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

Republic of the Marshall Islands
Jepilpilin Ke Ejukaan

CYBERCRIMES ACT 2025

Index

Section **Page**

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

Republic of the Marshall Islands
Jepilpilin Ke Ejukaan

CYBERCRIMES ACT 2025

AN ACT to define cybercrimes, establishing procedural provisions to enable investigation of cybercrimes and to promote international cooperation measures in relation to cybercrimes in a manner that is consistent with the obligations of the Republic of the Marshall Islands under international human rights law.

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

PART I - PRELIMINARY

§1. Short title.

This Chapter may be cited as the Cybercrimes Act 2025.

§2. Interpretation.

In this Chapter, unless context otherwise requires:

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

(b) 'child' shall mean any person who is below 18 years of age;

(c) 'child pornography' means any visual depiction of sexually explicit conduct, where:

(i) the production of such visual depiction involves the use of a child engaging in sexually explicit conduct;

(ii) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a child engaging in sexually explicit conduct; or

(iii) such visual depiction has been created, adapted, or modified by any means to appear that an identifiable child is engaging in sexually explicit conduct.

(d) '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;

(e) 'computer data storage medium' means an apparatus or object from which electronic information is capable of being reproduced, with or without the aid of a computer;

(f) '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;

(g) '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;

(h) '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;

(i) 'control' means the ability to manage, command or direct a computer system or computer data;

(j) 'corporation' includes:

(i) domestic and foreign corporations subject to the Business Corporations Act;

(ii) domestic and foreign limited liability company subject to the Limited Liability Company Act of 1996;

(iii) domestic and foreign non-profit entities subject to the Non-Profit Entities Act of 2020;

(iv) state-owned enterprises subject to the State-Owned Enterprises Act of 2015; and

(v) unincorporated associations and any other legal persons subject to the laws of the Republic.

(k) 'critical information infrastructure' has the meaning established in the Cybersecurity Act of 2025;

(l) 'electronic communication' means the transfer of a sign, signal, or computer data of any nature, transmitted in whole or in part by an electrical, digital, magnetic, electromagnetic, optical, wire, wireless, radio, photo electronic or photo optical system or any other similar form;

(m) 'function' includes logic, control, arithmetic, deletion, storage and retrieval and communication to, from or within a computer system;

(n) 'foreign country' means:

(i) any country other than the Republic; and

(ii) every constituent part of such country, including a territory, dependency or protectorate, or political subdivision which administers its own laws relating to international cooperation;

(o) 'government prosecutor' means the Attorney-General or other officer designated by the Attorney-General;

(p) 'identifiable child' means a person:

(i) who was a child at the time the visual depiction was created, adapted, or modified; or

(ii) whose image as a child was used in creating, adapting, or modifying the visual depiction; or

(iii) who is recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic.

The term 'identifiable child' shall not be construed to require proof of the actual identity of the child;

(q) 'judge' means any official authorized to issue a warrant under law;

(r) 'police officer' means a member of the Republic's Department of Public Safety;

(s) 'pornography' or 'pornographic material' means any visual depiction of a person engaged in sexually explicit conduct;

(t) 'producing' means producing, directing, manufacturing, issuing, publishing, or advertising;

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

(v) 'service provider' means:

(i) any public or private entity that provides users of its service the ability to communicate by means of a computer system; or

(ii) any other entity that processes or stores computer data on behalf of the entity or users of such service provided by the entity;

(w) 'sexually explicit conduct' means actual or simulated:

(i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;

(ii) bestiality;

(iii) masturbation;

(iv) sadistic or masochistic abuse; or

(v) lascivious exhibition of the anus, genitals, or pubic area of any person;

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

(y) 'visual depiction' includes:

(i) any photograph, film, video, picture, digital image, computer image, or computer-generated image, whether made or produced by electronic, mechanical, or other means;

(ii) undeveloped film and video;

(iii) data stored on a computer system or computer which is capable of conversion into a visual image, and

(iv) data which is capable of conversion into a visual image that has been transmitted by any means, including a computer system, whether or not stored in a permanent format.

§3. Applicability.

(1) A person may be convicted for an offense committed under this Chapter if:

(a) any of the applicability conditions set forth under section 1.03 of the Criminal Code, 2011 are met; or

(b) the computer, computer system, or computer data affected or which was to be affected by the conduct which constitutes an offence under this Chapter, was at the material time lawfully accessible in the Republic; or

(c) the conduct constituting an offense under this Chapter occurs outside the Republic and the result of that conduct occurs within the Republic; or

(d) the conduct constituting an offense under this Chapter occurs within the Republic and the result of that conduct occurs outside the Republic.

