CYBERCRIMES BILL 2026

ARRANGEMENT OF CLAUSES

PART I

PRELIMINARY

Clause

1. Short title and commencement
2. Extra-territorial application
3. Interpretation

PART II

COMMITTEE ON COMBATING CYBERCRIMES

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

PART III

OFFENCES RELATING TO CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF COMPUTER SYSTEM AND COMPUTER DATA

9. Access to computer system
10. Access to computer system without authority
11. Access to computer system without authority with intention to commit or facilitate commission of further offence
12. Interception without authority
13. Computer data interference
14. Computer system interference
15. Misuse of device

PART IV

OFFENCES RELATING TO COMPUTER-RELATED FORGERY AND COMPUTER-RELATED FRAUD

Clause

16. Computer-related forgery

17. Computer-related fraud

PART V

OFFENCES RELATING TO NATIONAL DIGITAL IDENTITY SERVICE

18. Interpretation

19. Disclosure of password or provision of other means of securing access in identity of user

20. Obtaining, etc., credential

PART VI

OTHER OFFENCES

21. Wrongful communication

22. Identity theft

23. Transmitting, etc., content generated or manipulated by means of computer system

24. Dissemination of intimate images

25. Offences committed which affects or involves national critical information infrastructure entity or national critical information infrastructure

PART VII

ENFORCEMENT

26. Authorization of public officer or officer of Commission

27. Power of investigation

28. Search and seizure with warrant

29. Search and seizure without warrant

30. Warrant admissible notwithstanding defect

Clause

31. List of things seized
32. Cost of holding things seized
33. Release of things seized
34. Forfeiture of things seized
35. Property in forfeited things
36. Access to computer system or computer data
37. No cost or damages arising from seizure to be recoverable
38. Expedited preservation of computer data
39. Disclosure of computer data
40. Real-time collection of traffic data
41. Interception of content data
42. Power to require attendance of person acquainted with case
43. Examination of person acquainted with case
44. Admissibility of statement in evidence
45. Additional powers
46. Obstruction
47. Power of search and seizure without warrant, access to computer system or computer data etc., by police officer
48. General procedural powers
49. Jurisdiction to try offence

PART VIII

MISCELLANEOUS

50. Integrated information system
51. General duty of service provider
52. Obligation to retain computer data
53. Service provider not liable for act done in good faith
54. Power of court to make certain orders
55. Service of notice
56. Attempt and abetment

Clause

57. Protection against suit and legal proceedings

58. Prosecution

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

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

61. Repeal and savings

A BILL

intituled

An Act to prevent and combat cybercrimes which consists of offences provided for under Parts III to VI of this Act and offences provided for under any other written law committed by means of a computer system, 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 Cybercrimes Act 2026.

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

Extra-territorial application

2. (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 computer system, program or computer data was in Malaysia or connected to or sent to or used by or with a computer system, program or computer data in Malaysia at the material time or the person affected by the commission of the offence is a Malaysian citizen.

Interpretation

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

"technical means" includes the use of any device, equipment, software, program, computer code, network or other technological means;

"content data" means any computer data, other than subscriber information or traffic data, relating to the substance of the data transferred by a computer system, including images, text messages, voice messages, audio recordings and video recordings;

"computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system which includes a program suitable to cause a computer system to perform a function, including content data, traffic data and subscriber information;

"traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that forms a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or type of underlying service;

"property" means an asset of every kind, whether corporeal or incorporeal, movable or immovable property, tangible or intangible, including virtual asset, digital currency and legal documents or instruments evidencing title to, or interest in, such asset;

"Committee" means the Committee on Combating Cybercrimes established under section 4;

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

"communications" means any communication, whether between persons and persons, things and things, or persons and things, in the form of sound, data, text, visual images, signals or any other form or any combination of those forms;

"subscriber information" means any information held by a service provider, relating to subscribers of its services, other than traffic data or content data, and which can be established by—

(a) the type of communication service used by the subscriber and the related technical provisions and period of service;

(b) the subscriber's identity, address, telephone or other access number, billing or payment information, available on the basis of the service agreement or arrangement; or

(c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement;

"Minister" means the Minister charged with the responsibility for matters relating to cybercrimes;

"authorized officer" means any police officer, or any other public officer or officer of the Commission authorized in writing by the Minister under section 26;

"officer of the Commission" means an officer of the Malaysian Communications and Multimedia Commission;

"service provider" means a person, whether licensed under the Communications and Multimedia Act 1998 [*Act 588*] or not, who—

(a) provides to users of its services the ability to communicate by means of a computer system;

(b) processes or stores computer data on behalf of a communications service or users of the communications service; or

(c) provides an information and communication service, including telecommunications;

"program" means a set of instructions or statements that when executed in a computer system causes the computer system to perform a function;

"computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, gathers, stores and performs automatic processing of computer data, including a computer;

"Commission" means the Malaysian Communications and Multimedia Commission established under section 4 of the Malaysian Communications and Multimedia Commission Act 1998 [*Act 589*].

PART II

COMMITTEE ON COMBATING CYBERCRIMES

Establishment of Committee

4. (1) A committee by the name of "Committee on Combating Cybercrimes" is established.

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

(a) the Chief Secretary to the Government who shall be the Chairman;

(b) the Director General of National Security who shall be the Deputy Chairman;

(c) the Secretary General of Treasury or his representative;

(d) the Attorney General or his representative;

(e) the Inspector-General of Police or his representative;

(f) the Secretary General of the Ministry charged with the responsibility for home affairs or his representative;

(g) the Secretary General of the Ministry charged with the responsibility for communications or his representative;

(h) the Secretary General of the Ministry charged with the responsibility for foreign affairs or his representative;

(i) the Secretary General of the Ministry charged with the responsibility for domestic trade and cost of living or his representative;

(j) the Secretary General of the Ministry charged with the responsibility for digital related matters or his representative;

(k) the Personal Data Protection Commissioner or his representative;

(l) the Director General of the Legal Affairs Division of the Prime Minister's Department or his representative;

(m) the Governor of the Central Bank of Malaysia or his representative;

(n) the Director General of the National Anti-Financial Crime Centre or his representative;

(o) the Chairman of the Malaysian Communications and Multimedia Commission or his representative;

(p) the Chairman of the Securities Commission or his representative;

(q) the Chief Executive Officer of the Companies Commission of Malaysia or his representative; and

(r) not more than two other persons who shall be appointed by the Chairman from among persons of standing, experience, knowledge and expertise in matters relating to cybercrimes.

