BERMUDA

CYBERSECURITY ACT 2024

2024 : 13

TABLE OF CONTENTS

WHEREAS it is expedient to provide for a cybersecurity legislative framework for the protection of critical national information infrastructure assets such as the computer systems supporting the Government and other essential services including energy supplies, telecommunications, health care, emergency services, water, and other essential public and private sector functions and services and for purposes connected and incidental to the foregoing;

Be it enacted by The King's Most Excellent Majesty, by and with the advice and consent of the Senate and the House of Assembly of Bermuda, and by the authority of the same, as follows:

PART 1

PRELIMINARY

Citation

1 This Act may be cited as the Cybersecurity Act 2024.

Interpretation

2 In this Act, unless the context otherwise provides—

"Board" means the Cybersecurity Advisory Board established under section 4;

"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;

"computer system" means an arrangement of interconnected computers that is designed to perform one or more specific functions, and includes an information system operating in combination with any of the following—

(a) an operational technology system;

(b) a programmable logic controller;

(c) a supervisory control;

(d) data acquisition system; or

(e) a distributed control system;

"critical national information infrastructure" or "CNII" means a computer, computer system, or part of a computer system located or conducting business in Bermuda which is essential for the maintenance of vital societal functions including health, safety, security, economic and social well-being of people, and the disruption or destruction of which, as a result of the failure to maintain those functions, would have a significant impact in Bermuda;

"critical national infrastructure sectors" means sectors dealing with health care, telecommunications, emergency services and energy and includes other sectors necessary for the economic and social well-being of people in Bermuda;

"CNII enforcement authority" means an entity designated as a CNII enforcement authority under section 9;

"CNII entity" means an entity designated as a CNII entity under section 10;

"cybersecurity event" means an event that could threaten the confidentiality, integrity, or availability of information or information systems and networks, or the safety of individuals by way of data breaches, cyber attacks, malware infections, and other forms of unauthorised access or use of information systems;

"Minister" means the Minister of National Security;

"National Cybersecurity Incident Response Team" means the team designated under section 8(1) as the National Cybersecurity Incident Response Team;

"National Cybersecurity Unit" or "Unit" means the Unit referred to under section 7(1);

"policy direction" means a policy direction issued in accordance with section12 by the Minister;

"significant cybersecurity event" means a cybersecurity threat or event that—

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

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

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

(d) is of a severe nature, in terms of the severity of the harm that may be caused to persons in Bermuda 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.

Application to the Crown

3 This Act binds the Crown.

PART 2

CYBERSECURITY ADVISORY BOARD AND NATIONAL CYBERSECURITY UNIT

Cybersecurity Advisory Board

4 (1) There is established a Board to be known as the Cybersecurity Advisory Board.

(2) The Board shall consist of the following persons—

(a) the Chief Information Security Officer in the Ministry of National Security;

(b) the Chief Information Officer in the Department of Information and Digital Technologies;

(c) the Head of the Bermuda Public Access to Information/Personal Information Protection Unit;

(d) the National Disaster Coordinator in the Ministry of National Security;

(e) a representative from the Bermuda Police Service Cybercrime Unit as designated by the Commissioner of Police;

(f) the Chief Health Information Officer from the Bermuda Hospitals Board;

(g) two private sector cybersecurity advisors; and

(h) a barrister and attorney of at least eight years' standing with experience in cybersecurity.

(3) The Minister shall, from among the members of the Board, appoint—

(a) a Chairman; and

(b) a Deputy Chairman.

(4) The Minister may appoint a person to act as alternate to any member of the Board appointed under subsection (2).

(5) The Schedule shall have effect as to terms of appointment, meetings and proceedings of the Board.

Functions of the Cybersecurity Advisory Board

5 (1) The principal function of the Board shall be to advise the Minister on the safeguarding of information resources connected to essential operations in Bermuda.

(2) Without derogating from the generality of subsection (1), the Board shall—

(a) provide advice on the management of cybersecurity to protect Bermuda's economic wellbeing and to prevent cybercrime;

(b) provide advice to the Cabinet on the management of Bermuda's national cybersecurity strategy and the internal Government cybersecurity programme;

(c) provide advice to the Public Service Executive on the management of the Government cybersecurity programme;

(d) provide advice to relevant Public Officers to enable them to meet responsibilities relating to the Government's cybersecurity programme;

(e) provide advice to CNII enforcement authorities;

(f) coordinate and encourage collaboration amongst the Government and other CNII enforcement authorities and the entities they regulate; and

(g) perform such other functions related to the foregoing as the Minister may determine.