(2) The provisions of this Chapter are in addition to and not in derogation of the Criminal Code, 2011, and where there are any inconsistencies between the provisions of this Act and the Criminal Code, 2011, the provisions of this Chapter shall apply.

PART II – OFFENSES AGAINST THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF COMPUTER DATA AND COMPUTER SYSTEMS

§4. Unauthorized access to a computer system.

(1) A person commits a felony of the second degree if the person intentionally causes, or attempts or conspires to cause, a computer system to perform a function or series of functions to secure access to the computer system and knows that the access the person intends to secure is unauthorized.

(2) The conduct described in subsection (1) is a felony of the first degree if it involves access to a critical information infrastructure or a computer system that is interconnected to or communicates with critical information infrastructure.

(3) Access by a person to a computer system or computer data shall be unauthorized where the person:

(a) is not entitled to have control or access of the kind in question; and

(b) is not authorized to access of the kind in question by any person who is so entitled.

(4) It is immaterial that the unauthorized access is not directed at:

(a) any particular computer data; or

(b) computer data held in any particular computer system.

(5) Access by a person to a computer system or computer shall be deemed lawfully authorized if the person is permitted or required by a court of law or under any other law to obtain information or take possession of any document or thing.

§5. Unauthorized interception of computer data.

(1) A person commits a felony of the second degree if the person intentionally and without authorization intercepts or causes to be intercepted, or attempts or conspires to intercept or cause to be intercepted, directly or indirectly, any computer data.

(2) The conduct described in subsection (1) is a felony of the first degree if it involves computer data related to the operation of critical information infrastructure.

(3) In this section, an act of interception of any computer data to, from or within a computer system, includes listening to, recording or acquiring the substance, meaning or purpose of the computer data.

(4) It is immaterial that the unauthorized access is not directed at:

(a) any particular computer data; or

(b) computer data held in any particular computer system.

(5) An interception under subsection (1) is deemed to be authorized if the person:

(a) has the express consent of the person who sent the computer data or the intended recipient of the computer data; or

(b) is permitted or required by a court or under any other law to obtain information or take possession of any document or thing.

§6. Unauthorized interference in relation to computer data or computer systems.

(1) A person commits a felony of the second degree if the person intentionally performs, or attempts or conspires to perform, any unauthorized act of interference in relation to computer data or a computer system intended to, permanently or temporarily:

(a) hinder the functioning of any computer system;

(b) prevent or impair access to any computer data held in any computer system; or

(c) impair the operation or the reliability of any such computer data.

(2) The conduct described in subsection (1) is a felony of the first degree if it involves interference in relation to computer data or a computer system designated as critical information infrastructure or a computer system that is interconnected to or communicates with critical information infrastructure.

(3) In this section:

(a) an act to hinder the operation of a computer system, includes intentionally:

(i) cutting the electricity supply to a computer system;

(ii) corrupting, damaging, or deteriorating a computer system by any means; or

(iii) impairing, by any means, the connectivity, infrastructure, or support of a computer system;

(b) an act to impair the operation or reliability of computer data, includes intentionally damaging, deleting, deteriorating, altering, or suppressing computer data.

(4) It is immaterial whether or not the unauthorized act is directed at:

(a) any particular computer data or computer system; or

(b) computer data held in any particular computer system.

(5) An act of interference performed in relation to computer data or a computer system is unauthorized if the person performing the act or causing it to be done:

(a) does not have responsibility for the computer data or computer system;

(b) is not entitled to determine whether the act may be performed; and

(c) is not authorized to perform the act by any person who is so entitled.

§7. Unlawful supply or possession of computer system, computer, computer data or computer program.

(1) A person commits a felony of the second degree if the person knowingly manufactures, sells, procures for use, imports, distributes, or otherwise makes available, or attempts or conspires to perform such acts, a computer system, a computer, computer data, or a computer program designed or adapted primarily for the purpose of committing an offense under this Chapter.

(2) A person commits a felony of the second degree if the person knowingly is in possession of, or attempts or conspires to be in possession of, any computer data or computer program, or a computer system or a computer designed or adapted primarily for the purpose of committing an offense under this Act with the intention that it be used by the person or another person to commit or facilitate the commission of an offense under this Chapter.

(3) For the purpose of subsection (2), possession includes:

(a) possession of a computer system or computer that holds or contains the computer data;

(b) possession of a document in which the computer data is recorded; or

(c) having control of computer data that is in the possession of another person.

PART III - COMPUTER-RELATED OFFENCES

§8. Computer-related forgery.

(1) A person commits a felony of the second degree if the person intentionally and without authorization inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data, regardless of

whether or not the data is directly readable and intelligible, to obtain a gain for the person or another person, or causing loss to another person or exposing another person to risk of loss.