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

Functions of Committee

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

(a) to plan, formulate and decide on approaches and strategies in preventing and combating cybercrimes;

(b) to advise and make recommendations to the Government on policies and strategic measures to prevent and combat cybercrimes;

(c) to coordinate initiatives to prevent and combat cybercrimes in an integrated manner among the enforcement agencies;

(d) to assess and oversee the effectiveness of existing actions and mechanisms in preventing and combating cybercrimes;

(e) to identify gaps and recommend improvements in the legal and enforcement framework relating to cybercrimes; and

(f) 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

6. (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

7. 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

8. (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

OFFENCES RELATING TO CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF COMPUTER SYSTEM AND COMPUTER DATA

Access to computer system

9. For the purposes of this Part—

(a) a person secures access to the whole or any part of a computer system if the person causes a computer system to perform any function, including by communicating with, instructing, storing data on, retrieving data from, altering or erasing any program or data in, or otherwise making use of any resource of, the computer system; and

(b) a person secures access of any kind to the whole or any part of a computer system without authority if in securing access—

(i) the person is not entitled to control access of the kind in question to the computer system; and

(ii) the person does not have the consent or exceeds any right or consent given, to access by him of the kind in question to the computer system from any person who is so entitled.

Access to computer system without authority

10. (1) Any person who, intentionally and without authority or without lawful purpose, secures access to the whole or any part of a computer system 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 three years or to both.

(2) For the purposes of subsection (1), it is immaterial whether the access to the computer system is directed at any particular program or computer data in the computer system.

Access to computer system without authority with intention to commit or facilitate commission of further offence

11. (1) Any person who commits an offence under section 10 with the intention—

(a) to commit a further offence involving fraud or dishonesty or which causes injury as defined in the Penal Code [*Act 574*]; or

(b) to facilitate the commission of such further offence whether by himself or by any other person,

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 seven years or to both.

(2) For the purposes of subsection (1), it is immaterial whether such further offence is to be committed at the same time when the access is secured without authority or on any future occasion.

Interception without authority

12. (1) Any person who, intentionally and without authority or without lawful purpose, intercepts by technical means any non-public transmission of computer data to, from or within a computer system, including any electromagnetic emissions from a computer system carrying computer data, 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 seven years or to both.

(2) For the purposes of subsection (1), it is immaterial whether the interception is directed at any particular non-public transmission of computer data.

Computer data interference

13. Any person who, intentionally and without authority or without lawful purpose—

(a) damages, deletes, deteriorates, alters, suppresses or modifies computer data;

(b) renders computer data meaningless, useless or ineffective;

(c) obstructs, interrupts or interferes with the lawful use of computer data; or

(d) denies access to computer data to any person entitled to it,

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 three years or to both.

Computer system interference

14. Any person who, intentionally and without authority or without lawful purpose, inputs, transmits, damages, deletes, deteriorates, alters or suppresses computer data so as to seriously hinder or interfere with the functioning of a computer system or lawful use or operation of a computer system 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 seven years or to both.

Misuse of device

15. (1) Any person who, intentionally and without authority or without lawful purpose, obtains, procures for use, produces, sells, imports or exports, distributes, discloses or otherwise makes available—

(a) a device including a program, that is designed or adapted primarily for the purpose of committing any offence under this Act; or

(b) a password, access credentials, electronic signature or similar computer data by which the whole or any part of a computer system or computer data is capable of being accessed,

with the intention that a device including a program, password, access credentials, electronic signature or similar computer data be used by himself or any other person for the purpose of committing an offence under this Act, 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 seven years or to both.

(2) Any person who has in his possession or control any device referred to in paragraph (1)*(a)* or any password, access credentials, electronic signature or computer data referred to in paragraph (1)*(b)* with the intention that the device, password, access credentials, electronic signature or computer data be used by himself or by any other person for the purpose of committing any offence under this Act commits an offence and shall, on conviction, be liable to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding five years or to both.

PART IV

OFFENCES RELATING TO COMPUTER-RELATED FORGERY AND COMPUTER-RELATED FRAUD

Computer-related forgery

16. (1) Any person who, intentionally and without authority or without lawful purpose, inputs, alters, deletes or suppresses computer data resulting in inauthentic computer data with the intention that such computer data be considered or acted upon for any legal purpose as if the computer data were authentic, whether or not such computer data is intended to deceive any particular person, commits an offence and shall, on conviction—

(a) where valuable security is involved, be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding seven years or to both; or

(b) in any other case, be liable to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding five years or to both.

(2) For the purposes of subsection (1)—

(a) "valuable security" means a document which is, or purports to be, a document that creates, extends, transfers, restricts, extinguishes or releases any legal right, or by which a person acknowledges that he lies under legal liability or does not have a certain legal right; and

(b) it is immaterial whether the computer data in question is directly readable or intelligible.

Computer-related fraud

17. Any person who, intentionally and without authority or without lawful purpose—

(a) inputs, alters, deletes or suppresses any computer data;

(b) interferes with the functioning of a computer system; or

(c) causes deception as to factual circumstances by means of a computer system that causes a person to do or omit to do anything which that person would not otherwise do or omit to do,

so as to cause loss of property to another person with the fraudulent or dishonest intention to procure without authority economic benefit for himself or for another person commits an offence and shall, on conviction, be liable to a fine not exceeding one million ringgit or to imprisonment for a term not exceeding ten years or to both.

PART V

OFFENCES RELATING TO NATIONAL DIGITAL IDENTITY SERVICE

Interpretation

18. For the purposes of this Part—

(a) "credential", in relation to a user includes—

(i) the user's national digital identity service password;

(ii) the user's biometric identifier which includes any personal data resulting from technical processing relating to the physical, physiological or behavioural characteristics of a person captured electronically; and

(iii) the user's digital certificate;

(b) "user" means a person who is registered with the national digital identity service; and

(c) "national digital identity service" means the electronic service owned by the Federal Government by which a user's identity is verified and authenticated.

Disclosure of password or provision of other means of securing access in identity of user

19. (1) Any user who—

(a) discloses his national digital identity service password to any person; or

(b) provides to any person any other means of securing access in the identity of the user to any program or computer data in any computer system by means of the national digital identity service,

knowing or having reasonable grounds to believe that the purpose of the disclosure or provision is for any person to commit or to facilitate the commission by any person of, any offence under any written law, 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 three years or to both.

(2) In any proceedings for an offence under subsection (1), if it is proven that the user discloses his national digital identity service password or provides any other means of securing access in the identity of the user to any person—

(a) for any gain, whether or not the gain is a wrongful gain, realized, or for himself or for another person; or

(b) knowing that the disclosure or provision is likely to cause wrongful loss to any person,

it shall be presumed until the contrary is proved that the user knew or had reasonable grounds to believe that the disclosure or provision was for the purpose of committing or facilitating the commission of, an offence under any written law.

