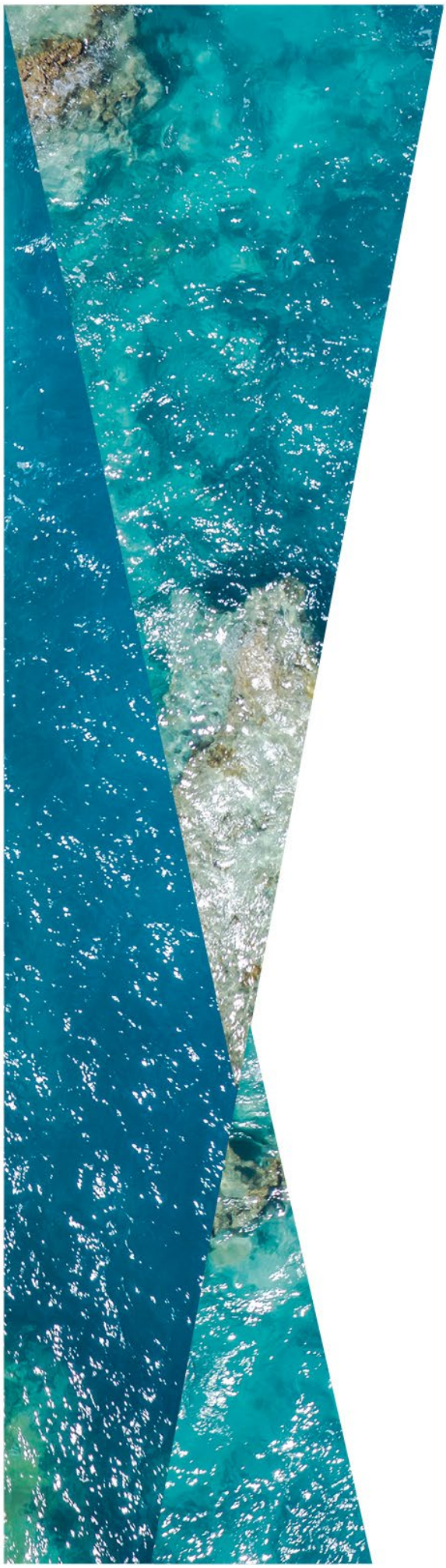


CYBERSECURITY FOR CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

Cybersecurity Act 2024 to usher in a new era for the protection of Bermuda's critical national information infrastructure.

3 June 2024

ATTORNEY CONTRIBUTOR

Ms. Gretchen Tucker is a Bermuda and England & Wales (non-practicing) qualified barrister and Counsel, Head of Regulatory & Governance at BeesMont Law Limited. She provides advice and representation in connection with regulatory and statutory compliance, administrative decision-making, statutory interpretation and legal reform.

The Cybersecurity Act 2024 (**Act**) is intended to propel the policy objectives of the Government of Bermuda (**Government**) to safeguard the welfare of economic growth and national interests into a bespoke legislative framework for the protection of the jurisdiction's critical national information infrastructure (**CNII**).

The legislation was tabled in the House of Assembly on the same date as the Computer Misuse Act 2024 on 3 May 2024. The proposed statute were received for debate in the wake of the September 2023 attack on the systems of the Government. This assault has been most recently described as a "cyberattack" by the Minister of National Security (**Minister**) in their 3 May 2024 Cyber Security Update. The cyberattack caused pro-longed disruptions to various public services in Bermuda which lasted weeks, or even months. The Minister has confirmed that the event served to fortify a commitment to ensure that the policies, legislation and capabilities around cybersecurity and cybercrime align with the Government's objective of being a premier financial technology jurisdiction. For those stakeholders identified as CNII enforcement authorities and CNII entities to be subject to the regulatory remit of the Act, now it is the time to get to grips with the newly proposed framework before the legislation comes into force

Status of the Cybersecurity Bill

The Act was passed by the House of Assembly on 31 May 2024. In Bermuda, proposed legislation starts as a bill which can be tabled in either the Senate or the House of Assembly, but traditionally bills are tabled in the House of Assembly. Once a bill has passed through one House, the bill will then be signed by the Speaker and sent to the Senate. After the bill has been approved in both Houses, it will go to the Premier of Bermuda and then to the Attorney General Chambers for review. Lasty, it will be sent to the Governor of Bermuda for Assent and then the Minister may publish a Commencement Day Notice in the Official Gazette which notifies of the day that the Act comes into operation within the jurisdiction.

Key Terms

For the purposes of this overview, the following four terms are critical to understanding the intended operation of the Act:

critical national information infrastructure / CNII

refers to 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

refers to 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.

cybersecurity event

refers to 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.

significant cybersecurity event

refers to 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.

Proposed Statutory Advisory and Supervisory Bodies

The Act will establish a Cybersecurity Advisory Board (**Board**) which will have the principal function of advising the Minister on the management and oversight of cybersecurity in Bermuda for the purpose of safeguarding information resources connected to essential operations in Bermuda. Interestingly, there is no definition of "cybersecurity" in the legislation at this time. On this basis, it would appear that anything contributing to, causing or otherwise involved in a cybersecurity event or a significant cybersecurity event *could* potentially fall within the advisory remit of the Board.