(2) The conduct described in subsection (1) is a felony of the first degree if it involves computer data related to the operation of critical information infrastructure.

§9. Computer-related extortion and fraud.

(1) A person commits a felony of the second degree if the person intentionally and without authorization performs or threatens to perform any act described under this Chapter for the purpose of procuring an economic benefit, for the person or another person, or causing loss to another person or exposing another person to risk of loss, including by undertaking to cease or desist from the act, or by undertaking to restore any damage caused as a result of the act.

(2) The conduct described in subsection (1) is a felony of the first degree if it involves or affects a computer system or computer data related to the operation of critical information infrastructure.

PART IV - CONTENT-RELATED OFFENCES

§10. Possession, access, reproduction, distribution, solicitation, and facilitation of child pornography.

(1) A person commits a felony of the first degree if the person knowingly possesses, or knowingly accesses with intent to view, child pornography by any means, including a computer system or a computer.

(2) A person commits a felony of the first degree if the person knowingly:

(a) reproduces, sells, gives away, distributes, electronically transmits, displays, purchases, or possesses with intent to sell, give away, distribute, transmit, or display child pornography by any means, including by a computer system; or

(b) commands, requests, or otherwise attempts to persuade another person to send, submit, transfer, or provide to the person, child pornography by any means, including by a computer system, in order to gain entry into a group,

association, or assembly of persons engaged in trading or sharing child pornography.

(3) All child pornography shall be subject to lawful seizure and forfeiture in accordance with the law.

(4) For purposes of this section, it may be inferred by text, title, or appearance that a person who is depicted as or presents the appearance of being less than 18 years of age in pornographic material, is less than 18 years of age.

(5) The provisions of this section shall not apply to any child pornography that is possessed for a bona fide medical, governmental, law-enforcement, or judicial purpose by a physician, psychologist, attorney, employee of the department of social services, employee of a law-enforcement agency, judge, or clerk and such person possesses such material in the course of conducting the person's professional or official duties.

(6) It shall be a defense to a charge of violating subsection (1) if the person:

(a) possessed less than three matters containing any visual depiction proscribed by subsection (1); and

(b) promptly and in good faith, and without retaining or allowing any person, other than a law enforcement agency, to access any visual depiction proscribed by subsection (1) or copy thereof:

(i) took reasonable steps to destroy each such visual depiction; or

(ii) reported the matter to a law enforcement agency and afforded that agency access to each such visual depiction.

(7) It shall be a defense to a charge of violating subsection (2) if the alleged child pornography was produced using an actual person or persons engaging in sexually explicit conduct and each such person or persons was not a child at the time the material was produced.

§10A. Relationship with Other Laws.

(1) The provisions of this Part are in addition to and not in derogation of the Criminal Code Act, 2011.

(2) Notwithstanding subsection (1), in respect of offences relating to child pornography, the provisions of this Part shall be applied in a manner consistent with the Child Rights Protection Act, 2025.

(3) Where there is any inconsistency between the provisions of this Part and the Child Rights Protections Act, 2015, the Child Rights Protection Act, 2015 shall prevail.

§11. Production of child pornography

(1) A person commits a felony of the first degree if the person intentionally, through any means, including a computer system:

(a) accosts, entices, or solicits a child with intent to induce or force such child to perform in or be a subject of child pornography;

(b) produces or makes, or attempts or prepares to produce or make child pornography;

(c) takes part in or participates in the filming, photographing, or in any other act of production of child pornography by any means; or

(d) finances, or attempts or prepares to finance child pornography.

(2) For the purposes of this section, it may be inferred by text, title, or appearance that a person who is depicted as or presents the appearance of being less than 18 years of age in pornographic material, is less than 18 years of age.

(3) It shall be a defense to a charge of violating subsection (1) if the alleged child pornography was produced using an actual person or persons engaging in sexually explicit conduct; and each such person or persons was an adult at the time the material was produced.

§12. Corruption of children.

A person commits a felony of the first degree if the person knowingly distributes, offers, transmits, sends, or provides to a child by any means, including a computer system, child pornography for purposes of inducing or persuading a child to participate in any activity that is illegal.

§13. Nonconsensual sharing of intimate imagery.

(1) A person commits a misdemeanor if the person intentionally, by any means, including a computer system or a computer, disseminates, transmits, distributes, publishes, sells, or otherwise makes available:

(a) an image that depicts another person 18 years or older engaged in a sexual act, or of the intimate parts of that person, in whole or in part; and

(b) the person depicted is identifiable from the image itself or from information displayed in connection with the image; and

(c) the image was made, captured, recorded, or obtained under circumstances in which a reasonable person would know, expect, or understand that the image was to remain private; and

(d) the image was disseminated, transmitted, distributed, published, sold or otherwise made available without the consent of the depicted person; and

(e) with knowledge or with reckless disregard for the likelihood that the depicted person will suffer harm, or with the intent to harass, intimidate, threaten, extort, or coerce the depicted person.