Obtaining, etc., credential

20. (1) Any person who obtains, retains, supplies, offers to supply, transmits or otherwise makes available any credential of any user—

(a) for the purpose of committing or facilitating the commission of, any offence under any written law; or

(b) knowing or having reason to believe that the credential will be used, or is likely to be used, for the purpose of committing, or facilitating the commission of, any offence under any written law,

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 three years or to both, and for a second or subsequent offence, to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding five years or to both.

(2) It shall not be an offence under subsection (1) for a person to transmit or otherwise make available credentials of any user by reason only that the person, in the ordinary course of providing such facilities or services, provides or operates facilities for network access, or provides services relating to, or connections for, the transmission, routing or storage of data.

PART VI

OTHER OFFENCES

Wrongful communication

21. Any person who communicates directly or indirectly a number, code, password or other means of access to a computer system to any person other than a person to whom he is duly authorized to communicate such number, code, password or other means of access, commits an offence and shall, on conviction, be liable to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding five years or to both.

Identity theft

22. (1) Any person who, intentionally and without authority or without lawful purpose, by means of a computer system, obtains, supplies, uses or has in his possession or control, any identity information of another person with the intention to commit or facilitate the commission of any offence under any written law, 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 seven years or to both.

(2) For the purposes of subsection (1), "identity information" means any information that identifies, or is capable of identifying or purports to identify, a person.

Transmitting, etc., content generated or manipulated by means of computer system

23. Any person who transmits, distributes, publishes, sells or offers for sale or otherwise makes available, any visual or audio content generated or manipulated, whether wholly or partly, by means of a computer system, resembling an existing person, object, place, entity or event that falsely appears to a person to be authentic or truthful with the intention to commit or facilitate the commission of any offence under any written law, whether by himself or by any other person, 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 seven years or to both.

Dissemination of intimate images

24. (1) Any person who transmits, distributes, publishes, sells or offers for sale or otherwise makes available by means of a computer system any intimate images of any person, commits an offence and shall, on conviction, be liable to imprisonment for a term not exceeding five years or to a fine not exceeding three hundred thousand ringgit or to both.

(2) Any person who commits an offence under subsection (1) with the intention to cause humiliation or harm to, or to coerce or intimidate, the person depicted in the intimate image, shall, on conviction, be liable to imprisonment for a term not exceeding seven years or to a fine not exceeding five hundred thousand ringgit or to both.

(3) For the purposes of this section—

(a) "intimate image" means a visual recording, including a photograph or video recording, made by any means, whether altered or otherwise, that is sexual in nature, in which the sexual parts of a person are exposed or a person is engaged in sexual activity; and

(b) "harm" means harm to a person's body, mind, reputation or property, including psychological harm.

Offences committed which affects or involves national critical information infrastructure entity or national critical information infrastructure

25. (1) Any person who commits an offence under Part III or IV or section 21, 22 or 23 which affects or involves a national critical information infrastructure entity or national critical information infrastructure, shall, on conviction—

(a) where such offence involves loss of life, be liable to imprisonment for a term of not less than thirty years but not exceeding forty years or to a fine not exceeding two million ringgit or to both;

(b) where such offence involves any injury to any person, be liable to imprisonment for a term not exceeding fifteen years or to a fine not exceeding one million and five hundred thousand ringgit or to both; and

(c) in any other case, be liable to a fine not exceeding one million ringgit or to imprisonment for a term not exceeding ten years or to both.

(2) For the purposes of subsection (1), "national critical information infrastructure entity" and "national critical information infrastructure" have the meaning assigned to them in the Cyber Security Act 2024 [*Act 854*].

PART VII

ENFORCEMENT

Authorization of public officer or officer of Commission

26. (1) The Minister may in writing authorize—

(a) any public officer; or

(b) with the concurrence of the Minister charged with the responsibility for communications, any officer of the Commission,

to exercise the powers of enforcement under this Act.

(2) Any such officer authorized under subsection (1) shall be deemed to be a public servant within the meaning of the Penal Code.

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

(4) Whenever an officer authorized under subsection (1) 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 (3).

Power of investigation

27. (1) An authorized officer shall have all the powers necessary to carry out an investigation 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

28. (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 an authorized officer—

(a) to search and seize—

(i) any computer system or part of the computer system;

(ii) any computer data in a computer system or part of the computer system;

(iii) any computer data storage medium containing computer data;

(iv) any book, account, document, signboard, card, letter, pamphlet, leaflet or notice, which contains or are reasonably suspected to contain information as to any offence so suspected to have been committed; or

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

(b) to activate any on-site computer system and computer data storage medium;

(c) to make and retain a copy of computer data;

(d) to maintain the integrity of the relevant computer data;

(e) to render inaccessible or remove computer data in the accessed computer system; or

(f) to take a printout of output of computer data.

(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 or amount, it is not practicable to remove any computer system or part of the computer system, computer data, computer data storage medium, book, account, document, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter seized under this section, the authorized officer who effected the seizure shall, by any means, seal such computer system or part of the computer system, computer data, computer data storage medium, book, account, document, 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 seal referred to in subsection (6) or removes any computer system or part of the computer system, computer data, computer data storage medium, book, account, document, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter under seal 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 three years or to both.

(8) If a search under this section indicates that there is any interference-causing equipment, radio apparatus or radio-sensitive equipment causing interference to the search, the authorized officer may direct the owner or the person in control of the equipment or apparatus or the premises in which the equipment or apparatus is located to take necessary steps to eliminate the interference.

Search and seizure without warrant

29. 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 28 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 28 in as full and ample a manner as if he were authorized to do so by a warrant issued under that section.

Warrant admissible notwithstanding defect

30. A search warrant issued under this Act shall be valid and enforceable notwithstanding any defect, mistake or omission in the search warrant or in the application for such warrant and any computer system or part of the computer system, computer data, computer data storage medium, book, account, document, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter seized under such warrant shall be admissible in evidence in any proceedings under this Act.

List of things seized

31. (1) Where any seizure is made under this Part, an authorized officer making the seizure shall prepare a list of computer system or part of the computer system, computer data, computer data storage medium, book, account, document, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter seized and of the premises in which it is found and shall sign the list.

(2) The list prepared in accordance with subsection (1) shall be delivered immediately to—

(a) the occupant of the premises where any computer system or part of the computer system, computer data, computer data storage medium, book, account, document, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter seized is found; and

(b) the person in control or in charge of the vehicle, where the seizure is made under section 29.

