LAWS OF BRUNEI

CHAPTER 272
CYBERSECURITY

S 20/2023

REVISED EDITION 2024

LAWS OF BRUNEI

REVISED EDITION 2024

CHAPTER 272

CYBERSECURITY

ARRANGEMENT OF SECTIONS

Section

PART 3

CRITICAL INFORMATION INFRASTRUCTURE

PART 4

RESPONSES TO CYBERSECURITY THREATS AND INCIDENTS

PART 5

GENERAL

CYBERSECURITY ACT

An Act to require or authorise the taking of measures to prevent, manage and respond to cybersecurity threats and incidents, to regulate owners of critical information infrastructure and for matters related thereto

Commencement: 20th May 2023

PART 1

PRELIMINARY

Citation

1. This Act may be cited as the Cybersecurity Act.

Interpretation

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

"Assistant Commissioner" means any Assistant Commissioner of Cybersecurity appointed under section 5(3);

"business entity" means —

(a) a corporation as defined in section 2(1) of the Companies Act (Chapter 39);

(b) an unincorporated association;

(c) a partnership; or

(d) a limited liability partnership registered under the Limited Liability Partnerships Order, 2010 (S 117/2010);

"code of practice" means any code of practice issued or approved under section 13(1);

"Commissioner" means the Commissioner of Cybersecurity appointed under section 5(1);

"computer" means an electronic, magnetic, optical, electrochemical or other data processing device performing logical, arithmetic or storage functions, and includes any data storage facility or communications

facility directly related to or operating in conjunction with such device, but does not include such device as the Minister may, by notification published in the *Gazette*, prescribe;

"computer program" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function;

"computer service" includes computer time, data processing and the storage or retrieval of data;

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

(a) an information technology system; and

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

"critical information infrastructure" means a computer or a computer system in respect of which a designation under section 9(1) is in effect;

"cybersecurity" means the state in which a computer or computer system is protected from unauthorised access or attack, and because of that state —

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

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

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

"cybersecurity incident" means an act or activity carried out without lawful authority on or through a computer or computer system that jeopardises or adversely affects its cybersecurity or the cybersecurity of another computer or computer system;

"cybersecurity officer" means any cybersecurity officer appointed under section 5(5);

"cybersecurity program" means any computer program designed for, or purported to be designed for, ensuring or enhancing the cybersecurity of a computer or computer system;

"cybersecurity service" means a service provided by a person for reward that is intended primarily for or aimed at ensuring or safeguarding the cybersecurity of a computer or computer system belonging to another person (*A*), and includes the following —

(a) assessing, testing or evaluating the cybersecurity of *A*'s computer or computer system by searching for vulnerabilities in, and compromising, the cybersecurity defences of the computer or computer system;

(b) conducting a forensic examination of *A*'s computer or computer system;

(c) investigating and responding to a cybersecurity incident that has affected *A*'s computer or computer system by conducting a thorough scan and examination of the computer or computer system to identify and remove elements relating to, and identify the root cause of, the cybersecurity incident, and which involves circumventing the controls implemented in the computer or computer system;

(d) conducting a thorough examination of *A*'s computer or computer system to detect any cybersecurity threat or incident that may have already penetrated the cybersecurity defences of the computer or computer system, and that may have evaded detection by conventional cybersecurity solutions;

(e) designing, selling, importing, exporting, installing, maintaining, repairing or servicing of one or more cybersecurity solutions;

(f) monitoring of the cybersecurity of *A*'s computer or computer system by acquiring, identifying and scanning information that is stored in, processed by, or transmitted through the computer or computer system for the purpose of identifying cybersecurity threats to the computer or computer system;

(g) maintaining control of the cybersecurity of *A*'s computer or computer system by effecting management, operational and technical controls for the purpose of protecting the computer or computer system against any unauthorised effort to adversely affect its cybersecurity;

(h) assessing or monitoring the compliance of an organisation with the organisation's cybersecurity policy;

(i) providing advice in relation to cybersecurity solutions, including —

(i) providing advice on a cybersecurity program; or

(ii) identifying and analysing cybersecurity threats and providing advice on solutions or management strategies to minimise the risk posed by cybersecurity threats;

(j) providing advice in relation to any practice that can enhance cybersecurity;

(k) providing training or instruction in relation to any cybersecurity service, including the assessment of the training, instruction or competencies of another person in relation to any such activity;

"cybersecurity service provider" means a person who provides a cybersecurity service;

"cybersecurity solution" means any computer, computer system, computer program or computer service designed for, or purported to be designed for, ensuring or enhancing the cybersecurity of another computer or computer system;

"cybersecurity threat" means an act or activity (whether known or suspected) carried out on or through a computer or computer system that may imminently jeopardise or affect adversely, without lawful authority, the cybersecurity of that or another computer or computer system;

"cybersecurity vulnerability" means any vulnerability in a computer or computer system that can be exploited by one or more cybersecurity threats;

"Deputy Commissioner" means the Deputy Commissioner of Cybersecurity appointed under section 5(3);

"essential service" means any service essential to the national security, defence, foreign relations, economy, public health, public safety or public order of Brunei Darussalam and specified in the Schedule;

"Minister" means the Minister of Transport and Infocommunications;

"owner", in relation to a critical information infrastructure, means the legal owner of the critical information infrastructure and, where the critical information infrastructure is jointly owned by more than one person, includes every joint owner;

"standard of performance" means any standard of performance issued or approved under section 13(1).

Application of Act

3. (1) Part 3 (except section 10) applies to any critical information infrastructure located wholly or partly in Brunei Darussalam.

(2) Section 10 applies to any computer or computer system located wholly or partly in Brunei Darussalam.

Act binds Government

4. (1) Except as provided in subsection (2), this Act shall bind the Government.

(2) Nothing in this Act shall render the Government liable to prosecution for an offence.

(3) For the avoidance of doubt, no person shall be immune from prosecution for any offence against this Act by reason that the person is engaged to provide services to the Government.

PART 2

ADMINISTRATION

Appointment of Commissioner of Cybersecurity and other officers

5. (1) The Minister may, with the consent of His Majesty the Sultan and Yang Di-Pertuan, appoint a Commissioner of Cybersecurity for the purposes of this Act.

(2) Subject to any general or special direction of the Minister, the Commissioner is responsible for the administration of this Act and may perform such duties and functions as are imposed and exercise such powers as are conferred on the Commissioner by this Act.

(3) The Minister may, with the consent of His Majesty the Sultan and Yang Di-Pertuan, appoint a Deputy Commissioner of Cybersecurity and one or more Assistant Commissioners of Cybersecurity to assist the Commissioner in the discharge of the Commissioner's duties and functions.

(4) The Minister may, with the consent of His Majesty the Sultan and Yang Di-Pertuan, appoint as an Assistant Commissioner under subsection (3) in respect of a critical information infrastructure —

(a) a public officer of another Ministry; or

(b) an employee of a statutory body under the charge of another Minister,

where that other Ministry or statutory body has supervisory or regulatory responsibility over an industry or a sector to which the owner of the critical information infrastructure belongs.

(5) The Commissioner may, in writing, appoint such number of persons as cybersecurity officers as the Commissioner thinks necessary for carrying this Act into effect.

(6) The Deputy Commissioner may exercise all the powers, duties and functions of the Commissioner except those exercisable under section 9 or 11.

(7) Subject to such conditions or limitations as the Commissioner may specify, an Assistant Commissioner or a cybersecurity officer may exercise all the powers, duties and functions of the Commissioner as may be delegated to that Assistant Commissioner or cybersecurity officer in writing, except —

(a) in the case of an Assistant Commissioner, those powers, duties or functions exercisable under this subsection or section 7, 9, 11 or 22(5); and

(b) in the case of a cybersecurity officer, those powers, duties or functions exercisable under this subsection or section 7, 9, 11, 13, 14 or 22(5).

