NITIJELA OF THE REPUBLIC OF THE MARSHALL ISLANDS
46TH CONSTITUTIONAL REGULAR SESSION, 2025

Republic of the Marshall Islands
Jepilpilin Ke Ejukaan

CYBERSECURITY ACT 2025

Index

Section **Page**

§101. Short title....3
§102. Purpose....3
§103. Interpretation....3
PART II –ADMINISTRATION....7
§104. Cybersecurity functions of the Office of National Security....7
PART III - CYBERSECURITY OF CRITICAL INFORMATION INFRASTRUCTURE....9
§105. Designation of critical information infrastructure....9
§106. Cybersecurity of critical information infrastructure....11
§107. Cybersecurity incident reporting obligations....13
§108. Provision of information relating to critical information infrastructure....14
§109. Power to issue written orders....15
§110. Change in ownership of critical information infrastructure....16
PART IV –THE CSIRT-MH....17
§111. Establishment of the CSIRT-MH....17
§112. Functions of the CSIRT-MH....17
§113. Responsibility relating to response to cybersecurity incidents....18
PART V – CYBERSECURITY SERVICE PROVIDERS....19
§114. Accreditation of cybersecurity service providers....19
§115. Regulations for the accreditation of cybersecurity service providers....19
PART VI - MISCELLANEOUS....20
§119. Initial designation of critical information infrastructure and essential services....20
§120. Liability of a corporation....20
§121. Exemptions....20
§122. General Non-Compliance....21
§123. Regulations on Penalties....21
§124. Effective date....21

NITIJELA OF THE REPUBLIC OF THE MARSHALL ISLANDS
46TH CONSTITUTIONAL REGULAR SESSION, 2025

Republic of the Marshall Islands
Jepilpilin Ke Ejukaan

CYBERSECURITY ACT 2025

AN ACT to create a new Chapter the Cybersecurity Act under Title 43 of MIRC establishing a legal framework to prioritize cybersecurity, identify and protect critical information infrastructure from cybersecurity threats and incidents, establish a framework to implement a team to effectively monitor and respond to cybersecurity incidents, and provide for other matters concerning cybersecurity both domestic and international.

BE IT ENACTED BY THE NITIJELA OF THE REPUBLIC OF THE MARSHALL ISLANDS

§101. Short title.

This Act may be cited as the Cybersecurity Act 2025.

§102. Purpose.

The purpose of this Act is to develop the legal framework for cybersecurity as a priority to advance the national security interests of the Republic and to strengthen and maintain secure, functioning, and resilient critical information infrastructure.

As part of this Act, the position of the Chief Information Security Officer (CISO), will be established and will be aligned in the Office of National Security and report to the Director of the Office of National Security.

§103. Interpretation.

In this Act, unless context otherwise requires:

(a) 'access' means gaining entry to a program or computer data stored in a computer system;

(b) 'CERT' means a computer emergency response team;

(c) 'computer' means a unit of physical or virtual hardware or equipment, or any part thereof, that performs predetermined arithmetic, logical, routing, processing or storage operations in accordance with set instructions and includes input devices, output devices, processing devices, computer data storage mediums, and other equipment and devices related to, or connected with a computer system;

(d) 'computer data' or 'data' means any representation of facts, information, or concepts in a form suitable for processing in a computer system, including a computer program;

(e) 'computer program' or 'program' means any computer data representing algorithms, codes, instructions, or statements suitable to cause a computer system to perform a function or a series of functions;

(f) 'computer system' means any computer or a group of interconnected or related computers, one or more of which, pursuant to a program, performs automatic processing of data and any other function related to data;

(g) 'critical information infrastructure' means such computers, computer systems, and computer data in respect of which a designation is made in accordance with section 5 or section 19;

(h) 'CSIRT-MH' means the Cyber Security Incident Response Team of the Marshall Islands established in accordance with section 11;

(i) 'cybersecurity' means the state in which a computer or computer system is protected from unauthorized access or attack, and because of that state:

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

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

(iii) the availability, authenticity, integrity or confidentiality of data stored in, processed by, or transmitted through the computer or computer system is maintained;

(j) 'cybersecurity incident' means an act, activity or event having an actual adverse effect on cybersecurity;

(k) 'CISO' refers to the Chief Information Security Officer who reports to the Director of the Office of National Security. The CISO will be responsible for overseeing the government's cybersecurity strategy, the protection of its information systems and data from cyber threats, and ensuring compliance with relevant policy and security regulations.