(3) Where the seizure is made in or from any premises which are unoccupied, the authorized officer shall whenever possible post a list of things seized conspicuously at the premises.

Cost of holding things seized

32. Where any computer system or part of the computer system, computer data, computer data storage medium, book, account, document, 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 things seized

33. (1) Where any computer system or part of the computer system, computer data, computer data storage medium, book, account, document, 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 Public Prosecutor, release the computer system or part of the computer system, computer data, computer data storage medium, book, account, document, 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 computer system or part of the computer system, computer data, computer data storage medium, book, account, document, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter if he is satisfied that the computer system or part of the computer system, computer data, computer data storage medium, book, account, document, 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 computer system or part of the computer system, computer data, computer data storage medium, book, account, document, 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 computer system or part of the computer system, computer data, computer data storage medium, book, account, document, 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 Public Prosecutor as soon as practicable.

Forfeiture of things seized

34. (1) Any computer system or part of the computer system, computer data, computer data storage medium, book, account, document, 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 computer system or part of the computer system, computer data, computer data storage medium, book, account, document, 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 computer system or part of the computer system, computer data, computer data storage medium, book, account, document, 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 computer system or part of the computer system, computer data, computer data storage medium, book, account, document, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter seized under this Act, such computer system or part of the computer system, computer data, computer data storage medium, book, account, document, 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 thirty days from the date of service of a notice to the last known address of the person from whom the computer system or part of the computer system, computer data, computer data storage medium, book, account, document, 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 computer system or part of the computer system, computer data, computer data storage medium, book, account, document, 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 provided in this section.

(4) Any person asserting that he is the owner of the computer system or part of the computer system, computer data, computer data storage medium, book, account, document, 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 computer system or part of the computer system, computer data, computer data storage medium, book, account, document, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter is held that he claims the computer system or part of the computer system, computer data, computer data storage medium, book, account, document, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter.

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

(6) The Sessions Court Judge to whom a matter is referred under subsection (5) shall issue a summons requiring the person asserting that he is the owner of the computer system or part of the computer system, computer data, computer data storage medium, book, account, document, 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 Sessions Court Judge 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 computer system or part of the computer system, computer data, computer data storage medium, book, account, document, 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 Sessions Court Judge shall order the computer system or part of the computer system, computer data, computer data storage medium, book, account, document, 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 computer system or part of the computer system, computer data, computer data storage medium, book, account, document, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter forfeited or deemed to be forfeited shall be delivered to an authorized officer and shall be disposed of in accordance with the directions of the Sessions Court Judge.

Property in forfeited things

35. Any computer system or part of the computer system, computer data, computer data storage medium, book, account, document, 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 computer system or computer data

36. (1) Any authorized officer conducting a search under this Act shall be given access to a computer system or computer data in a computer system.

(2) For the purposes of subsection (1), 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 recorded information in the computer system or computer data.

No cost or damages arising from seizure to be recoverable

37. No person shall, in any proceedings before any court in respect of any computer system or part of the computer system, computer data, computer data storage medium, book, account, document, 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.

Expedited preservation of computer data

38. (1) If an authorized officer is satisfied that—

(a) any computer data is reasonably required for the purposes of an investigation into an offence under this Act; and

(b) there is a risk that the computer data may be destroyed or rendered inaccessible,

the authorized officer may, by written notice given to a person in possession or control of the computer system where the computer data is contained, require the person to ensure that the computer data specified in the written notice be preserved for the period and in the manner as may be specified in the written notice.

(2) The person to whom the written notice was given under subsection (1)—

(a) shall preserve the computer data for the period and in the manner as may be specified in the written notice; and

(b) shall not, without lawful authority, disclose the existence and content of the written notice and any matter relating to the preservation of computer data under subsection (1).

(3) Any person who contravenes subsection (2) commits an offence and shall, on conviction, be liable to a fine not exceeding one million ringgit and shall be liable to a further fine not exceeding one hundred thousand ringgit for every day or part of a day during which the offence continues after conviction.

Disclosure of computer data

39. (1) If an authorized officer is satisfied that any computer data is reasonably required for the purposes of an investigation into an offence under this Act, the authorized officer may, by written notice given to a person in possession or control of the computer system where the computer data is contained, require the person to disclose such computer data in the manner as may be specified in the written notice.

(2) The person to whom the written notice was given under subsection (1)—

(a) shall disclose the computer data in the manner as may be specified in the written notice; and

(b) shall not, without lawful authority, disclose the existence and content of the written notice and any matter relating to the disclosure of computer data under subsection (1).

(3) Any person who contravenes subsection (2) commits an offence and shall, on conviction, be liable to a fine not exceeding one million ringgit and shall be liable to a further fine not exceeding one hundred thousand ringgit for every day or part of a day during which the offence continues after conviction.

Real-time collection of traffic data

40. (1) If the Public Prosecutor considers that any traffic data associated with specified communications transmitted by means of a computer system is relevant for the purposes of any investigation into an offence under this Act, he may, on the application of an authorized officer, require any service provider, within the service provider's existing technical capabilities, to—

(a) collect or record traffic data in real-time by technical means; and

(b) provide the traffic data collected or recorded to the authorized officer.

(2) Where any person is charged with an offence under this Act, any information obtained by an authorized officer under this section, whether before or after the person is charged, shall be admissible in evidence at his trial.

(3) The service provider shall keep confidential the execution of any power provided for under this section and any matter relating to it.

(4) Any service provider who—

(a) fails to collect or record traffic data in real-time as required under paragraph 1*(a)*; or

(b) fails to provide the traffic data collected or recorded to the authorized officer as required under paragraph 1*(b)*,

commits an offence and shall, on conviction, be liable to a fine not exceeding one million ringgit and shall be liable to a further fine not exceeding one hundred thousand ringgit for every day or part of a day during which the offence continues after conviction.

(5) Any service provider who contravenes subsection (3) commits an offence and shall, on conviction, be liable to a fine not exceeding one million ringgit.

Interception of content data

41. (1) Notwithstanding the provisions of any other written law, the Public Prosecutor may, if he considers that any communication is likely to contain content data which is relevant for the purposes of any investigation into an offence under this Act, on the application of an authorized officer, require a service provider, within the service provider's technical capability—

(a) to intercept or retain by technical means a specified communication or communications of a specified description received or transmitted, or about to be received or transmitted by the service provider;

(b) to collect or record, by technical means and in real-time, content data contained in the communications referred to in paragraph *(a)*; or

(c) to assist the authorized officer in the interception, retention, collection or recording referred to in paragraphs *(a)* and *(b)*.