Duties and functions of Commissioner

6. The Commissioner has the following duties and functions —

(a) to oversee and promote the cybersecurity of computers and computer systems in Brunei Darussalam;

(b) to advise the Government or any other public authority on national needs and policies in respect of cybersecurity matters generally;

(c) to monitor cybersecurity threats, whether such cybersecurity threats occur in or outside Brunei Darussalam;

(d) to respond to cybersecurity incidents that threaten the national security, defence, economy, foreign relations, public health, public order or public safety, or any essential services, of Brunei Darussalam, whether such cybersecurity incidents occur in or outside Brunei Darussalam;

(e) to identify and designate critical information infrastructure and to regulate owners of critical information infrastructure with regard to the cybersecurity of the critical information infrastructure;

(f) to establish cybersecurity codes of practice and standards of performance for implementation by owners of critical information infrastructure;

(g) to represent the Government on cybersecurity issues internationally;

(h) to cooperate with computer emergency response teams (CERTs) of other countries or territories on cybersecurity incidents;

(i) to develop and promote the cybersecurity services industry in Brunei Darussalam;

(j) to establish standards within Brunei Darussalam in relation to cybersecurity products or services and the recommended level of cybersecurity of computer hardware or software, including certification or accreditation schemes;

(k) to promote, develop, maintain and improve competencies and professional standards of persons working in the field of cybersecurity;

(l) to support the advancement of technology and research and development relating to cybersecurity;

(m) to promote awareness of the need for and the importance of cybersecurity in Brunei Darussalam;

(n) to perform such other functions and discharge such other duties as may be conferred on the Commissioner under any other written law.

Appointment of authorised officers

7. (1) The Commissioner may, with the approval of the Minister, in writing appoint any authorised officer to assist the Commissioner in exercising the powers under Part 4.

(2) In exercising any of the powers of enforcement under Part 4, an authorised officer shall, on demand, produce to the person against whom the authorised officer is acting the authority issued to the authorised officer by the Commissioner.

(3) All authorised officers are deemed to be public servants for the purposes of the Penal Code (Chapter 22).

Committees

8. (1) The Minister may appoint such committees as the Minister thinks fit to assist or advise the Commissioner on such matters arising out of his functions as the Commissioner under this Act.

(2) The Commissioner may define or vary the terms of reference of the committees.

(3) Subject to this Act and to the control of the Commissioner, each committee may regulate its procedure in such manner as the committee thinks fit.

PART 3

CRITICAL INFORMATION INFRASTRUCTURE

Designation of critical information infrastructure

9. (1) The Commissioner may, by written notice to the owner of a computer or computer system, designate the computer or computer system as a critical information infrastructure for the purposes of this Act, if the Commissioner is satisfied that —

(a) the computer or computer system is necessary for the continuous delivery of an essential service and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Brunei Darussalam; and

(b) the computer or computer system is located wholly or partly in Brunei Darussalam.

(2) A notice issued under subsection (1) shall —

(a) identify the computer or computer system that is being designated as a critical information infrastructure;

(b) identify the owner of the computer or computer system so designated as a critical information infrastructure;

(c) inform the owner of the computer or computer system, regarding the duties and responsibilities of the owner under this Act that arise from the designation;

(d) provide the name and contact particulars of the officer assigned by the Commissioner to supervise the critical information infrastructure;

(e) inform the owner of the computer or computer system that any representation against the designation is to be made to the Commissioner by a specified date, being a date not earlier than 14 days after the date of the notice; and

(f) inform the owner of the computer or computer system that the owner may appeal to the Minister against the designation and provide information on the applicable procedure.

(3) Any designation under subsection (1) has effect for a period of 5 years, unless it is withdrawn by the Commissioner before the expiry of the period.

(4) The person who receives a notice under subsection (1) may request the Commissioner to proceed under subsection (5) on showing proof that —

(a) the person is not able to comply with the requirements in this Part for the reason that the person has neither effective control over the operations of the computer or computer system, nor the ability or right to carry out changes to the computer or computer system; and

(b) another person has effective control over the operations of the computer or computer system and the ability and right to carry out changes to the computer or computer system.

(5) If the Commissioner is satisfied that the conditions mentioned in subsection (4)*(a)* and *(b)* are met, the Commissioner may amend the notice issued to the person under subsection (1) and address and send that amended notice to the person mentioned in subsection (4)*(b)*.

(6) During the period when a notice amended under subsection (5) is in effect, the provisions of this Part apply to the person mentioned in subsection (4)*(b)* as if every reference to the owner of a critical information infrastructure is a reference to the person mentioned in subsection (4)*(b)*.

(7) Where —

(a) a notice issued under this section and amended under subsection (5) is addressed and sent to the person mentioned in subsection (4)*(b)*; and

(b) the person mentioned in subsection (4)*(b)* then ceases to have the control, ability and right mentioned in that provision,

the owner of the critical information infrastructure shall notify the Commissioner of this without delay.

(8) Where a critical information infrastructure is owned by the Government and operated by a Ministry, the Permanent Secretary allocated to the Ministry who has responsibility for the critical information

infrastructure is treated as the owner of the critical information infrastructure for the purposes of this Act.

(9) A notice issued under this section need not be published in the *Gazette*.

Power to obtain information to ascertain if computer etc. fulfils criteria of critical information infrastructure

10. (1) This section applies where the Commissioner has reason to believe that a computer or computer system may fulfil the criteria of a critical information infrastructure.

(2) The Commissioner may, by notice issued in such form and manner as the Commissioner may determine, require any person who appears to be exercising control over the computer or computer system, to provide to the Commissioner, within a reasonable period specified in the notice, such relevant information relating to that computer or computer system as may be required by the Commissioner for the purpose of ascertaining whether the computer or computer system fulfils the criteria of a critical information infrastructure.

(3) Without affecting the generality of subsection (2), the Commissioner may in the notice require the person who appears to be exercising control over the computer or computer system to provide —

(a) information relating to —

(i) the function that the computer or computer system is employed to serve; and

(ii) the person or persons who is or are, or other computer or computer systems that is or are, served by that computer or computer system;

(b) information relating to the design of the computer or computer system; and

(c) such other information as the Commissioner may require in order to ascertain whether the computer or computer system fulfils the criteria of a critical information infrastructure.

(4) Any person who, without reasonable excuse, fails to comply with a notice issued under subsection (2) is guilty of an offence and liable on conviction to a fine not exceeding $100,000, imprisonment for a term not exceeding 2 years or both and, in the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part thereof during which the offence continues after conviction.

(5) Any person to whom a notice is issued under subsection (2) is not obliged to disclose any information that is subject to any right, privilege or immunity conferred, or obligation or limitation imposed, by or under any law, contract or rules of professional conduct in relation to the disclosure of such information.

Withdrawal of designation of critical information infrastructure

11. The Commissioner may, by written notice, withdraw the designation of any critical information infrastructure at any time if the Commissioner is of the opinion that the computer or computer system no longer fulfils the criteria of a critical information infrastructure.

Furnishing of information relating to critical information infrastructure

12. (1) The Commissioner may, by notice issued in such form and manner as the Commissioner may determine, require the owner of a critical information infrastructure to furnish, within a reasonable period specified in the notice, the following —

(a) information on the design, configuration and security of the critical information infrastructure;

(b) information on the design, configuration and security of any other computer or computer system under the control of the owner that is interconnected with or that communicates with the critical information infrastructure;

(c) information relating to the operation of the critical information infrastructure and of any other computer or computer system under the control of the owner that is interconnected with or that communicates with the critical information infrastructure;

(d) such other information as the Commissioner may require in order to ascertain the level of cybersecurity of the critical information infrastructure.