(k) 'cybersecurity service' means a service provided by a person for compensation that is intended primarily for or aimed at safeguarding the cybersecurity of a computer or computer system belonging to another person, and includes specific activities defined in regulation;

(l) 'cybersecurity service provider' means a person who provides a cybersecurity service;

(m) 'cybersecurity solution' means any computer, computer system, computer program or computer data designed for, or purported to be designed for, ensuring or enhancing the cybersecurity of another computer or computer system;

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

(o) 'cybersecurity vulnerability' means any weakness, susceptibility or flaw of a computer or computer system that can be exploited by one or more cybersecurity threats;

(p) 'de minimis' means an owner that supplies less than ten (10) percent of the market for an essential service;

(q) 'Director' means the Director of National Security established in the National Security Act, 2024, or its successor;

(r) 'Government' means the National Government of the Republic of the Marshall Islands;

(s) "National Security Council' shall have the meaning established in the National Security Act, 2024, and includes any successor agency;

(t) 'Office of National Security' shall have the meaning established in the National Security Act, 2024, and includes any successor agency;

(u) 'owner, 'in relation to critical information infrastructure, means:

(i) a person that is 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; or

(ii) where the legal owner of the critical information infrastructure and the operator of the critical information infrastructure are different persons, the person that operates the critical information infrastructure within the Republic is treated as the owner of the critical information infrastructure for the purposes of this Act;

(iii) where a critical information infrastructure is legally owned by the Government and operated by a Ministry, the Secretary of 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;

(v) 'person' means a natural person, public body, commercial, non-commercial organization, or other legal person;

(w) 'Republic' means the Republic of the Marshall Islands;

(x) 'risk' means the potential for loss or disruption caused by a cybersecurity threat or cybersecurity incidentand is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the cybersecurity threat or cybersecurity incident;

(y) 'Security Operations Center (SOC)' means equipment, resources and processes used for the monitoring of the level of cybersecurity of a computer or computer system of another person 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.

(z) 'significant cybersecurity incident' means a cybersecurity incident that:

(i) severely harms or creates a risk of severe harm being caused to critical information infrastructure;

(ii) disrupts or creates a significant risk of disruption to the provision of an essential service;

(iii) creates a threat to the national security, defense, foreign relations, economy, public health, public safety or public order of the Republic; or

(iv) is of a severe nature, in terms of the severity of the harm that has been or may be caused to persons in the Republic or the number of computers or value of the data put at risk, whether or not the computers or computer systems put at risk are themselves critical information infrastructure.

PART II –ADMINISTRATION

§104. Cybersecurity functions of the Office of National Security.

(1) The Office of National Security shall exercise the following functions in relation to cybersecurity:

(a) advise the National Security Council on cybersecurity matters;

(b) lead the development, review, and update of a national cybersecurity policy and strategy;

(c) designate critical information infrastructure for purposes of cybersecurity;

(d) coordinate and facilitate the implementation of the framework to manage the risksto critical information infrastructure from cybersecurity threats and cybersecurity incidents;

(e) issue orders and directions to owners of critical information infrastructure with regard to the cybersecurity;

(f) direct owners of critical information infrastructure to:

(i) take appropriate and proportionate technical, operational and organizational measures to manage cybersecurity risks that may affect critical information infrastructure;

(ii) conduct cybersecurity exercises for the purpose of testing their state of readiness in responding to

cybersecurity incidents and their cybersecurity solutions; and

(iii) take appropriate measures to prevent or minimize the impact of cybersecurity incidents on recipients of essential services;

(g) transmit to the Attorney General information relating to cybersecurity threats and cybersecurity incidents affecting critical information infrastructure;

(h) undertake awareness and cyber hygiene campaigns relating to cybersecurity;

(i) issue and renew accreditations to cybersecurity service providers;

(j) adopt technical standards, protocols, guidelines, and codes of practice for cybersecurity of critical information infrastructure;

(k) provide technical support for cybersecurity investigations and forensic analysis;

(l) define and manage technical response procedures and protocols for cybersecurity incidents;

(m) facilitate technical coordination and information sharing in relation to cybersecurity across Government agencies, departments, state owned entities and the private sector;

(n) operate and manage the CSIRT-MH;

(o) cooperate with CSIRTs or CERTs of other countries or territories on cybersecurity threat intelligence and cybersecurity incidents;

(p) make rules and regulations necessary to implement this Act;

(q) represent the Republic on cybersecurity issues internationally; and

(r) perform any other functions in relation to cybersecurity conferred on it under this Act or necessary to implement this Act.