(2) The Public Prosecutor may authorize an authorized officer to enter any premises and to install on such premises, any device for the interception, retention, collection or recording of the communication or content data and to remove and retain such device.

(3) Where any person is charged with an offence under this Act, any information obtained by an authorized officer under this section, whether before or after the person is charged, shall be admissible in evidence at his trial.

(4) The service provider shall keep confidential the execution of any power provided for under this section and any matter relating to it.

(5) Any service provider who contravenes subsection (4) commits an offence and shall, on conviction, be liable to a fine not exceeding one million ringgit.

Power to require attendance of person acquainted with case

42. (1) An authorized officer making an investigation under this Act 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

43. (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 legally 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

44. (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

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

(a) to require the production of any computer system or part of the computer system, computer data, computer data storage medium, book, account, document, card, letter, pamphlet, leaflet, notice, thing or matter and to inspect, examine and make any copy 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 three years or to both.

Obstruction

46. Any person who assaults, impedes, obstructs or interferes with, or refuses access to any premises or a computer system or computer data to the 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 three years or to both.

Power of search and seizure without warrant, access to computer system or computer data etc., by police officer

47. For the purposes of sections 29, 36 and 41, where the authorized officer is a police officer, the powers under that sections shall only be exercised by a police officer not below the rank of Inspector.

General procedural powers

48. Notwithstanding any other written law, sections 36, 38, 39, 40 and 41 shall also apply in respect of—

(a) any investigation into offences under any other written law committed by means of a computer system; or

(b) the collection of evidence in electronic form for the purposes of any investigation or proceedings relating to an offence under any written law.

Jurisdiction to try offence

49. Notwithstanding any written law to the contrary, a Sessions Court shall have jurisdiction to try any offence under this Act.

PART VIII

MISCELLANEOUS

Integrated information system

50. (1) The Chief Executive shall establish, administer, maintain and manage an integrated information system containing such information received or gathered by the Chief Executive which may be used to prevent and investigate cybercrimes.

(2) For the purposes of subsection (1), the Chief Executive may, by written notice, request any person or Government Entity to provide any information relating to cybercrimes in such manner as may be determined by the Chief Executive.

(3) Any person or Government Entity to whom the written notice is given under subsection (2) may, to the extent permitted under any applicable written laws, provide to the Chief Executive the information as requested.

(4) Any person or Government Entity may, on its own initiative, provide to the Chief Executive any information relating to cybercrimes in such manner as may be determined by the Chief Executive and the Chief Executive may receive and retain such information.

(5) The Chief Executive may, to the extent permitted under the applicable written laws, disclose or share any information contained in the integrated information system with any Government Entity where such disclosure or sharing is necessary for the purposes of the prevention and investigation of cybercrimes.

(6) For the purposes of this section, "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.

General duty of service provider

51. (1) A service provider shall take necessary measures to prevent any services provided by the service provider from being used for the commission of cybercrimes.

(2) An authorized officer may, in consultation with the Commission, by written notice, require a service provider to take such measures to prevent the commission or attempted commission of any cybercrime, or to assist the enforcement in relation to such offence, in such manner as may be specified in the written notice.

(3) Any service provider who fails to comply with the written notice under subsection (2) commits an offence and shall, on conviction, be liable to a fine not exceeding one million ringgit or to imprisonment for a term not exceeding ten years or to both.

Obligation to retain computer data

52. (1) The Minister may, if he is satisfied that it is necessary in the interest of national security or public safety and proportionate to the purpose of prevention, investigation, detection or prosecution of any offence under any written law, by order published in the *Gazette*, require a service provider to retain certain computer data other than content data.

(2) The order referred to in subsection (1) shall contain the following particulars:

(a) type or category of computer data which shall be retained;

(b) the period during which the computer data shall be retained;

(c) the method of use of the retained computer data; and

(d) any other particulars as the Minister deems necessary for the purposes of the retention of the computer data.

(3) Any service provider who fails to comply with the order under subsection (1) commits an offence and shall, on conviction, be liable to a fine not exceeding one million ringgit or to imprisonment for a term not exceeding ten years or to both.

Service provider not liable for act done in good faith

53. Any service provider or any of his employees, shall not be liable in any criminal or civil proceedings of any nature, for any damages, including punitive damages, loss, cost or expenditure suffered or to be suffered, whether directly or indirectly, for any act or omission done in good faith, in the performance of the duty imposed under section 51.

Power of court to make certain orders

54. (1) Where on an application by the Public Prosecutor or authorized officer, as the case may be, it appears to the court that—

(a) there is reasonable likelihood that any person will contravene any provision of this Act; or

(b) any person has contravened a provision of this Act and that there are steps which could be taken to remedy the contravention,

whether or not that person has been charged with an offence in respect of the contravention or whether or not a contravention has been proved in a prosecution, the court may, without prejudice to any order it would be entitled to make otherwise than pursuant to this section, make all or any of the following orders:

(A) an order restraining or requiring the cessation of the contravention;

(B) an order requiring that person, or any other person, who appears to have been knowingly involved in the contravention, to take such steps as the court may direct to remedy it or to mitigate its effect including making restitution to any other person aggrieved by such contravention;

(C) for the purpose of securing compliance with any other order under this section, an order directing a person to do or refrain from doing a specified act;

(D) an order restraining the person from acquiring, disposing of or otherwise dealing with property which the court is satisfied such person is reasonably likely to dispose of or otherwise deal with the property;

(E) where a person has refused or failed, or is refusing or failing, or is proposing to refuse or fail, to do any act that the person is required to do under any provision of this Act, an order requiring such person to do such act; or

(F) any ancillary order deemed to be desirable in consequence of the making of an order under paragraph (A), (B), (C), (D) or (E).

(2) If an application is made to a court for an order under subsection (1), the court may, if in its opinion it is desirable to do so, before considering the application, make an interim order and such order shall be expressed to have effect pending the determination of the application.

(3) Where an application is made to the court for an order under paragraph (1)(E), the court may grant the order—

(a) where the court is satisfied that the person has refused or failed to do the required act, whether or not it appears to the court that the person intends to again refuse or fail, or continue to refuse or fail, to do the required act; or

(b) where it appears to the court that in the event that such an order is not granted, it is likely that the person will refuse or fail to do the required act, whether or not the person has previously refused or failed to do the act or whether or not there is any imminent risk of damage to any person if the person required to do such act or thing refuses or fails to do so.