(2) Any owner of a critical information infrastructure who fails, without reasonable excuse, to comply with a notice issued under subsection (1) is guilty of an offence and liable on conviction to a fine not exceeding $100,000, imprisonment for a term not exceeding 2 years or both and, in the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part thereof during which the offence continues after conviction.

(3) The owner of a critical information infrastructure to whom a notice is issued under subsection (1) is not obliged to disclose any information that is subject to any right, privilege or immunity conferred, or obligation or limitation imposed, by or under any law or rules of professional conduct in relation to the disclosure of such information, except that the performance of a contractual obligation is not an excuse for not disclosing the information.

(4) The owner of a critical information infrastructure is not treated as being in breach of any contractual obligation mentioned in subsection (3) for doing or omitting to do any act, if the act is done or omitted to be done with reasonable care and in good faith and for the purpose of complying with a notice issued under subsection (1).

(5) If a material change is made by or on behalf of the owner of a critical information infrastructure to the design, configuration, security or operation of the critical information infrastructure after any information has been furnished to the Commissioner pursuant to a notice issued under subsection (1), the owner of the critical information infrastructure shall notify the Commissioner of the change not later than 30 days after the change is made.

(6) For the purposes of subsection (5), a change is a material change if the change affects or may affect the cybersecurity of the critical information infrastructure or the ability of the owner of the critical information infrastructure to respond to a cybersecurity threat or incident affecting the critical information infrastructure.

(7) Any owner of a critical information infrastructure who fails, without reasonable excuse, to comply with subsection (5) is guilty of an offence and liable on conviction to a fine not exceeding $25,000, imprisonment for a term not exceeding 12 months or both.

Codes of practice and standards of performance

13. (1) The Commissioner may —

(a) issue or approve one or more codes of practice or standards of performance for the regulation of the owners of critical information infrastructure with respect to measures to be taken by them to ensure the cybersecurity of the critical information infrastructure; or

(b) amend or revoke any code of practice or standard of performance issued or approved under paragraph *(a)*.

(2) If any provision in any code of practice or standard of performance is inconsistent with this Act, such provision, to the extent of the inconsistency, does not have effect.

(3) Where a code of practice or standard of performance is issued, approved, amended or revoked by the Commissioner under subsection (1), the Commissioner shall —

(a) publish a notice of the issue, approval, amendment or revocation (as the case may be) in such manner as will secure adequate publicity for such issue, approval, amendment or revocation;

(b) specify in the notice the date of the issue, approval, amendment or revocation (as the case may be); and

(c) ensure that, so long as the code of practice or standard of performance remains in force, copies of that code or standard, and of all amendments to that code or standard, are available free of charge to the owner of a critical information infrastructure to which that code or standard applies.

(4) None of the following has any effect until the notice relating to it is published in accordance with subsection (3) —

(a) a code of practice or standard of performance;

(b) an amendment to a code of practice or standard of performance;

(c) a revocation of a code of practice or standard of performance.

(5) Any code of practice or standard of performance has no legislative effect.

(6) Subject to subsections (4) and (7), every owner of a critical information infrastructure shall comply with the codes of practice and standards of performance that apply to the critical information infrastructure.

(7) The Commissioner may, either generally or for such time as the Commissioner may specify, waive the application to the owner of a critical information infrastructure of any code of practice or standard of performance, or any part of it.

Power of Commissioner to issue written directions

14. (1) The Commissioner may, if the Commissioner thinks —

(a) it is necessary or expedient for ensuring the cybersecurity of a critical information infrastructure or a class of critical information infrastructure; or

(b) it is necessary or expedient for the effective administration of this Act,

issue a written direction, either of a general or specific nature, to the owner of a critical information infrastructure or a class of such owners.

(2) Without affecting the generality of subsection (1), a direction under that subsection may relate to —

(a) the action to be taken by the owner or owners in relation to a cybersecurity threat;

(b) compliance with any code of practice or standard of performance applicable to the owner;

(c) the appointment of an auditor approved by the Commissioner to audit the owner or owners on their compliance with this Act or any code of practice or standard of performance applicable to the owner or owners; or

(d) such other matters as the Commissioner may think fit or expedient to ensure the cybersecurity of the critical information infrastructure.

(3) The Commissioner may at any time vary or revoke any direction issued under subsection (1).

(4) Before giving a direction under subsection (1), the Commissioner shall, unless the Commissioner thinks it is not practicable or desirable to do so, give notice to the person or persons whom the Commissioner proposes to issue the direction —

(a) stating that the Commissioner proposes to issue the direction and setting out its effect; and

(b) specifying the time within which representations or objections to the proposed direction may be made.

(5) The Commissioner shall consider any representation or objection which is duly made before giving any direction.

(6) Any person who, without reasonable excuse, fails to comply with a direction under subsection (1) is guilty of an offence and liable on conviction to a fine not exceeding $100,000, imprisonment for a term not exceeding 2 years or both and, in the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part thereof during which the offence continues after conviction.

Change in ownership of critical information infrastructure

15. (1) Where there is any change in the beneficial or legal ownership (including any share in such ownership) of a critical information infrastructure, the relevant person shall inform the Commissioner of the change in ownership not later than 7 days after the date of that change in ownership.

(2) Any person who, without reasonable excuse, fails to comply with subsection (1) is guilty of an offence and liable on conviction to a fine not exceeding $100,000, imprisonment for a term not exceeding 2 years or both.

(3) In subsection (1), the relevant person is —

(a) in the case of a transfer of the whole of the legal ownership of the critical information infrastructure to another person, the person who was the owner of the critical information infrastructure before the change in ownership; or

(b) in any other case, an owner of the critical information infrastructure.

Duty to report cybersecurity incident in respect of critical information infrastructure etc.

16. (1) The owner of a critical information infrastructure shall notify the Commissioner of the occurrence of any of the following in such form and manner as the Commissioner may determine, within the prescribed period after becoming aware of such occurrence —

(a) a prescribed cybersecurity incident in respect of the critical information infrastructure;

(b) a prescribed cybersecurity incident in respect of any computer or computer system under the control of the owner that is interconnected with or that communicates with the critical information infrastructure;

(c) any other type of cybersecurity incident in respect of the critical information infrastructure that the Commissioner has specified by written direction to the owner.

(2) The owner of a critical information infrastructure shall establish such mechanisms and processes for the purposes of detecting cybersecurity threats and incidents in respect of the critical information infrastructure as set out in any applicable code of practice.

(3) Any owner of a critical information infrastructure who, without reasonable excuse, fails to comply with subsection (1) is guilty of an offence and liable on conviction to a fine not exceeding $100,000, imprisonment for a term not exceeding 2 years or both.

Cybersecurity audits and risk assessments of critical information infrastructure

17. (1) The owner of a critical information infrastructure shall —

(a) at least once every 2 years (or at such higher frequency as may be directed by the Commissioner in any particular case), starting from the date of the notice issued under section 9, cause an audit of the compliance of the critical information infrastructure with this Act and the applicable codes of practice and standards of performance to be

carried out by an auditor approved or appointed by the Commissioner; and

(b) at least once a year, starting from the date of the notice issued under section 9, conduct a cybersecurity risk assessment of the critical information infrastructure in such form and manner as the Commissioner may determine.

(2) The owner of the critical information infrastructure shall, not later than 30 days after the completion of the audit mentioned in subsection (1)*(a)* or the cybersecurity risk assessment mentioned in subsection (1)*(b)*, furnish a copy of the report of the audit or assessment to the Commissioner.

(3) Where it appears to the Commissioner from the report of an audit furnished under subsection (2) that any aspect of the audit was not carried out satisfactorily, the Commissioner may direct the owner of the critical information infrastructure to cause the auditor to carry out that aspect of the audit again.