(2) The cybersecurity functions of the Office of National Security established in this Act shall be exercised by the Director.

(3) The Director may, by written instrument, delegate functions established in this Act to any of the staff of the Office of National

Security or to such other Government agency with technical capabilities to exercise or perform such functions.

(4) A delegation under subsection (3) shall be revocable in writing, at will, and shall not prevent the exercise or performance of a function by the Director under the Act.

PART III - CYBERSECURITY OF CRITICAL INFORMATION INFRASTRUCTURE

§105. Designation of critical information infrastructure.

(1) The Director may, by written order to the owner, designate a computer or computer system as critical information infrastructure for purposes of cybersecurity protections under this Act, provided that:

(a) the computer or computer system is necessary for the continuous delivery of an essential service, and

(b) the loss or compromise of the computer or computer system, or of the computer data stored in, processed by, or transmitted through the computer or computer system, could significantly degrade, impede, disrupt, or otherwise adversely impact the delivery of that essential service in the Republic.

(2) A service qualifies as an essential service for purpose of cybersecurity protections under this Act, if the Director has determined by order that:

(a) the service is essential for the national security, economy, foreign relations, public health, public safety, public order, or the continuous provision of basic public services; and

(b) the loss, damage, compromise, or disruption of the service may severely prejudice:

(i) the national security of the Republic;

(ii) the functioning or stability of the national economy;

(iii) public safety; or

(iv) the public interest.

(3) An order under subsection (1) shall be made after consultation with:

(a) the ministry, department, agency, or authority responsible for regulating, controlling or overseeing any essential service related to a declaration of critical information infrastructure, as applicable;

(b) the owner of such critical information infrastructure; and

(c) any other ministry, department, agency or authority the Office of National Security considers necessary.

(4) An order issued under subsection (1) shall identify:

(a) the computers or computer systems being designated as critical information infrastructure;

(b) the essential service delivered though the critical information infrastructure;

(c) the person or persons that shall be considered as the owner of the critical information infrastructure for purpose of compliance with the obligations set forth under this Act;

(d) the technical standards, protocols, guidelines, or codes of practice on cybersecurity applicable to the owner, if any, and

(e) a timeframe for compliance with obligations under this Act.

(5) The owner of critical information infrastructure may appeal an order issued under subsection (1) to the Cabinet.

(6) The Director may, upon request made by the owner of critical information infrastructure, establish special plans of action and milestones to achieve compliance with an order issued under subsection (1) for that owner, if the Director is satisfied that:

(a) the owner or class of owners is de minimise;

(b) the owner or class of owners has annual revenues below the applicable revenue threshold determined by the Director in regulation; or

(c) compliance with a designation order under subsection (1) would result in a disproportionate burden or excessive costs for the owner.

(7) The Director may consider providing or facilitating the mobilization of financial assistance for owners of critical information infrastructure subject to a special plan of action and milestones in accordance with subsection (6).

(8) The Director may, by written order, at any time amend or withdraw a designation made under subsection (1) if the Director is of the opinion, following consultations consistent with subsection (3), that a designated computer or computer system no longer fulfils the criteria for designation as critical information infrastructure for purposes of cybersecurity protections.

§106. Cybersecurity of critical information infrastructure.

(1) The owner of critical information infrastructure is responsible for implementing:

(a) such technical, operational and organizational measures as necessary to manage cybersecurity risks that may affect critical information infrastructure; and

(b) such measures needed to prevent and mitigate the impact of cybersecurity incidents and cybersecurity threats that may affect critical information infrastructure.

(2) Without limiting the generality of subsection (1), to meet the obligations set forth therein the owner of critical information infrastructure must, at a minimum:

(a) conduct rolling cybersecurity risk assessments of critical information infrastructure with frequent revisit rates as dictated by the cyber threat environment and as prescribed by the CISO.. This assessment will include consideration of:

(i) cybersecurity threats, cybersecurity vulnerabilities, and other risk factors;

(ii) cybersecurity solutions implemented;

(iii) compliance with this Act and any technical standard, protocol, guideline, or code of practice on cybersecurity applicable to the owner; and

(iv) the overall cybersecurity preparedness of the owner's critical information infrastructure against damage or unauthorized access;

(b) develop and implement internal cybersecurity policies and procedures for critical information infrastructure;

(c) develop and implement an internal cybersecurity incident reporting policy; and

(d) develop and implement an internal cybersecurity awareness program.