A National Cybersecurity Unit (**Unit**) is further proposed to operate and to maintain a Cybersecurity Operation Centre, which will provide the technology and other resources for this statutory body. The Unit is also designated by the Act as the National Cybersecurity Incident Response Team for the island and is proposed to have 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;

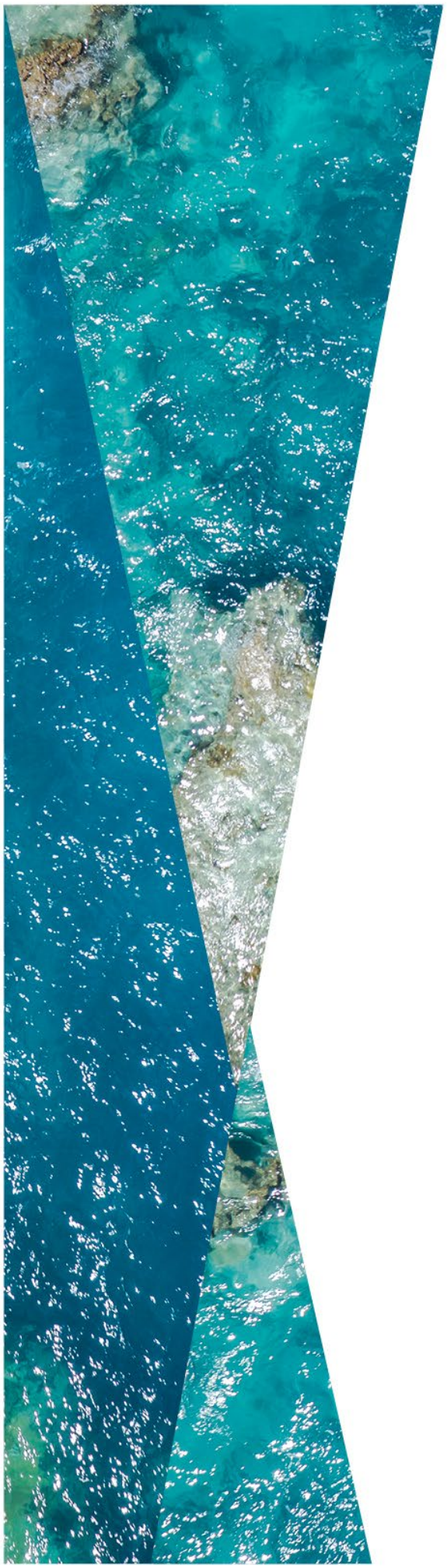
  (iii) cybersecurity regulators of other jurisdictions, with the written consent of the Minister and the Attorney General;

(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.



Statutory Designations and Reporting Obligations

The Act identifies an initial listing of CNII enforcement authorities and confirms that the Minister, after consulting the Board, may designate further entities in Bermuda as CNII enforcement authorities charged with certain statutory duties and functions.

Amongst other activities, CNII enforcement authorities will be responsible for:

- submission to the Minister of a listing of CNII entities that provide essential services and are within its sector or are regulated by the CNII enforcement authority which meet certain criteria; and

- implementation and enforcement of cybersecurity legislative requirements, policy directions, codes of practice and standards of performance for the CNII entities that it is designated to regulate.

The Act similarly provides an initial listing of CNII entities and confirms that the Minister, after consulting the Board and the appropriate CNII enforcement authority, may designate further entities in Bermuda as CNII entities *if* they meet certain criteria.

Enforcement Measures

The Act proposes a sliding scale of enforcement measures dependent on the nature and extent of non-compliance in respect of its provisions:

(a) Non-compliance with Policy Directions

If the Minister concludes that a CNII enforcement authority or entity has not complied *within a reasonable period of time* with a Ministerial policy direction, the Minister may require the CNII enforcement authority or entity to provide a written response. Such a response must be provided within a reasonable period of time, as specified by the Minister. The response must identify and explain the actions that the CNII enforcement authority or entity has taken, or will take, to implement the policy direction.

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.

Following the meeting with the CNII enforcement authority or entity, the Minister may issue a further policy direction that clarifies, modifies or reaffirms the original Ministerial policy direction or a notice that rescinds that policy direction.

Enforcement Measures (continued)

Where the Minister concludes that the CNII enforcement authority or entity has not complied with any further policy direction and is not likely to do so within a reasonable period of time, the Minister may apply to the Supreme Court of Bermuda for an order that the CNII enforcement authority or entity comply with the direction.

(b) Non-compliance with Regulations

The Act proposes that the Minister may make regulations for the purposes of the legislative framework.

Such regulations, amongst other matters, 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.

BEESMONT
Law Limited

The content of this article is intended to provide a general overview of legislation which is not yet in force in Bermuda as of the date of its publication. Specific legal advice should be sought for any matters pertaining to its subject matter and this article is not a substitute for the undertaking of legal advice by a Bermuda registered attorney.