(4) Where it appears to the Commissioner —

(a) that the owner of a critical information infrastructure has not complied with a provision of this Act, or an applicable code of practice or standard of performance; or

(b) that any information provided by the owner of a critical information infrastructure under section 12 is false, misleading, inaccurate or incomplete,

the Commissioner may by order require an audit in respect of the critical information infrastructure to be carried out by an auditor appointed by the Commissioner, for the purpose of ascertaining the compliance of the owner with this Act or an applicable code of practice or standard of performance, or the accuracy or completeness of the information, as the case may be, and the cost of such audit shall be borne by the owner.

(5) Where it appears to the Commissioner from the report of a cybersecurity risk assessment furnished under subsection (2) that the assessment was not carried out satisfactorily, the Commissioner may either —

(a) direct the owner of the critical information infrastructure to carry out further steps to evaluate the level of cybersecurity of the critical information infrastructure; or

(b) appoint a cybersecurity service provider to conduct another cybersecurity risk assessment of the critical information infrastructure and the cost of such assessment shall be borne by the owner.

(6) Where the owner of a critical information infrastructure has notified the Commissioner under section 12(5) of a material change made to the design, configuration, security or operation of the critical information infrastructure, or the Commissioner otherwise becomes aware of such material change having been made, the Commissioner may by written notice direct the owner to carry out another audit or cybersecurity risk assessment in addition to the audit or cybersecurity risk assessment mentioned in subsection (1).

(7) Any owner of a critical information infrastructure who —

(a) fails, without reasonable excuse, to comply with subsection (1);

(b) fails to comply with the direction of the Commissioner under subsection (3), (5)*(a)* or (6); or

(c) obstructs or prevents an audit mentioned in subsection (4) or a cybersecurity risk assessment mentioned in subsection (5)*(b)* from being carried out,

is guilty of an offence and liable on conviction to a fine not exceeding $100,000, imprisonment for a term not exceeding 2 years or both and, in the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part thereof during which the offence continues after conviction.

(8) Any owner of a critical information infrastructure who, without reasonable excuse, fails to comply with subsection (2) is guilty of an offence and liable on conviction to a fine not exceeding $25,000, imprisonment for a term not exceeding 12 months or both and, in the case of a continuing offence, to a further fine not exceeding $2,500 for every day or part thereof during which the offence continues after conviction.

Cybersecurity exercises

18. (1) The Commissioner may conduct cybersecurity exercises for the purpose of testing the state of readiness of owners of different critical information infrastructure in responding to significant cybersecurity incidents.

(2) An owner of a critical information infrastructure shall participate in a cybersecurity exercise if directed in writing to do so by the Commissioner.

(3) Any person who, without reasonable excuse, fails to comply with a direction under subsection (2) is guilty of an offence and liable on conviction to a fine not exceeding $100,000.

Appeal to Minister

19. (1) The owner of a critical information infrastructure who is aggrieved by —

(a) the decision of the Commissioner to issue the notice under section 9(1) designating the critical information infrastructure as such;

(b) a written direction of the Commissioner under section 14 or 18(2); or

(c) any provision in any code of practice or standard of performance issued or approved by the Commissioner that applies to the owner, or any amendment made to it,

may appeal to the Minister against the decision, direction, provision or amendment in the manner prescribed.

(2) An appeal under subsection (1) shall be made within 30 days after the date of the notice or direction, or the issue, approval or amendment (as the case may be) of the code of practice or standard of performance, as the case may be, or such longer period as the Minister allows in a particular case (whether allowed before or after the end of the 30 days).

(3) Any person who makes an appeal to the Minister under subsection (1) shall, within the period specified in subsection (2) —

(a) state as concisely as possible the circumstances under which the appeal arises, and the issues and grounds for the appeal; and

(b) submit to the Minister all relevant facts, evidence and arguments for the appeal.

(4) Where an appeal has been made to the Minister under subsection (1), the Minister may require —

(a) any party to the appeal; and

(b) any person who is not a party to the appeal but appears to the Minister to have information that is relevant to the matters appealed against,

to provide the Minister with all such information as the Minister may require, whether for the purpose of deciding if an Appeals Advisory Panel should be established or for determining the appeal, and any person so required shall provide the information in such manner and within such period as may be specified by the Minister.

(5) The Minister may dismiss an appeal of an appellant who fails to comply with subsection (3) or (4).

(6) Unless otherwise provided by this Act or allowed by the Minister, where an appeal is lodged under this section, the decision, direction or other thing appealed against shall be complied with until the determination of the appeal.

(7) The Minister may determine an appeal under this section —

(a) by confirming, varying or reversing a decision, notice, direction, provision of a code of practice or standard of performance, or an amendment to such code or standard; or

(b) by directing the Commissioner to reconsider the Commissioner's decision, notice, direction, or provision of a code of practice or standard of performance, as the case may be.

(8) Before determining an appeal under subsection (7), the Minister may consult any Appeals Advisory Panel established for the purpose of advising the Minister in respect of the appeal but, in making such determination, is not bound by the advice of the Panel.

(9) The decision of the Minister in any appeal is final.

Appeals Advisory Panel

20. (1) Where the Minister considers that an appeal lodged under section 19(1) involves issues the resolution or understanding of which require particular technical skills or specialised knowledge, the Minister may establish an Appeals Advisory Panel to provide advice to the Minister in respect of the appeal.

(2) For the purposes of establishing an Appeals Advisory Panel, the Minister may do all or any of the following —

(a) determine and vary the terms of reference of the Appeals Advisory Panel;

(b) appoint persons possessing particular technical skills or specialised knowledge to be the chairperson and other members of an Appeals Advisory Panel;

(c) at any time remove the chairperson or other member of an Appeals Advisory Panel from such office;

(d) determine any other matters which the Minister considers incidental to or expedient for the proper and efficient conduct of business by the Appeals Advisory Panel.

(3) An Appeals Advisory Panel may regulate its proceedings in such manner as it considers appropriate, subject to the following —

(a) the *quorum* for a meeting of the Appeals Advisory Panel is a majority of its members;

(b) a decision supported by a majority of the votes cast at a meeting of the Appeals Advisory Panel at which a *quorum* is present is the decision of that Panel.

(4) The remuneration and allowances, if any, of a member of an Appeals Advisory Panel is to be determined by the Minister.

(5) An Appeals Advisory Panel is independent in the performance of its functions.

PART 4

RESPONSES TO CYBERSECURITY THREATS AND INCIDENTS

Powers to investigate and prevent cybersecurity incidents etc.

21. (1) Where information regarding a cybersecurity threat or incident has been received by the Commissioner, the Commissioner may exercise, or may authorise the Deputy Commissioner, an Assistant Commissioner, a cybersecurity officer or an authorised officer to exercise such of the powers mentioned in subsection (2) as are necessary to investigate the cybersecurity threat or incident for the purpose of —

(a) assessing the impact or potential impact of the cybersecurity threat or incident;

(b) preventing any or further harm arising from the cybersecurity incident; or

(c) preventing a further cybersecurity incident from arising from that cybersecurity threat or incident.

(2) The powers mentioned in subsection (1) are the following —

(a) require, by written notice, any person to attend at such reasonable time and at such place as may be specified by the incident response officer to answer any question or to provide a signed statement in writing concerning the cybersecurity threat or incident;

(b) require, by written notice, any person to produce to the incident response officer any physical or electronic record, or document, or a copy of the record or document, that is in the possession of that person, or to provide the incident response officer with any information, which the incident response officer considers to be related to any matter relevant to the investigation;

(c) without giving any fee or reward, inspect, copy or take extracts from such record or document or copy of the record or document mentioned in paragraph *(b)*;

(d) examine orally any person who appears to be acquainted with the facts and circumstances relating to the cybersecurity threat or

incident and reduce to writing any statement made by the person so examined.

(3) The incident response officer shall specify in the notice mentioned in subsection (2)*(b)* —

(a) the time and place at which any record, document or copy is to be produced or any information is to be provided; and

(b) the manner and form in which it is to be produced or provided.