(3) No later than thirty (30) days after completion of the cybersecurity risk assessment referred to in subsection (2)(a), the owner of the critical information infrastructure must transmit a copy of the cybersecurity mitigation actions to the Director.

(4) The Director may, by order, require an audit of critical information infrastructure under the cognizance Office of the CISO or by an auditor appointed by the Director after consultation with the owner, for the purpose of:

(a) determining the owner's compliance with this Act;

(b) determining compliance with any technical standard, protocol, guideline, or code of practice on cybersecurity applicable to the owner; or

(c) determining the accuracy or completeness of the information transmitted by the owner under this section or under section 8.

(5) The Director may issue an order under subsection (4), if the Director has reason to believe that:

(a) the owner of a critical information infrastructure has not complied:

(i) with an obligation under this Act; or

(ii) a technical standard, protocol, guideline, or code of practice on cybersecurity applicable to the owner; or

(b) any information provided by the owner of a critical information infrastructure under section 8 is false, misleading, inaccurate, or incomplete.

(6) The cost of an audit ordered under subsection (4) must reflect prevailing market prices and be borne by the owner of the critical information infrastructure. The Director may:

(a) decide to make payments to the auditor directly and recover such costs from the owner; or

(b) require the owner to pay the auditordirectly.

(7) Payments made by the Office of National Security to the auditor in accordance with subsection (6)(a) constitute a debt, which may be

recovered by the Director from the owner in a court of competent jurisdiction.

(8) The Director may notmandate an audit in accordance with subsection (4) on the same critical information infrastructure more than once every two (2) years.

(9) A person commits a petty misdemeanor if the person intentionally and without reasonable excuse, fails to comply with the obligation set forth in this section.

§107. Cybersecurity incident reporting obligations.

(1) The owner of critical information infrastructure must immediately notify the Director and the CSIRT-MH of the occurrence of any of the following:

(a) a significant cybersecurity incident in respect to critical information infrastructure;

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

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

(2) To comply with notification requirements set forth in subsection (1), the owner must:

(a) within twenty-four (24) hours of becoming aware of the occurrence, submit an early warning of the cybersecurity incident with information available at that time;

(b) within seventy-two (72) hours after becoming aware of the occurrence, submit a cybersecurity incident notification which must:

(i) update the information referred to in subsection 2(a); and

(ii) indicate an initial assessment of the cybersecurity incident, including its severity and impact, where available;

(c) not later than thirty (30) days after the submission of the notification under subsection 2(b), a final report including the following:

(i) a detailed description of the cybersecurity incident, including its severity and impact;

(ii) the type of threat or root cause that is likely to have triggered the cybersecurity incident; and

(iii) applied and ongoing mitigation measures;

(d) in the event of an ongoing cybersecurity incident, the owner must provide a progress report no later than thirty (30) days after the submission of the notification under subsection 2(b) and a final report within thirty (30) days of the handling of the cybersecurity incident.

(3) The owner of a critical information infrastructure must establish such mechanisms and processes for the purposes of promptly detecting cybersecurity threats, cybersecurity vulnerabilities and cybersecurity incidents in respect of the critical information infrastructure, in a manner consistent with this Act and applicable standards, protocols, guidelines, or codes of practice.

(4) A person commits a petty misdemeanor if the person intentionally and without reasonable excuse fails to make a notification in accordance with this section.

§108. Provision of information relating to critical information infrastructure.

(1) The Director may require the owner of critical information infrastructure to provide, within a reasonable period specified in the order, the following:

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

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

(c) information relating to the operation of critical information infrastructure, and of any other computer or computer system

under the owner's control that is interconnected with or that communicates with critical information infrastructure; and

(d) such other information as the Director may require by order to ascertain the state of cybersecurity of the owner's critical information infrastructure.

(2) The information provided in accordance with an order issued under subsection (1) shall be prepared by a qualified person and shall meet generally acceptable industry standards to ensure accuracy, completeness and quality of such information.

(3) The Office of National Security must implement security measures to safeguard information obtained pursuant to subsection (1).