(4) Where an application for an order under subsection (1) is made by the Public Prosecutor or authorized officer, the court shall not, as a condition of the grant of the order, require any undertaking as to damages to be given by or on behalf of the Public Prosecutor or authorized officer, as the case may be.

(5) The court may rescind, vary or discharge an order made by it under this section or suspend the operation of such an order.

Service of notice

55. (1) Every notice or any other documents required to be served on any person under this Act may be served—

(a) personally upon the person;

(b) by sending it to the person by registered post; or

(c) by electronic means.

(2) The notice or other documents sent by registered post to a person shall be deemed to have been served on that person at the time at which it would have been delivered to that person in the ordinary course of the post if the notice or other document was addressed—

(a) in the case of a company, limited liability partnership, firm, society or other body of persons—

(i) to its registered office;

(ii) to its last-known address; or

(iii) to any person authorized by it to accept service of process; and

(b) in the case of an individual, to his last known address.

(3) Where a person has given his consent for a notice or document to be served on him through electronic means, the notice or document shall be deemed to have been served at the time when the electronic notice or document is transmitted to his account through the electronic means.

Attempt and abetment

56. Any person who attempts to commit or abets the commission of any offence under this Act shall, on conviction, be liable to the punishment provided for such offence.

Protection against suit and legal proceedings

57. 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

58. 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.

59. 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; or

(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.

60. 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.

Repeal and savings

61. (1) The Computer Crimes Act 1997 [*Act 563*] (the "repealed Act") is repealed.

(2) Any reference in any written law to a provision of the repealed Act relating to access to any program or data held in a computer shall, on the date of coming into operation of this Act, be construed as a reference to the provisions of this Act relating to access to a computer system.

(3) Any investigation, trial, proceedings or action done, taken or commenced under the repealed Act immediately before the date of coming into operation of this Act, shall, on the date of coming into operation of this Act, be dealt with as if the repealed Act has not been repealed by this Act.

EXPLANATORY STATEMENT

This Bill ("the proposed Act") seeks to repeal the Computer Crimes Act 1997 [*Act 563*] and to establish a new and comprehensive legal framework to prevent and combat cybercrimes, being offences provided for under Parts III to VI of the proposed Act and offences under any other written law committed by means of a computer system. The proposed Act seeks to strengthen the legal framework relating to cybercrimes through the criminalization of certain acts involving the use of computer systems and the strengthening of powers relating to the investigation and prosecution of cybercrimes. The proposed Act is necessitated by the rapid advancement of digital technology, the borderless nature of cyberspace and the increasing sophistication of cybercrime activities which threaten national security, the economy, public order and the safety of persons. In drafting the proposed Act, consideration has also been given to relevant international instruments relating to cybercrimes, including the Budapest Convention on Cybercrime and the United Nations Convention against Cybercrime, in line with Malaysia's commitment towards strengthening efforts in addressing cybercrime-related threats. The proposed Act provides, among others, for the extra-territorial application of offences, the establishment of the Committee on Combating Cybercrimes and various categories of offences, including offences relating to the confidentiality, integrity and availability of computer system and computer data, offences relating to computer-related forgery and computer-related fraud, offences relating to the national digital identity service and other cybercrime-related offences. The proposed Act further provides for enforcement powers, the establishment of an integrated information system, the duties of service providers as well as other related provisions.

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 the provision on the commencement of the proposed Act.

4. *Clause 2* seeks to provide for the extra-territorial application of the proposed Act.

5. *Clause 3* contains the definitions of certain words and expressions used in the proposed Act.

PART II

6. Part II of the proposed Act deals with the establishment of the Committee on Combating Cybercrimes ("Committee").

7. *Clause 4* seeks to provide for the establishment and membership of the Committee.

8. *Clause 5* seeks to provide for the functions of the Committee which include, among others, to plan, formulate and decide on approaches and strategies in preventing and combating cybercrimes.

9. *Clause 6* seeks to provide for meetings of the Committee. This *clause* also provides that the Committee may determine its own procedure.

10. *Clause 7* 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.

11. *Clause 8* seeks to provide that the Committee may establish subcommittees to assist the Committee in the performance of its functions under the proposed Act.

PART III

12. Part III of the proposed Act provides for offences relating to the confidentiality, integrity and availability of computer system and computer data.

13. *Clause 9* seeks to explain when a person secures access to a computer system and secures access to a computer system without authority for the purposes of other offences under the proposed Act.

14. *Clause 10* seeks to provide for the offence of intentionally and without authority or without lawful purpose securing access to the whole or any part of a computer system. Any person who commits an offence under this *clause* shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding three years or to both.

15. *Clause 11* seeks to provide that any person who commits an offence under *clause 10* of the proposed Act with the intention to commit a further offence involving fraud or dishonesty or which causes injury as defined in the Penal Code [*Act 574*] or to facilitate the commission of such further offence whether by himself or by any other person commits an offence under this *clause* and shall, on conviction, be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding seven years or to both.

16. *Clause 12* seeks to provide for the offence of intentionally and without authority or without lawful purpose intercepting by technical means, any non-public transmission of computer data to, from or within a computer system including any electromagnetic emissions from a computer system carrying computer data. Any person who commits an offence under this *clause* shall, on conviction, be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding seven years or to both.

17. *Clause 13* seeks to provide for the offence of intentionally and without authority or without lawful purpose damaging, deleting, deteriorating, altering, suppressing or modifying computer data, rendering computer data meaningless, useless or ineffective, obstructing, interrupting or interfering with the lawful use of computer data or denying access to computer data to any person entitled to it. Any person who commits an offence under this *clause* shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding three years or to both.

18. *Clause 14* seeks to provide for the offence of intentionally and without authority or without lawful purpose inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data so as to seriously hinder or interfere with the functioning of a computer system or lawful use or operation of a computer system. Any person who commits an offence under this *clause* shall, on conviction, be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding seven years or to both.

19. *Clause 15* seeks to provide for the offence of intentionally and without authority or without lawful purpose obtaining, procuring for using, producing, selling, importing or exporting, distributing, disclosing or otherwise making available a device including a program, that is designed or adapted primarily for the purpose of committing any offence under the proposed Act or a password, access credentials, electronic signature or similar computer data by which the whole or any part of a computer system or computer data is capable of being accessed with the intention that it be used by himself or any other person for the purpose of committing an offence under the proposed Act. Any person who commits an offence under this *clause* shall, on conviction, be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding seven years or to both. This *clause* also seeks to provide that any person who has in his possession or control any of the device or password, access credentials, electronic signature or computer data referred to in

subclause 15(1) of the proposed Act with the intention that the device or password, access credentials, electronic signature or computer data be used by himself or by any other person for the purpose of committing any offence under the proposed Act, commits an offence and shall, on conviction, be liable to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding five years or to both. An example of a situation in which a person commits an offence under this *clause* is where the person produces a computer program with the intention that the program be used to create fake websites to obtain information from members of the public who access such websites, as the program is capable of being used by another person to commit computer-related fraud under *clause 17*. A person who procures for use such computer program with the intention of committing computer-related fraud also commits an offence under this *clause*.