(4) A statement made by a person examined under this section shall —

(a) be reduced to writing;

(b) be read over to the person;

(c) if the person does not understand English, be interpreted for the person in a language that he or she understands; and

(d) after correction (if necessary), be signed by that person.

(5) If any person fails to comply with a written notice under subsection (2)*(a)*, the incident response officer may report such failure to a Magistrate who may then issue an order for the person to attend before the Commissioner, at a time and place specified in the order, to answer any question or provide a signed statement in writing concerning the cybersecurity threat or incident.

(6) Any person examined under this section or to whom a notice under subsection (2) or an order under subsection (5) is issued is not obliged to disclose any information that is subject to any right, privilege or immunity conferred, or obligation or limitation imposed, by or under any law or rules of professional conduct in relation to the disclosure of such information, except that the performance of a contractual obligation is not an excuse for not disclosing the information.

(7) The person examined under this section or to whom a notice under subsection (2) or an order under subsection (5) is issued is not treated as being in breach of any contractual obligation mentioned in subsection (6) for doing or omitting to do any act if the act is done or omitted to be done with

reasonable care and in good faith and for the purpose of answering any question asked during the examination or complying with the notice or order.

(8) Any person who —

(a) wilfully misstates or without reasonable excuse refuses to give any information, provide any statement or produce any record, document or copy required of the person by an incident response officer under subsection (2); or

(b) fails, without reasonable excuse, to comply with an order issued by a Magistrate under subsection (5),

is guilty of an offence and liable on conviction to a fine not exceeding $5,000, imprisonment for a term not exceeding 6 months or both.

(9) In this section and sections 22, 23 and 24, "incident response officer" means the Commissioner, the Deputy Commissioner or any Assistant Commissioner, cybersecurity officer or authorised officer exercising the powers under this section or section 22, as the case may be.

Powers to investigate and prevent serious cybersecurity incidents etc.

22. (1) Where the Commissioner receives information regarding a cybersecurity threat or incident which satisfies the severity threshold in subsection (3), the Commissioner may exercise, or may authorise the Deputy Commissioner, an Assistant Commissioner, a cybersecurity officer or an authorised officer to exercise, such of the powers mentioned in subsection (2) as are necessary to investigate the cybersecurity threat or incident for the purpose of —

(a) assessing the impact or potential impact of the cybersecurity threat or incident;

(b) eliminating the cybersecurity threat or otherwise preventing any or further harm arising from the cybersecurity incident; or

(c) preventing a further cybersecurity incident.

(2) The powers mentioned in subsection (1) are the following —

(a) any power mentioned in section 21(2)*(a)*, *(b)*, *(c)* or *(d)*;

(b) direct, by written notice, any person to carry out such remedial measures, or to cease carrying on such activities, as may be specified to the person, in relation to a computer or computer system that the incident response officer has reasonable cause to suspect is or was affected by the cybersecurity incident, in order to minimise cybersecurity vulnerabilities in the computer or computer system;

Examples

Examples of remedial measures include —

(a) the removal of malicious software from the computer;

(b) the installation of software updates to address cybersecurity vulnerabilities;

(c) temporarily disconnecting infected computers from a computer network until paragraph *(a)* or *(b)* is carried out; and

(d) the redirection of malicious data traffic towards a designated computer or computer system.

(c) require the owner of a computer or computer system to take any action to assist with the investigation, including but not limited to —

(i) preserving the state of the computer or computer system by not using it;

(ii) monitoring the computer or computer system for a specified period of time;

(iii) performing a scan of the computer or computer system to detect cybersecurity vulnerabilities and to assess the manner and extent that the computer or computer system is affected by the cybersecurity incident; and

(iv) allowing the incident response officer to connect any equipment to the computer or computer system, or install on the computer or computer system any computer program, as is necessary for the purpose of the investigation;

(d) after giving reasonable notice to the owner or occupier of any premises, enter those premises if the incident response officer

reasonably suspects that there is within the premises a computer or computer system that is or was affected by the cybersecurity incident;

(e) access, inspect and check the operation of a computer or computer system that the incident response officer has reasonable cause to suspect is or was affected by the cybersecurity incident, or use or cause to be used any such computer or computer system to search any data contained in or available to such computer or computer system;

(f) perform a scan of a computer or computer system to detect cybersecurity vulnerabilities in the computer or computer system;

(g) take a copy of, or extracts from, any electronic record or computer program contained in a computer that the incident response officer has reasonable cause to suspect is or was affected by the cybersecurity incident;

(h) subject to subsection (5), with the consent of the owner, take possession of any computer or other equipment for the purpose of carrying out further examination or analysis.

(3) A cybersecurity threat or incident satisfies the severity threshold mentioned in subsection (1) if —

(a) it creates a risk of significant harm being caused to a critical information infrastructure;

(b) it creates a risk of disruption to the provision of an essential service;

(c) it creates a threat to the national security, defence, foreign relations, economy, public health, public safety or public order of Brunei Darussalam; or

(d) the cybersecurity threat or incident is of a severe nature, in terms of the severity of the harm that may be caused to persons in Brunei Darussalam or the number of computers or value of the information put at risk, whether or not the computers or computer systems put at risk are themselves critical information infrastructure.

(4) An incident response officer exercising the power mentioned in subsection (2)*(e)* may require any assistance the incident response officer needs to gain such access from —

(a) any person whom the incident response officer reasonably suspects uses or has used the computer or computer system; or

(b) any person having charge of, or who is otherwise concerned with the operation of, such computer or computer system.

(5) Where the owner of the computer or other equipment does not consent to the exercise of the power mentioned in subsection (2)*(h)*, the power may be exercised if the Commissioner is satisfied that —

(a) the exercise of the power is necessary for the purposes of the investigation;

(b) there is no less disruptive method of achieving the purpose of the investigation; and

(c) after consultation with the owner, and having regard to the importance of the computer or other equipment to the business or operational needs of the owner, the benefit from the exercise of the power outweighs the detriment caused to the owner,

and the Commissioner has issued to the incident response officer a written authorisation to exercise the power.

(6) The incident response officer shall, immediately after the completion of the further examination or analysis on the computer or other equipment which was taken into possession in exercise of the power mentioned in subsection (2)*(h)*, return the computer or other equipment to the owner.

(7) Any person who —

(a) in relation to an investigation under this section, wilfully misstates or without reasonable excuse, refuses to give any information, provide any statement or produce any record, document or copy required of the person by the incident response officer under section 21(2);

(b) in relation to an investigation under this section, fails, without reasonable excuse, to comply with an order issued by a Magistrate under section 21(5);

(c) fails, without reasonable excuse, to comply with a direction or requirement of an incident response officer under subsection (2)*(b)* or *(c)*; or

(d) fails, without reasonable excuse, to comply with a lawful demand of an incident response officer made in the discharge of the duties of the incident response officer under this section,

is guilty of an offence and liable on conviction to a fine not exceeding $25,000, imprisonment for a term not exceeding 2 years or both.

Production of identification card by incident response officer

23. Every incident response officer, when exercising any of the powers under this Part, shall declare the office of the incident response officer and shall, on demand, produce to any person affected by the exercise of that power such identification card as the Commissioner may direct to be carried by the incident response officer when exercising such power.

Appointment of cybersecurity technical experts

24. (1) The Commissioner may, in writing, appoint any of the following as a cybersecurity technical expert for a specified period to assist any incident response officer in the course of an investigation under section 21 or 22 —

(a) a public officer or an employee of a statutory body;

(b) an individual (who is not a public officer or an employee of a statutory body) with suitable qualifications or experience to properly perform the role of a cybersecurity technical expert.

(2) The role of a cybersecurity technical expert is to provide such advice of a technical nature as the incident response officer may require in the course of an investigation under section 21 or 22.