Reports of the Board

6 (1) The Board shall, at the end of every period of six months or as soon as practicable thereafter, forward to the Minister a report on the exercise of the functions of the Board during that period.

(2) The report referred to in subsection (1) shall include—

(a) information on the general state of cybersecurity in Bermuda, significant changes to the state of cybersecurity and any threats to cybersecurity in Bermuda;

(b) any general or policy directions given by the Minister to the Board during that period and the manner in which those directions were carried out.

(3) Where a significant cybersecurity event has occurred, the Board shall provide a report of the event to the Minister as directed by the Minister.

National Cybersecurity Unit

7 (1) There shall continue in existence within the Ministry of National Security a unit known as the National Cybersecurity Unit.

(2) The National Cybersecurity Unit shall conduct such functions in relation to cybersecurity as the Minister may determine after consulting the Board and, without derogating from the generality of the foregoing, the Unit shall—

(a) operate and maintain the Cybersecurity Operation Centre;

(b) operate and maintain the National Cybersecurity Incident Response Team in accordance with the designation of the Team under section 8;

(c) provide specialised security services, capabilities, and expertise to support the Government and other CNII enforcement authorities and entities to enable the detection, identification, response, recovery and protection against cybersecurity threats and incidents;

(d) perform secure centralised security logging and monitoring of the Government's information and technology systems and environment to support the detection, analysis, response and investigation of cybersecurity threats and incidents;

(e) perform security and risk assessments of Government information technology systems and environment (independent of the Government information technology staff members, vendors, contractors, and service providers responsible for implementing, operating and maintaining the Government computer systems) including—

(i) security testing;

(ii) threat and vulnerability identification;

(iii) risk analysis;

(iv) evaluation protection measures; and

(v) other related matters;

(f) conduct an annual national cyber risk assessment of critical national infrastructure sectors in Bermuda and provide a report and recommendations to the Minister and the Board;

(g) provide specialized expertise and services to support computer system security planning, secure computer system design and enterprise security architecture for Government Ministries and Departments;

(h) operate as the single point of contact for cybersecurity matters at national and international levels.

(3) In this section, "Cybersecurity Operation Centre" means the centre providing the technology and other resources necessary to support the National Cybersecurity Unit and the National Cybersecurity Incident Response Team.

PART 3

DESIGNATION OF NATIONAL CYBERSECURITY INCIDENT RESPONSE TEAM, CNII ENFORCEMENT AUTHORITIES AND ENTITIES

Designation of National Cybersecurity Incident Response Team

8 (1) The Unit is designated as the National Cybersecurity Incident Response Team to lead the detection of, and response to, cybersecurity events in Bermuda.

(2) The National Cybersecurity Incident Response Team shall conduct the following functions—

(a) monitor cybersecurity events in Bermuda;

(b) provide early warnings, alerts, announcements and dissemination of information to relevant stakeholders about risks and cybersecurity events;

(c) respond to any cybersecurity event notified to it as the Minister may direct;

(d) establish relationships to facilitate cooperation and coordination to address threats of cybersecurity events with—

(i) CNII enforcement authorities and entities in Bermuda;

(ii) other Cybersecurity Incident Response Teams established within Bermuda;

(iii) cybersecurity regulators of other jurisdictions, with the written consent of the Minister and the Attorney General;

(e) promote the adoption and use of common or standardised practices for—

(i) managing cybersecurity events and risk-handling procedures;

(ii) cybersecurity events, risk and information classification schemes; and

(f) co-operate with CNII enforcement authorities to enable the authorities to fulfil their obligations under the Act.

Designation of CNII enforcement authorities

9 (1) For the purposes of this Act, the Minister may, after consulting the Board, designate an entity in Bermuda as a CNII enforcement authority charged with the duties and functions provided by and under this Act.