(4) A person commits a petty misdemeanor if the person intentionally and without reasonable excuse fails to comply with an order issued by the Director under subsection (1).

§109. Power to issue written orders.

(1) The Director may issue a written order, either of a general or specific nature, to the owner of critical information infrastructure or a class of such owners, if the Director is satisfied that such order:

(a) is necessary or expedient for compliance with a standard, protocol, guideline, or code of practice on cybersecurity of critical information infrastructure; or

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

(2) Without limiting the generality of subsection (1), an order issued under that subsection may relate to:

(a) actions to be taken by the owner to:

(i) manage a cybersecurity threat;

(ii) manage cybersecurity risks that may affect critical information infrastructure; or

(iii) prevent or minimize the impact of cybersecurity incidents on recipients of essential services;

(b) compliance with any technical standard, protocol, guideline, or code of practice on cybersecurity applicable to the owner;

(c) the appointment of an auditor approved by the Director to audit critical information infrastructure;

(d) conducting cybersecurity exercises for the purpose of testing the state of readiness of the owner in responding to significant cybersecurity incidents and the cybersecurity solutions implemented to manage cybersecurity risks; or

(e) such other matters as the Director may consider necessary or expedient to ensure the cybersecurity of the critical information infrastructure.

(3) Prior to issuing an order under subsection (1), the Director must, unless the Director considers that it is not practicable or desirable to do so, give notice to the person or persons whom the Director proposes to issue the order:

(a) stating that the Director proposes to issue the order and setting out its effect; and

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

(4) A person commits a petty misdemeanor if the person intentionally and without reasonable excuse fails to comply with an order issued by the Director under subsection (1).

§110. Change in ownership of critical information infrastructure.

(1) Where there is a change in ownership resulting in a change of control of a critical information infrastructure, the relevant person must inform the Director of the change in ownership no later than seven (7) days after the date of that change in ownership.

(2) For the purpose of this section:

(a) "control" means:

(i) the ability to direct the management or operation of the critical information infrastructure; or

(ii) the ability to obtain economic benefits from the essential service operated by the critical information infrastructure;

(b) "relevant person" means the owner of the critical information infrastructure identified by the Director in an order issued under section 5(4)(c).

(3) A person commits a petty misdemeanor if the person intentionally and without reasonable excuse fails to comply the obligation set forth under subsection (1).

PART IV –THE CSIRT-MH

§111. Establishment of the CSIRT-MH.

(1) The Director is responsible for the establishment of the CSIRT-MH which shall be the responsible team for coordinating cybersecurity incident response activities at the national level.

(2) The Director shall appoint a suitable qualified person to be the Administrator of CSIRT-MH, who shall lead and be responsible for the performance of the CSIRT-MH.

(3) The Administrator of CSIRT-MH, having had regard to the required skills and experience for an effective cybersecurity incident response team, shall determine:

(a) the appropriate members of the CSIRT-MH;

(b) whether such members shall be locally based or internationally based; and

(c) whether such members shall be natural persons or one or more legal persons.

§112. Functions of the CSIRT-MH.

(1) The CSIRT-MH shall have the following functions:

(a) provide cybersecurity incident response services;

(b) disseminate cybersecurity alerts, advisories, and cybersecurity vulnerability notes to Government and to the public;

(c) assess and analyze the impact of cybersecurity incidents;

(d) perform SOC functions for the national government;

(e) serve as the first point of contact with reference to the handling of cybersecurity incidents and communication with foreign CSIRTs or CERTs;

(f) promote awareness of technical cybersecurity standards, protocols, guidelines and codes of practice and cyber hygiene within the Government and to owners of critical information infrastructure;

(g) participate in information sharing and disseminate information with foreign CSIRTs and CERTs on emerging cybersecurity threats to critical information infrastructure;

(h) participate in and be a member of regional and international CSIRTs and CERT groups; and

(i) perform any other technical functions delegated on it by the Director for purposes of implementing this Act.

(2) The Office of National Security may enter into agreements with third parties, including regional bodies or private corporations, to undertake some or all of the functions of the CSIRT-MH, provided that such agreements are in the opinion of the Director necessary to:

(a) achieve national security interests of the Republic; or

(b) achieve compliance with the objectives and requirements of this Act.

§113. Responsibility relating to response to cybersecurity incidents.

(1) The Director must ensure that the CSIRT-MH is appropriately resourced to effectively respond to cybersecurity incidents.