(3) The Commissioner may, for any reason that appears to the Commissioner to be sufficient, at any time revoke the appointment of an individual as a cybersecurity technical expert.

(4) The Commissioner shall issue to each cybersecurity technical expert an identification card which shall be carried at all times by the cybersecurity technical expert when performing the role of a cybersecurity technical expert.

(5) A cybersecurity technical expert whose appointment as such ceases shall return any identification card issued to the cybersecurity technical expert under subsection (4) to the Commissioner.

Emergency cybersecurity measures and requirements

25. (1) The Minister may, if satisfied that it is necessary for the purposes of preventing, detecting or countering any serious and imminent threat to —

(a) the provision of any essential service; or

(b) the national security, defence, foreign relations, economy, public health, public safety or public order of Brunei Darussalam,

by a certificate under the hand of the Minister, authorise or direct any person or organisation specified in the certificate (referred to in this section as the specified person) to take such measures or comply with such requirements as may be necessary to prevent, detect or counter any threat to a computer or computer system or any class of computers or computer systems.

(2) The measures and requirements mentioned in subsection (1) may include, without limitation —

(a) the exercise by the specified person of the powers in section 18(1) of the Computer Misuse Act (Chapter 194);

(b) requiring or authorising the specified person to direct another person to provide any information that is necessary to identify, detect or counter any such threat, including —

(i) information relating to the design, configuration or operation of any computer, computer program or computer system; and

(ii) information relating to the cybersecurity of any computer, computer program or computer system;

(c) providing to the Minister or the Commissioner any information (including real time information) obtained from any computer controlled or operated by the specified person, or obtained by the specified person from another person pursuant to a measure or requirement under paragraph *(b)*, that is necessary to identify, detect or counter any such threat, including —

(i) information relating to the design, configuration or operation of any computer, computer program or computer system; and

(ii) information relating to the cybersecurity of any computer, computer program or computer system; and

(d) providing to the Minister or the Commissioner a report of a breach or an attempted breach of cybersecurity of a description specified in the certificate under subsection (1) relating to any computer controlled or operated by the specified person.

(3) Any measure or requirement mentioned in subsection (1) and any direction given by a specified person for the purpose of taking any such measure or complying with any such requirement —

(a) does not confer any right to the production of, or of access to, information subject to legal privilege; and

(b) subject to paragraph *(a)*, has effect despite any obligation or limitation imposed or right, privilege or immunity conferred by or under any law, contract or rules of professional conduct, including any restriction on the disclosure of information imposed by law, contract or rules of professional conduct.

(4) A specified person who, without reasonable excuse, fails to take any measure or comply with any requirement directed by the Minister under subsection (1) is guilty of an offence and liable on conviction to a fine not exceeding $50,000, imprisonment for a term not exceeding 10 years or both.

(5) Any person who, without reasonable excuse —

(a) obstructs a specified person in the taking of any measure or in complying with any requirement under subsection (1); or

(b) fails to comply with any direction given by a specified person for the purpose of the specified person taking any such measure or complying with any such requirement,

is guilty of an offence and liable on conviction to a fine not exceeding $50,000, imprisonment for a term not exceeding 10 years or both.

(6) No civil or criminal liability is incurred by —

(a) a specified person for doing or omitting to do any act if the specified person had done or omitted to do the act in good faith and for the purpose of or as a result of taking any measure or complying with any requirement under subsection (1); or

(b) a person for doing or omitting to do any act if the person had done or omitted to do the act in good faith and for the purpose of or as a result of complying with a direction given by a specified person for the purpose of taking any such measure or complying with any such requirement.

(7) The following persons are not considered to be in breach of any restriction on the disclosure of information imposed by law, contract or rules of professional conduct —

(a) a specified person who, in good faith, obtains any information for the purpose of taking any measure under subsection (1) or complying with any requirement under that subsection, or who discloses any information to the Minister or the Commissioner, in compliance with any requirement under that subsection;

(b) a person who, in good faith, obtains any information, or discloses any information to a specified person, in compliance with a direction given by the specified person for the purpose of taking any measure under subsection (1) or complying with any requirement under that subsection.

(8) The following persons, namely —

(a) a specified person to whom a person has provided information in compliance with a direction given by the specified person for the purpose of taking any measure under subsection (1) or complying with any requirement under that subsection;

(b) a person to whom a specified person provides information in compliance with any requirement under subsection (1),

shall not use or disclose the information, except —

(i) with the written permission of the person from whom the information was obtained or, where the information is the confidential information of a third person, with the written permission of the third person;

(ii) for the purpose of preventing, detecting or countering a threat to a computer, computer system or class of computers or computer systems;

(iii) to disclose to any police officer or other law enforcement authority any information which discloses the commission of an offence under this Act or any other written law; or

(iv) in compliance with a requirement of a court or the provisions of this Act or any other written law.

(9) Any person who contravenes subsection (8) is guilty of an offence and liable on conviction to a fine not exceeding $10,000, imprisonment for a term not exceeding 12 months or both.

(10) Where an offence is disclosed in the course of or pursuant to the exercise of any power under this section —

(a) no information for that offence may be admitted in evidence in any civil or criminal proceedings; and

(b) no witness in any civil or criminal proceedings is obliged —

(i) to disclose the name, address or other particulars of any informer who has given information with respect to that offence; or

(ii) to answer any question if the answer would lead, or would tend to lead, to the discovery of the name, address or other particulars of the informer.

(11) If any book, document, data or computer output which is admitted in evidence or liable to inspection in any civil or criminal proceedings

contains any entry in which any informer is named or described or which may lead to the discovery of the informer, the court shall cause those entries to be concealed from view or to be obliterated so far as may be necessary to protect the informer from discovery.

PART 5

GENERAL

Reserve fund

26. There shall be established a reserve fund for the purposes of mitigating any cybersecurity risk which shall not be withdrawn except with the approval of the Minister.

Corporate offenders and unincorporated associations

27. (1) Where an offence under this Act committed by a body corporate is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, an officer of the body corporate, he as well as the body corporate is guilty of that offence and liable to be proceeded against and punished accordingly.

(2) Where the affairs of the body corporate are managed by its members, subsection (1) applies in relation to the acts and defaults of a member in connection with his functions of management as if he were a director of the body corporate.

(3) Where an offence under this Act committed by a partnership is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, a partner, the partner as well as the partnership is guilty of that offence and liable to be proceeded against and punished accordingly.

(4) Where an offence under this Act committed by a limited liability partnership is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, a partner or manager of the limited liability partnership, the partner or manager (as the case may be) as well as the partnership is guilty of that offence and liable to be proceeded against and punished accordingly.

(5) Where an offence under this Act committed by an unincorporated association (other than a partnership) is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, an officer of the unincorporated association or a member of its governing body, the officer or member (as the case may be) as well as the unincorporated association is guilty of that offence and liable to be proceeded against and punished accordingly.

(6) In this section —

"officer" —

(a) in relation to a body corporate, means a director, member of the committee of management, chief executive, manager, secretary or other similar officer of the body corporate, and includes a person purporting to act in such capacity; or

(b) in relation to an unincorporated association (other than a partnership), means the president, the secretary or a member of the committee of the unincorporated association or a person holding a position analogous to that of president, secretary or member of a committee, and includes a person purporting to act in any such capacity;

"partner", in relation to a partnership, includes a person purporting to act as a partner.

(7) The Minister may, with the consent of His Majesty the Sultan and Yang Di-Pertuan, make regulations to provide for the application of any provision of this section, with such modifications as he considers appropriate, to any body corporate or unincorporated association formed or recognised under the law of a country or territory outside Brunei Darussalam.