(2) Each CNII enforcement authority shall, within 30 days of being designated as a CNII enforcement authority, submit to the Minister—

(a) a list of CNII entities that provide essential services and are within its sector or are regulated by the CNII enforcement authority, that meet the criteria as provided in section 10(2);

(b) the particular criteria utilised by the CNII enforcement authority to determine an entity as qualifying to be a CNII entity for the purposes of paragraph (a).

(3) A CNII enforcement authority designated under subsection (1) shall, with respect to the CNII entities it is designated to regulate for the purposes of this Act, implement and enforce—

(a) cybersecurity legislative requirements;

(b) policy directions;

(c) codes of practice; and

(d) standards of performance,

as provided under this Act and regulations made under this Act.

Designation of CNII entities

10 (1) The Minister may, after consulting the Board and the appropriate CNII enforcement authority, designate an entity as a CNII entity if—

(a) that entity is listed as an entity providing an essential service under the sector of a CNII enforcement authority as mentioned under section 9(2)(a); and

(b) the CNII enforcement authority has concluded that the entity meets the criteria to be designated as a CNII entity as provided in subsections (2) and (3).

(2) An entity meets the criteria to be determined to be a CNII entity for purposes of subsection (1) if—

(a) it provides an essential service provided by a critical national infrastructure sector;

(b) its provision of that essential service relies on computer systems, the disruption of which would have a significant effect on the provision of the essential service in Bermuda; and

(c) the CNII enforcement authority concludes, after considering the factors set out in subsection (3), that a cybersecurity event affecting the provision of that essential service by that entity is likely to have significant disruptive effects on the provision of the essential service.

(3) In order to arrive at the conclusion mentioned in subsection (2)(c), the CNII enforcement authority shall have regard to the following factors—

(a) the number of users relying on the service provided by the entity;

(b) the degree of dependency of the other relevant sectors on the service provided by that entity;

(c) the likely impact of cybersecurity events on the essential service provided by that entity, in terms of its degree and duration, on economic and societal activities or public safety;

(d) the market share of the essential service provided by that entity;

(e) the importance of the provision of the service by that entity for maintaining a sufficient level of that service, taking into account the availability of alternative means of essential service provision;

(f) the likely consequences for national security if a cybersecurity event impacts on the service provided by that entity; and

(g) any other factor the CNII enforcement authority considers appropriate to have regard to, in order to arrive at the conclusion under subsection (2)(c).

Minister to issue order to designate CNII enforcement authorities and entities

11 (1) The Minister may, after consultation with the Board and an entity that he proposes to designate as a CNII enforcement authority, by order published in the Gazette designate the entity as a CNII enforcement authority.

(2) Where a designated CNII enforcement authority has, in accordance with section 9(2), submitted to the Minister the list of entities to be designated CNII entities under the CNII enforcement authority, the Minister may by order published in the Gazette designate such entities as CNII entities.

(3) The Minister may vary a designation of, or remove from designation, a designated CNII enforcement authority or entity by order published in the Gazette.

PART 4

POLICY DIRECTIONS, CODES OF PRACTICE AND STANDARDS OF PERFORMANCE

Power of Minister to issue written policy directions

12 (1) The Minister may, after consultation with the Board and relevant CNII enforcement authorities, issue a written policy direction, either of a general or specific

nature, to a CNII enforcement authority where he considers it necessary or expedient for—

(a) ensuring the cybersecurity of a CNII entity under the CNII enforcement authority's sector; or

(b) the effective administration of this Act.

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

(a) the action to be taken by the CNII entity in relation to a cybersecurity threat;

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

(c) the appointment of an auditor approved by the Minister as provided in regulations made under section 16 to audit the CNII enforcement authority on its compliance with this Act or any code of practice or standard of performance applicable to the CNII entity; or

(d) any other matter that the Minister may consider necessary or expedient to ensure the cybersecurity of the critical national information infrastructure in Bermuda.

(3) A policy direction under subsection (1) may, after consultation with the Board and relevant CNII enforcement authorities, be revoked at any time by the Minister.

(4) Before giving a policy direction under subsection (1), the Minister shall, unless the Minister considers that it is not practicable or desirable to do so, give notice to the CNII enforcement authority—

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

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

(5) The Minister shall consider any representations or objections which are duly made before giving any policy direction.

(6) Any policy direction shall be published in the Gazette, but the Minister may cause to be redacted any portion of the policy direction if he reasonably concludes that publication of that portion of the policy direction would—

(a) jeopardize national security;

(b) result in the disclosure of confidential, proprietary or sensitive information; or

(c) harm the public interest.

