeks to provide for the revocation or suspension of a licence.

41. *Clause 34* seeks to prohibit the transfer or assignment of a licence under the proposed Act. Be that as it may, the transfer of such licence may still be made with the approval of the Chief Executive.

PART VII

42. Part VII of the proposed Act deals with cyber security incidents.

43. *Clause 35* seeks to provide for the investigation of a cyber security incident and the power of the Chief Executive to issue a directive on the measures necessary to respond to or recover from the cyber security incident and to prevent such cyber security incident from occurring in the future.

PART VIII

44. Part VIII of the proposed Act deals with enforcement provisions.

45. *Clause 36* seeks to provide that the Minister may authorize any public officer to exercise the powers of enforcement under the proposed Act.

46. *Clause 37* seeks to provide for the issuance of authority cards to the authorized officers.

47. *Clause 38* seeks to provide for the power of investigation of the authorized officers.

48. *Clause 39* deals with the provision relating to search and seizure with warrant.

49. *Clause 40* deals with the provision relating to search and seizure without warrant.

50. *Clause 41* seeks to require an authorized officer to prepare a list of things seized in the course of his investigation.

51. *Clause 42* seeks to provide that the cost of holding any thing seized under the proposed Act pending the completion of criminal proceedings against a person for an offence under the proposed Act shall be a debt due to the Federal Government by such person and shall be recoverable upon conviction of such person.

52. *Clause 43* seeks to provide for the release of any thing seized under the proposed Act.

53. *Clause 44* deals with the provision relating to the forfeiture of any thing seized under the proposed Act.

54. *Clause 45* seeks to provide that any thing forfeited or deemed to be forfeited under the proposed Act shall be the property of the Federal Government.

55. *Clause 46* seeks to provide for the access to computerized data by the authorized officer. This includes access to the computerized data stored in the cloud computing infrastructures.

56. *Clause 47* seeks to provide that no cost or damages arising from the seizure of any thing under the proposed Act to be recoverable in any proceedings before any court unless such seizure was done without reasonable cause.

57. *Clause 48* seeks to provide that an authorized officer may require the attendance of any person acquainted with the facts and circumstances of a case being investigated by the authorized officer.

58. *Clause 49* seeks to provide that an authorized officer may examine any person supposed to be acquainted with the facts and circumstances of a case being investigated by the authorized officer.

59. *Clause 50* seeks to provide for the admissibility of a statement made by a person to an authorized officer in the course of an investigation made under the proposed Act as evidence.

60. *Clause 51* deals with additional powers of an authorized officer for the purpose of the execution of the proposed Act.

61. *Clause 52* seeks to provide that it shall be an offence for any person who obstructs the Chief Executive or any authorized officer in the performance of their duties under the proposed Act.

PART IX

62. Part IX of the proposed Act deals with general provisions.

63. *Clause 53* seeks to provide that any person aggrieved by the refusal of the Chief Executive to issue a licence to him or by the revocation or suspension of his licence may appeal to the Minister.

64. *Clause 54* deals with the service of documents under the proposed Act.

65. *Clause 55* seeks to prohibit any member of the Committee, the Chief Executive and authorized officers from disclosing any information obtained in the course of carrying out their duties unless the disclosure is done for the purposes of legal proceedings under any written law or as authorized by the Committee.

66. *Clause 56* seeks to provide for the protection of the Minister, any member of the Committee, the Chief Executive or any authorized officer against suits and legal proceedings in respect of any act, neglect or default done or omitted by him in the course of carrying out his duties under the proposed Act.

67. *Clause 57* provides that no prosecution shall be instituted for any offence under the proposed Act without the consent in writing of the Public Prosecutor.

68. *Clause 58* deals with the liability of a director, compliance officer, partner, manager, secretary or other similar officer in respect of an offence by a company, limited liability partnership, firm, society or other body of persons under the proposed Act.

69. *Clause 59* deals with the liability of a person for any act, omission, neglect or default by an employee of the person, agent of the person or employee of the person's agent under the proposed Act.

70. *Clause 60* seeks to provide for the compounding of offences under the proposed Act.

71. *Clause 61* seeks to empower the Minister to exempt any person or class of persons from any or all of the provisions of the proposed Act.

72. *Clause 62* seeks to empower the Minister to amend the Schedule to the proposed Act upon recommendation of the Chief Executive.

73. *Clause 63* seeks to empower the Minister to make regulations under the proposed Act.

74. *Clause 64* deals with saving provision.

FINANCIAL IMPLICATIONS

This Bill will involve the Government in extra financial expenditure the amount of which cannot at present be ascertained.

[PN(U2)3081]