Powers of investigation

28. (1) An investigation officer authorised by the Commissioner may, in relation to any offence under this Act (except any offence under section 25) or any regulations made under this Act, on declaration of the office of the investigation officer and production to the person against whom the investigation officer is acting such identification card as the Commissioner may direct to be carried —

(a) require any person whom the investigation officer reasonably believes to have committed that offence to furnish evidence of the person's identity;

(b) require, by written notice, any person whom the investigation officer reasonably believes has —

(i) any information; or

(ii) any document in the custody or control of the person,

that is relevant to the investigation, to furnish that information or document within the time and manner specified in the written notice;

(c) require, by order in writing, the attendance before the investigation officer of any person within the limits of Brunei Darussalam who, from any information given or otherwise obtained by the investigation officer, appears to be acquainted with the facts or circumstances of the case; or

(d) examine orally any person who appears to be acquainted with the facts or circumstances of the case —

(i) whether before or after that person or anyone else is charged with an offence in connection with the case; and

(ii) whether or not that person is to be called as a witness in any inquiry, trial or other proceedings in connection with the case.

(2) The person mentioned in subsection (1)*(d)* is bound to state truly the facts and circumstances with which the person is acquainted concerning the case except that the person need not say anything that might expose the person to a criminal charge, penalty or forfeiture.

(3) A statement made by a person examined under subsection (1)*(d)* shall —

(a) be reduced to writing;

(b) be read over to the person;

(c) if the person does not understand English, be interpreted to the person in a language that the person understands; and

(d) after correction (if necessary), be signed by the person.

(4) If any person fails to attend as required by an order under subsection (1)*(c)*, the investigation officer may report such failure to a Magistrate who may then issue a warrant to secure the attendance of that person as required by the order.

(5) An investigation officer may, without payment, take possession or make copies of any document (or any part of it) furnished under subsection (1), for further investigation.

(6) Any person who —

(a) refuses to give access to, or assaults, obstructs, hinders or delays, an investigation officer in the discharge of the duties of the investigation officer under this Act;

(b) wilfully misstates or without lawful excuse refuses to give any information or produce any document required by an investigation officer under subsection (1); or

(c) fails to comply with a lawful demand of an investigation officer in the discharge of the duties of the investigation officer under this Act,

is guilty of an offence and liable on conviction to a fine not exceeding $20,000, imprisonment for a term not exceeding 12 months or both.

(7) In this section and section 29, "investigation officer" means the Deputy Commissioner, or any Assistant Commissioner or cybersecurity officer authorised by the Commissioner, exercising the powers of investigation under this section or section 29.

Power to enter premises under warrant

29. (1) A Magistrate may, on the application of an investigation officer, issue a warrant in respect of any premises if the Magistrate is satisfied that there are reasonable grounds to suspect that there is on the premises any document —

(a) which has been required by an investigation officer under section 28 to be furnished, but has not been furnished in compliance with that requirement; or

(b) which, if required by an investigation officer under section 28 to be furnished, will be concealed, removed, tampered with or destroyed.

(2) If the Magistrate is also satisfied that there are reasonable grounds to suspect that there is on those premises any other document that relates to any matter relevant to the investigation concerned, the Magistrate may direct that the powers exercisable under the warrant extend to that other document.

(3) A warrant under subsection (1) may authorise a named investigation officer, and any other officer whom the Commissioner has authorised in writing to accompany the investigation officer —

(a) to enter and search the premises specified in the warrant, using such force as is reasonably necessary for the purpose;

(b) to take possession of, make copies of, or secure against interference, any document (or any part of it) that appears to be a document mentioned in subsection (1) or (2) (referred to in this section as the relevant document);

(c) to require any person on the premises to provide an explanation of any relevant document or, where applicable, to state, to the best of that person's knowledge and belief, where the relevant document may be found; and

(d) to require any relevant document that is stored in electronic form and accessible at the premises to be produced in a form that —

(i) can be taken away; and

(ii) is visible and legible.

(4) The warrant continues in force until the end of the period of one month beginning on the day on which it is issued.

(5) If the owner or occupier of the premises is present when the investigation officer proposes to execute the warrant, the investigation officer shall —

(a) identify himself to the owner or occupier;

(b) show the owner or occupier proof of the identity and authorisation of the investigation officer; and

(c) give the owner or occupier a copy of the warrant.

(6) If there is no one at the premises when the investigation officer proposes to execute the warrant, the investigation officer shall, before executing it —

(a) take such steps as are reasonable in all the circumstances to inform the owner or occupier of the premises of the intended entry into the premises; and

(b) where the owner or occupier is so informed, give the owner or occupier or the legal or other representative of the owner or occupier a reasonable opportunity to be present when the warrant is executed.

(7) If the investigation officer is unable to inform the owner or occupier of the premises of the intended entry into the premises, the investigation officer shall, when executing the warrant, leave a copy of it in a prominent place on the premises.

(8) The investigation officer shall —

(a) prepare and sign a list of all documents and other things taken under subsection (3)*(b)* and *(d)* in execution of the warrant; and

(b) give a copy of the list to the owner or occupier of the premises or the legal or other representative of the owner or occupier.

(9) On leaving the premises after executing the warrant, the investigation officer shall, if the premises are unoccupied or the owner or occupier of the premises is temporarily absent, leave the premises as effectively secured as the investigation officer found them.

(10) In this section —

"occupier", in relation to any premises specified in a warrant under subsection (1), means a person whom the investigation officer named in the warrant reasonably believes to be the occupier of those premises;

"premises" includes any building, structure, vehicle, vessel or aircraft.

Jurisdiction of court

30. Notwithstanding the provision of any other written laws, the Court of a Magistrate shall have jurisdiction to try all offences under this Act.

Composition of offences

31. (1) The Commissioner or any Assistant Commissioner authorised by the Commissioner in writing in that behalf may compound any offence under this Act or any regulations made thereunder which is prescribed as a compoundable offence by collecting from a person reasonably suspected of having committed the offence a sum not exceeding —

(a) one half of the amount of the maximum fine that is prescribed for the offence; or

(b) $5,000,

whichever is the lower.

(2) Where any offence is compoundable under this section, the abetment of or a conspiracy to commit the offence, or an attempt to commit the offence when the attempt is itself an offence, may be compounded in like manner.

(3) On payment of such sum of money, no further proceedings are to be taken against that person in respect of the offence.

(4) All sums collected under this section shall be paid into the Consolidated Fund.

Service of documents

32. (1) Any document required or authorised by this Act to be given or served on any person may be given or served either by delivering it to that person, or by leaving it at his proper address, or by the recorded delivery service.

(2) Any such document required or authorised to be given to or served on an authority or body being a corporation shall be duly given or served if it is given to or served on the secretary or clerk of the authority or body.

(3) For the purposes of this section, the proper address of any person to or on whom any such document is to be given or served shall, in the case of the secretary or clerk of a corporation, be that of the registered or principal office of the corporation, and in any other case, be the last known address of the person to be served:

Provided that, where the person to or on whom the document is to be given or served has, in accordance with arrangements agreed or in accordance with this Act, furnished an address for the giving or service of the document, being an address in Brunei Darussalam, his proper address for such purposes shall be the address furnished.

Preservation of secrecy

33. (1) Subject to subsections (3) and (7), every specified person shall preserve, and aid in preserving, the secrecy of —

(a) all matters relating to a computer or computer system of any person;

(b) all matters relating to the business, commercial or official affairs of any person;

(c) all matters that have been identified as confidential under subsection (5); and

(d) all matters relating to the identity of persons furnishing information to any specified person,

that may come to the knowledge of the specified person in the performance of his functions or the discharge of his duties under this Act.

(2) The specified person shall not communicate any matter mentioned in subsection (1) to any person, except insofar as such communication —

(a) is necessary for the performance of any such function or the discharge of any such duty; or

(b) is lawfully required by any court or lawfully required or allowed by or under this Act or any other written law.

(3) This section does not apply to any information provided in compliance with a direction or requirement under section 25.