(7) A CNII enforcement authority and any CNII entity to which the policy direction applies shall act in accordance with any policy directions made pursuant to subsection (1).

Codes of practice and standards of performance

13 (1) The Minister may, after consultation with the Board and CNII enforcement authorities, from time to time—

(a) issue codes of practice or minimum standards of performance for CNII entities; or

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

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

PART 5

ENFORCEMENT MEASURES

Enforcement of policy directions

14 (1) In any case in which the Minister concludes that a CNII enforcement authority or entity has not complied within a reasonable period of time with a policy direction issued by the Minister under section 12, the Minister may require the CNII enforcement authority or entity to provide a written response, within a reasonable period of time specified by the Minister, that identifies and explains the actions that the CNII enforcement authority or entity has taken, or will take, to implement the policy direction.

(2) If the Minister concludes that the response of the CNII enforcement authority or entity does not resolve the matter, the Minister may require the CNII enforcement authority or entity to meet with the Minister, at a reasonable time specified by the Minister, to discuss the matter.

(3) Following the meeting with the CNII enforcement authority or entity, the Minister may issue—

(a) a further policy direction that clarifies, modifies or reaffirms the original policy direction; or

(b) a notice that rescinds the policy direction.

(4) The further policy direction or notice, as the case may be, shall be published in the Gazette, but the Minister may cause to be redacted any portion of the direction or notice that he reasonably concludes meets the standards specified in section 12(6).

(5) In any case in which the Minister concludes that the CNII enforcement authority or entity has not complied with a further policy direction that the Minister issued pursuant to subsection (3), and is not likely to do so within a reasonable period of time, the Minister may apply to the Supreme Court for an order that the CNII enforcement authority or entity comply with the direction.

PART 6

MISCELLANEOUS

Minister's review and report

15 (1) The Minister shall—

(a) carry out an annual review of compliance with cybersecurity requirements under this Act; and

(b) publish a report setting out the conclusions of that review.

(2) The Minister shall as soon as practicable after publication of the report cause a copy to be laid before both Houses of the Legislature.

(3) The Minister shall cause the first annual review of compliance with cybersecurity requirements under this Act to be carried out by 30 June 2025.

Regulations

16 (1) The Minister may make regulations for the purposes of this Act prescribing anything that is necessary or expedient to be prescribed for the carrying out of the provisions of this Act or to give effect to it and, without derogating from the generality of the foregoing, provide for the conduct of the functions of the—

(a) National Cybersecurity Unit; and

(b) National Cybersecurity Incident Response Team.

(2) Regulations made by the Minister under subsection (1) may require a CNII enforcement authority or entity to—

(a) implement and maintain an organization-wide, risk-based cybersecurity programme aligned with industry standards and commensurate to the associated level of risk—

(i) to individuals;

(ii) to the organization;

(iii) to other organizations; and

(iv) that may impact Bermuda;

(b) appoint an appropriately qualified individual to lead the development and administration of the cybersecurity programme;

(c) identify computer systems supporting its critical services;

(d) identify vulnerabilities and threats related to computer systems supporting its critical services;

(e) appropriately manage cyber risks related to computer systems supporting its critical services that may impact—

(i) individuals;

(ii) other organizations; and

(iii) Bermuda;

(f) provide appropriate role-specific, cybersecurity awareness and training for employees at every level across the organization;

(g) maintain board-level or equivalent, and senior management level direction and oversight of the cybersecurity programme and cyber risk management within the organization;

(h) obtain independent assessments and audits of its cybersecurity programme and the security of computer systems supporting its critical services;

(i) report significant cybersecurity event threats, vulnerabilities, and events related to computer systems supporting critical services to the relevant CNII enforcement authority and the National Cybersecurity Incident Response Team;

(j) implement and maintain adequate monitoring of the computer systems supporting its critical services to detect significant cybersecurity events, cybersecurity breaches and support cybersecurity event response and investigation;

(k) implement, maintain, and test cybersecurity event response plans and capabilities to identify, respond to, and recover from cybersecurity events related to computer systems supporting its critical services;

(l) implement, maintain, and test adequate disaster recovery plans and capabilities to the failures or losses of computer systems supporting its critical services;

(m) act in such other manner or conduct such other functions determined necessary for the purposes of maintaining adequate security of computer systems supporting critical services.