Part IV

20. Part IV of the proposed Act provides for offences relating to computer-related forgery and computer-related fraud.

21. *Clause 16* seeks to provide for the offence of computer-related forgery, being the offence of intentionally and without authority or without lawful purpose inputting, altering, deleting or suppressing computer data resulting in inauthentic computer data with the intention that such computer data be considered or acted upon for any legal purpose as if the computer data were authentic, whether or not such computer data is intended to deceive any particular person. Any person who commits an offence under this *clause* shall, on conviction, in the case where valuable security is involved, be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding seven years or to both or in any other case, be liable to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding five years or both.

22. *Clause 17* seeks to provide for the offence of computer-related fraud, being the offence of intentionally and without authority or without lawful purpose inputting, altering, deleting or suppressing any computer data, interfering with the functioning of a computer system or causing deception as to factual circumstances by means of a computer system that causes a person to do or omit to do anything which that person would not otherwise do or omit to do, so as to cause loss of property to another person with the fraudulent or dishonest intention to procure without authority economic benefit for himself or for another person. Any person who commits an offence under this *clause* shall, on conviction, be liable to a fine not exceeding one million ringgit or to imprisonment for a term not exceeding ten years or to both.

PART V

23. Part V of the proposed Act provides for offences relating to national digital identity service, which is the electronic service owned by the Federal Government by which a user's identity is verified and authenticated.

24. *Clause 18* contains the definitions of "credential", "user" and "national digital identity service" used in Part V of the proposed Act. The term "user" is defined as a person who is registered with the national digital identity service.

25. *Clause 19* seeks to provide for the offence of a user disclosing his national digital identity service password or providing any other means of securing access in the identity of the user to any program or computer data in any computer system by means of the national digital identity service, to any person knowing or having reasonable grounds to believe that the purpose of the disclosure or provision is for any person to commit or to facilitate the commission by any person of, any offence under any written law. Any person who commits an offence under this *clause* shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding three years or to both. This *clause* also seeks to provide for a rebuttable presumption that the user has reasonable grounds to believe that the disclosure or provision is for the commission of, or to facilitate the commission of, an offence under any written law if it is proved in any proceedings for an offence under this *clause* that the user discloses his national digital identity service password or provides any other means of securing access in the identity of the user to any person for any gain whether or not the gain is a wrongful gain or realized or knowing that the disclosure or provision is likely to cause wrongful loss to any person.

26. *Clause 20* seeks to provide for the offence of obtaining, retaining, supplying, offering to supply, transmitting or otherwise making available any credential of any user for the purpose of committing or facilitating the commission of, any offence under any written law or knowing or having reason to believe that the credential will be used, or is likely to be used, for the commission of, or to facilitate the commission of, any offence under any written law. Any person who commits an offence under this *clause* shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding three years or to both, and for a second or subsequent offence, to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding five years or to both.

PART VI

27. Part VI of the proposed Act provides for other offences relating to cybercrimes such as wrongful communication, identity theft, transmission of content generated or manipulated by means of computer system and dissemination of intimate images. This Part also provides for enhanced punishments for certain offences under the proposed Act which affects or involves national critical information infrastructure entities or national critical information infrastructure.

28. *Clause 21* seeks to provide for the offence of communicating directly or indirectly a number, code, password or other means of access to a computer system to any person other than a person to whom he is duly authorized to communicate the number, code, password or other means of access to the computer system. Any person who commits an offence under this *clause* shall, on conviction, be liable to a fine not exceeding three hundred thousand ringgit or to imprisonment for a term not exceeding five years or to both.

29. *Clause 22* seeks to provide for the offence of identity theft being the offence of intentionally and without authority or without lawful purpose by means of a computer system, obtaining, supplying, using or having in possession or control any identity information of another person with the intention to commit or facilitate the commission of any offence under any written law. Any person who commits an offence under this *clause* shall, on conviction, be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding seven years or to both.

30. *Clause 23* seeks to provide for the offence of transmitting, distributing, publishing, selling or offering for sale or otherwise making available, any visual or audio content generated or manipulated, whether wholly or partly, by means of a computer system, resembling existing persons, objects, places, entities or events that falsely appears to a person to be authentic or truthful with the intention to commit or facilitate the commission of any offence under any written law, whether by himself or by any other person. Any person who commits an offence under this *clause* shall, on conviction, be liable to a fine not exceeding five hundred thousand ringgit or to imprisonment for a term not exceeding seven years or to both.

31. *Clause 24* seeks to provide for the offence of disseminating intimate images of any person by transmitting, distributing, publishing, selling or offering for sale or otherwise making available the intimate image by means of a computer system. Any person who commits an offence under this *clause* shall, on conviction, be liable to imprisonment for a term not exceeding five years or to a fine not exceeding three hundred thousand ringgit or to both. This *clause* also seeks to provide for enhanced punishment where an offence under this *clause* is committed with the intention to cause humiliation or harm to, or to coerce or intimidate, the person depicted in the intimate image. Based on the definition of "intimate image" provided for under the proposed Act, the intimate image may include images, videos or visual depictions that are wholly or partly generated, manipulated, altered or synthesized through artificial intelligence, machine learning, deepfake technology or other automated digital technologies, including content generated using generative artificial intelligence platforms and such image depicts a person's sexual parts or portrays the person as being engaged in sexual activity. This *clause* is intended to address the misuse of emerging technologies to create and disseminate fabricated or manipulated intimate images, irrespective of whether the image is authentic, digitally altered or entirely computer-generated.

32. *Clause 25* seeks to provide for enhanced punishment for commission of offences under Parts III and IV and *clauses 21*, *22* and *23* of the proposed Act which affect or involve a national critical information infrastructure entity or national critical information infrastructure. Any person who commits such offence shall, on conviction, where the offence causes loss of life, be liable to imprisonment for a term of not less than thirty years but not exceeding forty years or to a fine not exceeding two million ringgit or to both. Where such offence causes any injury to any person, be liable to imprisonment for a term not exceeding fifteen years or to a fine not exceeding one million and five hundred thousand ringgit or to both and in any other case be liable to a fine not exceeding one million ringgit or to imprisonment for a term not exceeding ten years or to both.