(4) Any person who fails to comply with subsection (1) or (2) is guilty of an offence and liable on conviction to a fine not exceeding $10,000, imprisonment for a term not exceeding 12 months or both.

(5) Any person, when furnishing any information to a specified person, may identify information that the person claims to be confidential information.

(6) Every claim made under subsection (5) shall be supported by a written statement giving reasons why the information is confidential.

(7) Notwithstanding subsection (1), the Commissioner may disclose any information relating to any matter mentioned in subsection (1) in any of the following circumstances —

(a) where the written consent of the person to whom the information relates has been obtained;

(b) for the purposes of —

(i) a prosecution under this Act;

(ii) subject to subsection (8), enabling the Commissioner to give effect to any provision of this Act;

(iii) enabling the Commissioner or any authorised officer to investigate a suspected offence under this Act or to enforce a provision of this Act;

(iv) disclosing to any police officer any information which discloses the commission of an offence under the Computer Misuse Act (Chapter 194); or

(v) complying with such provision of an agreement between Brunei Darussalam and a country or territory outside Brunei Darussalam (referred to in this section as a foreign country) as may be prescribed, where the conditions specified in subsection (9) are satisfied.

(8) If the Commissioner is considering whether to disclose any information under subsection (7)*(b)*(ii), the Commissioner shall have regard to —

(a) the need to exclude, so far as is practicable, information the disclosure of which would in his opinion be contrary to the public interest;

(b) the need to exclude, so far as is practicable —

(i) commercial information the disclosure of which would, or might, in his opinion, significantly harm the legitimate business interests of the undertaking to which it relates; or

(ii) information relating to the private affairs of an individual the disclosure of which would, or might, in his opinion, significantly harm the interest of the individual; and

(c) the extent to which the disclosure is necessary for the purposes for which the Commissioner is proposing to make the disclosure.

(9) The conditions referred to in subsection (7)*(b)*(v) are —

(a) the information or documents requested by the foreign country are available to the Commissioner;

(b) unless the Government otherwise allows, the foreign country undertakes to keep the information or documents given confidential at all times; and

(c) the disclosure of the information or documents is not likely to be contrary to the public interest.

(10) In this section, "specified person" means a person who is or has been —

(a) the Commissioner, the Deputy Commissioner, an Assistant Commissioner, a cybersecurity officer or a person appointed or employed to assist the Commissioner;

(b) an authorised officer appointed under section 7;

(c) a member of an Appeals Advisory Panel established under section 20;

(d) a cybersecurity technical expert appointed under section 24; or

(e) the Minister, or a person appointed or employed to assist the Minister.

Protection against suit and legal proceedings

34. (1) No action, suit, prosecution or other proceedings shall lie or to be brought, instituted or maintained in any court against —

(a) the Commissioner;

(b) the Deputy Commissioner;

(c) an Assistant Commissioner;

(d) a cybersecurity officer;

(e) an authorised officer appointed under section 7,

(f) a member of an Appeals Advisory Panel established under section 20; or

(g) any other person lawfully acting under the direction of the Commissioner,

in respect of any act, neglect or default done or committed by him in good faith or any omission omitted by him or in good faith in such capacity to do anything in —

(i) the exercise or purported exercise of any power under this Act; or

(ii) the performance or purported performance of any function or duty under this Act.

(2) Where the Commissioner provides a service to the public whereby information is supplied to the public pursuant to any written law, neither the Commissioner nor any person acting under the direction of the Commissioner who is involved in the supply of such information is liable for any loss or damage suffered by any person by reason of any error or omission of whatever nature appearing in the information or however caused, if the error or omission was made in good faith and despite the exercise of reasonable care in the ordinary course of the discharge of the duties of the Commissioner or such person.

Protection of informers

35. (1) Except as provided in subsection (3) —

(a) no information for an offence against this Act shall be admitted in evidence in any proceedings; and

(b) no witness in any proceedings for an offence under Part 3 is obliged or permitted to —

(i) disclose the name, address or other particulars of an informer who has given information with respect to that offence, or the substance of the information received from the informer; or

(ii) answer any question if the answer thereto would lead, or would tend to lead, to the discovery of the name, address or other particulars of the informer.

(2) If any book, document or paper which is in evidence or liable to inspection in any proceedings contains any entry in which any informer is named or described or which might lead to his discovery, the court shall cause the entries to be concealed from view or to be obliterated so far only as may be necessary to protect the informer from discovery.

(3) If, in any proceedings before a court for an offence against this Act, the court after full inquiry into the case, is satisfied that an informer wilfully made a material statement which he knew or believed to be false or did not believe to be true, or if in any other proceedings the court is of the opinion that justice cannot be fully done between the parties thereto without the discovery of the name of an informer, the court may permit inquiry and require full disclosure concerning the informer.

Exemption

36. (1) The Minister may, with the consent of His Majesty the Sultan and Yang Di-Pertuan, either permanently or for such period as the Minister thinks fit by order published in the *Gazette*, exempt any person or any class of persons from all or any of the provisions of this Act, either generally or in a particular case and subject to such conditions as may be prescribed.

(2) If any exemption is granted under subsection (1) with conditions, the exemption operates only if the conditions are complied with.

Amendment of Schedule

37. The Minister may, with the consent of His Majesty the Sultan and Yang Di-Pertuan, by order published in the *Gazette*, amend the Schedule to this Act.

Regulations

38. (1) The Minister may, with the consent of His Majesty the Sultan and Yang Di-Pertuan, make regulations as he considers necessary or expedient for giving effect to or carrying out the purposes and provisions of this Act, including the prescription of fees and of any other thing required to be or which may be prescribed under this Act, and for the due administration thereof, and such regulations may include such incidental, consequential and supplementary provision as he considers necessary or expedient.

(2) Notwithstanding subsection (1), the Minister may make regulations for or in respect of all or any of the following matters —

(a) the procedure for the designation of a critical information infrastructure;

(b) the technical or other standards relating to cybersecurity to be maintained in respect of a critical information infrastructure;

(c) the responsibilities and duties of the owner of a critical information infrastructure;

(d) the type of changes that are considered material changes to the design, configuration, security or operations of a critical information infrastructure to be reported by the owner of the critical information infrastructure;

(e) the type of cybersecurity incidents in respect of a critical information infrastructure that are required to be reported by the owner of the critical information infrastructure;

(f) the manner in which an appeal may be made to, and the procedure to be adopted in the hearing of any appeal by, the Minister;

(g) the requirements for, and the manner for the carrying out of, cybersecurity audits and cybersecurity risk assessments required to be conducted by the owner of a critical information infrastructure;

(h) the form and nature of cybersecurity exercises that may be conducted;

(i) the fees to be paid in respect of any matter or thing required for the purposes of this Act, including the refund and remission (in whole or part) of such fees;

(j) the prescribing of the offences which may be compounded and the method and procedure by which they may be compounded; and

(k) all matters and things which by this Act are required or permitted to be prescribed or which are necessary or expedient to be prescribed to give effect to this Act.

(3) Except as otherwise expressly provided in this Act, the regulations —

(a) may be of general or specific application;

(b) may provide that any contravention of any specified provision of the regulations shall be an offence; and

(c) may provide for penalties not exceeding a fine of $50,000, imprisonment for a term not exceeding 12 months or both for each offence and, in the case of a continuing offence, a further penalty not exceeding a fine of 10 *per cent* of the maximum fine prescribed for that offence for every day or part thereof during which the offence continues after conviction.

SCHEDULE

(sections 2 and 37)

ESSENTIAL SERVICES

1. Services relating to energy
2. Services relating to infocommunications
3. Services relating to healthcare
4. Services relating to banking and finance
5. Services relating to defence and security
6. Services relating to emergency services
7. Services relating to aviation
8. Services relating to functioning of Government
9. Services relating to media
10. Services relating to water.