(2) To meet the obligation set forth in subsection (1), the Director may:

(a) enter into agreements, including with international agencies, development partners and donors, to secure funding, access cybersecurity solutions, or obtain other resources to support the CSIRT-MH functions; and

(b) enter into contracts for the purchase, lease, license or use of cybersecurity solutions and provision of support services for the CSIRT-MH, including fees, licenses and other costs.

PART V – CYBERSECURITY SERVICE PROVIDERS

§114. Accreditation of cybersecurity service providers.

(1) No person may engage in the business of providing accreditable cybersecurity services except if that person holds an accreditation issued by the Director or an accreditation officer appointed by the Director.

(2) The Director or an accreditation officer shall grant an application for accreditation or renewal of accreditation under subsection (1) if the Director or accreditation officer is of the opinion that:

(a) the person is a fit and proper person to hold or to continue to hold the accreditation; or

(b) it is in the public interest to grant or renew the accreditation; or

(c) the grant or renewal of the accreditation is consistent with national security.

(3) An accreditation shall be in force for a period not exceeding five (5) years as specified in the accreditation, starting from the date of issuance with the understanding that the entity maintains currency in applicable certifications and required trainings.

(4) A person commits a misdemeanor if the person provides a cybersecurity service in contravention with contravenes subsection (1).

§115. Regulations for the accreditation of cybersecurity service providers.

(1) The Director shall make regulations establishing:

(a) the types of cybersecurity services covered under this Act;

(b) the specific cybersecurity services subject to accreditation;

(c) the process, conditions and requirements that must be satisfied by an applicant to obtain an accreditation under section 14(1);

(d) the eligibility requirements applicable to obtain an accreditation under section 14(1);

(e) the conditions applicable to the accreditation, including prescribed fees, if any;

(f) the obligations of accredited cybersecurity service providers; and

(g) such other matters relevant to the effective implementation of this subchapter.

PART VI - MISCELLANEOUS

§119. Initial designation of critical information infrastructure and essential services.

(1) The Director shall, no later than twelve (12) months after the effective date of this Act, issue an initial designation order:

(a) designating critical information infrastructure in accordance with the requirements of section 5; and

(b) identifying essential services in accordance with section 6.

(2) In the initial designation order made pursuant to subsection (1), the Director may establish a timeline of up to twelve (12) months from the date of the order for owners or classes of owners of critical information infrastructure to take the necessary actions and make the necessary investments to comply with the obligations set forth in this Act.

§120. Liability of a corporation.

A corporation may be convicted of the commission of an offense under this Act in accordance with the requirements of section 2.07(1) of the Criminal Code.

§121. Exemptions.

The Director may, by order and prior consultation with the National Security Council, exempt any person or any class of persons from all or part of the obligations of this Act, either generally or in a particular case and subject to such conditions as may be prescribed.

§122. General Non-Compliance.

Any person who, without reasonable excuse, fails to comply with any obligation imposed under this Act, or any regulations made pursuant to this, commit an offense and shall, upon conviction, be liable to:

(1) In the case of an individual:

(i) a fine not exceeding $10,000, or imprisonment for a term not exceeding two (2) years, or both;

(2) In the case of a corporation:

(i) a fine not exceeding $100,000; or suspension or revocation of relevant cybersecurity accreditations, where applicable.

§123. Regulations on Penalties.

The Director, by regulation, shall establish additional penalties guidelines, include administrative fines and settlement mechanism for minor violations which shall be made in accordance with the Administrative Procedures Act.

§124. Effective date.

(1) Parts I, II, III, IV, and VI of this Act will take effect on the date of certification in accordance with Article IV, section 21 of the Constitution.

(1) Part V of this Act shall enter into effect upon the promulgation of implementing regulations by the Director.

CERTIFICATE

I hereby certify:

1. That Nitijela Bill No: 42ND1 was passed by the Nitijela of the Republic of the Marshall Islands on the 7th day of April 2025; and

2. That I am satisfied that Nitijela Bill No: 42ND1 was passed in accordance with the relevant provisions of the Constitution of the Republic of the Marshall Islands and the Rules of Procedures of the Nitijela.

I hereby place my signature before the Clerk this 21st day of April 2025.

Attest:

Brenson S. Wase
Speaker
Nitijela of the Marshall Islands

Morean S. Watak
Clerk
Nitijela of the Marshall Islands