PART VII

33. Part VII of the proposed Act deals with enforcement provisions.

34. *Clause 26* seeks to provide that the Minister may authorize any public officer, or with the concurrence of the Minister charged with the responsibility for communications, any officer of the Malaysian Communications and Multimedia Commission, to exercise the powers of enforcement under the proposed Act.

35. *Clause 27* seeks to provide for the power of investigation of the authorized officers.

36. *Clause 28* deals with the provision relating to search and seizure with warrant.

37. *Clause 29* deals with the provision relating to search and seizure without warrant.

38. *Clause 30* seeks to provide that a search warrant issued under the proposed Act shall be valid and enforceable notwithstanding any defect, mistake or omission in the search warrant.

39. *Clause 31* seeks to require an authorized officer to prepare a list of things seized in the course of his investigation.

40. *Clause 32* 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.

41. *Clause 33* seeks to provide for the release of any thing seized under the proposed Act.

42. *Clause 34* deals with the provision relating to the forfeiture of any thing seized under the proposed Act.

43. *Clause 35* seeks to provide that any thing forfeited or deemed to be forfeited under the proposed Act shall be the property of the Federal Government.

44. *Clause 36* seeks to provide for the access to computer system and computer data by the authorized officer.

45. *Clause 37* 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 made without reasonable cause.

46. *Clause 38* seeks to provide that if an authorized officer is satisfied that any computer data is reasonably required for the purposes of an investigation into an offence under the proposed Act and there is a risk that the computer data may be destroyed or rendered inaccessible, the authorized officer may, by written notice given to a person in possession or control of the computer system where the computer data is contained, require the person to ensure that the computer data be preserved for the period and in the manner as may be specified in the written notice.

47. *Clause 39* seeks to empower an authorized officer to require by written notice a person in possession or control of the computer system where the computer data is contained to disclose such computer data in the manner as specified in the written notice if the authorized officer is satisfied that the computer data is reasonably required for the purposes of an investigation into an offence under the proposed Act.

48. *Clause 40* seeks to provide that a Public Prosecutor may, on the application of an authorized officer, require any service provider to collect or record traffic data in real-time by technical means and provide the traffic data to the authorized officer within the service provider's existing technical capability, if the Public Prosecutor considers that the traffic data associated with specified communications transmitted by means of a computer system is relevant for the purposes of any investigation into an offence under the proposed Act.

49. *Clause 41* seeks to provide that a Public Prosecutor may, on the application of an authorized officer, require the service provider, within the service provider's technical capability, to intercept or retain a specified communication or communications of a specified description, to collect or record, by technical means any content data, in real-time, contained in such communications or to assist the authorized officer in the interception, retention, collection or recording if the Public Prosecutor considers that the communications is likely to contain content data which is relevant for the purposes of an investigation into an offence under the proposed Act.

50. *Clause 42* 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.

51. *Clause 43* 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.

52. *Clause 44* 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.

53. *Clause 45* deals with additional powers of an authorized officer for the purposes of the execution of the proposed Act.

54. *Clause 46* seeks to provide that it shall be an offence for any person who obstructs any authorized officer in the performance of their duties under the proposed Act.

55. *Clause 47* seeks to provide that for the purposes of search and seizure without warrant under *clause 29,* access to computer system or computer data under *clause* 36 and interception of content data under *clause 41*, where the authorized officer is a police officer, the powers under those *clauses* shall only be exercised by a police officer not below the rank of Inspector.

56. *Clause 48* seeks to provide that, notwithstanding any other written law, *clauses 36, 38, 39, 40* and *41* of the proposed Act shall also apply in respect of any investigation into any offences committed by means of a computer system under any other written law and the collection of evidence in electronic form for the purposes of any investigation or proceedings relating to an offence under any written law.

57. *Clause 49* seeks to provide for the jurisdiction of a Sessions Court to try any offence under the proposed Act notwithstanding any written law to the contrary.

PART VIII

58. Part VIII of the proposed Act deals with miscellaneous provisions.

59. *Clause 50* seeks to provide for the establishment, administration, maintenance and management of an integrated information system by the Chief Executive of the National Cyber Security Agency ("Chief Executive") which contains information received or gathered by the Chief Executive which may be used to prevent and investigate cybercrimes.

60. *Clause 51* seeks to provide for the general duty of service provider to take necessary measures to prevent any services that it provides from being used for the commission of cybercrimes. A service provider who fails to comply with the written notice given under this *clause* commits an offence and shall, on conviction, be liable to a fine not exceeding one million ringgit or to imprisonment for a term not exceeding ten years or to both.

61. *Clause 52* seeks to empower the Minister, where the Minister is satisfied that it is necessary in the interest of national security or public safety and proportionate to the purpose of the prevention, investigation, detection or prosecution of any offence under any written law, to require a service provider, by an order published in the *Gazette*, to retain certain computer data other than content data. This *clause* further seeks to provide for the particulars to be specified in the order, including the type or category of computer data which shall be retained, the retention period of the computer data, the method of use of the computer data and any other particulars which the Minister deems necessary for the purposes of the retention of the computer data. This *clause* also seeks to provide that a service provider who fails to comply with the order commits an offence and shall, on conviction, be liable to a fine not exceeding one million ringgit or to imprisonment for a term not exceeding ten years or to both.

62. *Clause 53* seeks to provide that any service provider or any of his employees, shall not be liable in any criminal or civil proceedings of any nature, for any damages, including punitive damages, loss, cost or expenditure suffered or to be suffered, whether directly or indirectly, for any act or omission done in good faith, in the performance of the duty imposed under *clause 51* of the proposed Act.

63. *Clause 54* seeks to empower the court to make certain orders upon application by the Public Prosecutor or authorized officer if it appears to the court that there is reasonable likelihood that any person will contravene any provision of the proposed Act or any person has contravened a provision of the proposed Act and that there are steps which could be taken to remedy the contravention.

64. *Clause 55* seeks to provide for the service of notice or other documents required to be served on any person under the proposed Act.

65. *Clause 56* seeks to provide that any person who attempts to commit or abets the commission of any offence under the proposed Act shall, on conviction, be liable to the punishment provided for such offence.

66. *Clause 57* 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 58* seeks to provide that no prosecution shall be instituted for any offence under the proposed Act without the written consent of the Public Prosecutor.

68. *Clause 59* 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 60* 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 61* seeks to provide for the repeal and savings provisions.

FINANCIAL IMPLICATIONS

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

[PN(U2)3438]