(3) Regulations made under this Act may create offences and provide that a person who commits an offence against the regulations is liable on summary conviction to a fine not exceeding $100,000.

(4) Regulations and any orders made under this Act are subject to the negative resolution procedure.

Consequential amendments

17 The Minister may, by regulations, make amendments to such enactments or instruments as appear to the Minister to be necessary or expedient in consequence of, or for the purposes of, this Act or regulations made under this Act.

Commencement

18 This Act shall come into operation on such day as the Minister may appoint by notice published in the Gazette.

SCHEDULE

(section 4(5))

PROCEEDINGS OF CYBERSECURITY ADVISORY BOARD

1 A member of the Cybersecurity Advisory Board, referred to in section 4(2)(g) and (h), shall be appointed on such conditions and for such terms as may be determined by the Minister.

2 The members of the Cybersecurity Advisory Board, referred to in section 4(2)(g) and (h), shall be appointed as follows—

(a) at least one member for a term of two years;

(b) at least one member for a term of three years;

(c) at least one member for a term of four years,

and may be reappointed.

3 (1) Any member of the Board referred to in section 4(2)(g) and (h), other than the Chairman or Deputy Chairman, may at any time resign his office by instrument in writing addressed to the Minister and transmitted through the Chairman, and from the date of the receipt by the Minister of such instrument, such member shall cease to be a member of the Board.

(2) The Chairman or Deputy Chairman may at any time resign his office by instrument in writing addressed to the Minister and such resignation shall take effect as from the date of the receipt of such instrument by the Minister.

4 The Minister may declare the office of a member of the Board appointed under section 4(2)(g) and (h) vacant if he is satisfied that the member—

(a) has without reasonable excuse been absent from—

(i) three consecutive meetings of the Board; or

(ii) two-thirds of the meetings of the Board convened in any year;

(b) has been convicted (whether before or after his appointment) of a criminal offence of dishonesty;

(c) is an undischarged bankrupt or his estate has been sequestrated and he has not been discharged;

(d) has made a composition or arrangement with, or granted a trust deed for, his creditors; or

(e) is otherwise unable, unfit or unwilling to carry out his functions as Chairman, Deputy Chairman or member, as the case may be.

5 A person appointed to fill the place of a member of the Board before the end of the member's term of office shall hold office so long only as the vacating member would have held office.

6 No member of the Board shall take part in an inquiry, consultation or decision relating to any specified business in which he or his spouse is a member or shareholder or has any private interest, direct or indirect, whereby his private interest may conflict with his duties as a member.

7 The Board may act notwithstanding any vacancy in its membership, and no act of the Board shall be deemed to be invalid only by reason of a defect in the appointment of a member thereof.

8 The Board shall meet at least once every quarter but meetings may be held at any time to enable the Board to dispatch its business under this Act.

9 If at any meeting of the Board the Chairman is absent, the Deputy Chairman shall preside over that meeting; and if both the Chairman and the Deputy Chairman are absent the members present shall elect one of their number to act as Chairman at that meeting.

10 The Chairman shall cause copies of the minutes taken at each meeting of the Board during each quarter of the year to be delivered to the Minister no later than 30 days after the end of the quarter.

11 The quorum of the Board shall be at least five members.

12 The validity of any business transacted by the Board and the proceedings thereof shall not be affected by reason of the absence of any member or any vacancy in the numbers thereof.

13 Any direction of the Board given under this Act shall be deemed to be duly authenticated if it is given under the hand of the Chairman or, in his absence, the Deputy Chairman.

14 In any matter before the Board, the Chairman or person acting as Chairman shall have a deliberative as well as a casting vote.

15 Every question or matter to be determined by the Board at any meeting shall be decided by a majority of the votes of the members present and voting on the question or

matter; provided that in the event of an equal division of votes the Chairman of the meeting may, if he thinks fit, give a second or casting vote.

16 Subject to this Schedule, the Board may determine its procedure.

17 For the purposes of this Schedule, a reference to a member or the membership of the Board shall, unless the context otherwise requires, be construed as including the Chairman and Deputy Chairman.

[Assent Date: 24 June 2024]