(2) This section does not apply to the following acts:

(a) the reporting of unlawful conduct;

(b) dissemination or publication of an intimate image made during lawful and common practices of law enforcement, legal proceedings, or medical treatment;

(c) images involving voluntary exposure in a public or commercial setting; or

(d) dissemination or publication of an intimate image made for a legitimate public purpose.

(3) For the purpose of this section, the following terms have the following meanings:

(a) 'identifiable' means the ability to ascertain the identity of an individual;

(b) 'image' includes a photograph, film, video, digital recording or other depiction or portrayal of an object, including a human body, including an image created or altered by digitization;

(c) 'intimate parts' means the naked genitals, pubic area, anus, or female nipple of the person; and

(d) 'sexual act' means sexual intercourse including genital, anal or oral sex.

(e) 'digitization' means to alter an image in a realistic manner utilizing an image or images of a person, other than the person depicted, or computer-generated images.

PART V – PROCEDURAL MEASURES FOR CYBERCRIMES

§14. General procedural powers.

(1) All powers and procedures under this Chapter are applicable to, and may be exercised with respect to any:

(a) criminal offense established in this Act;

(b) other criminal offenses committed by means of a computer system established under any other law; and

(c) the collection of evidence in electronic form of a criminal offense under this Chapter or any other law.

§15. Admissibility of evidence.

(1) In any proceedings related to any offense under law, the fact that evidence has been generated, transmitted, or seized from, or identified in a search of a computer system must not of itself prevent that evidence from being presented, relied on, or admitted.

(2) The powers and procedures provided under this Chapter are without prejudice to the operation of, or powers granted under law, when exercised lawfully by a police officer or government prosecutor, or any regulatory authority.

§16. Expedited preservation of stored computer data.

(1) A police officer or government prosecutor may issue a written notice to a person to preserve and maintain for integrity specified computer data stored by means of a computer system or computer data storage medium if the police officer or government prosecutor is satisfied that:

(a) the specified computer data is reasonably required for the purpose of a criminal investigation;

(b) the specified computer data is particularly vulnerable to loss or modification; and

(c) there is a reasonable risk that the specified computer data may be modified, lost, destroyed, or rendered inaccessible.

(2) The police officer or government prosecutor may serve the written notice on any person who is in possession or control of the computer system, computer program, computer data, computer data storage medium, or computer, requiring the person to expeditiously preserve the specified computer data.

(3) The written notice must specify a maximum period of 90 days for which the specified computer data is to be preserved and maintained for integrity. This period may be renewed once, for an additional period of up to 90 days.

(4) A person who is served a written notice must keep the notice and all its particulars confidential, unless expressly permitted to disclose the matter by the police officer or government prosecutor.

(5) A person commits a felony in the third degree if the person intentionally contravenes or in any manner fails to fully comply with a written notice served under this section.

§17. Expedited preservation and partial disclosure of traffic data.

(1) A police officer or government prosecutor may, by written order given to the service provider in possession or control of the computer system or computer data storage medium, require the service provider to:

(a) undertake expeditious preservation and maintenance of integrity of the specified traffic data for a period specified in the notice not exceeding 90 days, regardless of whether one or more service providers were involved in the transmission of that electronic communication; and

(b) disclose sufficient traffic data about any electronic communication to identify the service provider and the path through which the electronic communication was transmitted.

(2) An order in accordance with subsection (1) may be issued if a police officer or government prosecutor is satisfied that:

(a) any specified traffic data stored in a computer system or computer data storage medium, or by means of a computer system in the possession of, or controlled by, one or more service providers, is reasonably required for the purposes of a criminal investigation;

(b) the specified traffic data is particularly vulnerable to loss or modification; and

(c) there is a reasonable risk that the specified traffic data may be modified, lost, destroyed, or rendered inaccessible.

(3) The period of preservation and maintenance of integrity in accordance with subsection (1) may be extended for an additional period not exceeding 90 days if, on an affidavit presented by the police officer or government prosecutor to a judge, the judge is satisfied that:

(a) an extension of the period of preservation is reasonably required for the purpose of a criminal investigation or prosecution;

(b) there is a risk that the specified traffic data may be modified, lost, destroyed, or rendered inaccessible; and

(c) the cost of such preservation is not overly burdensome on the service provider in possession or control of the computer system or computer data storage medium.

(4) A service provider who is served a notice under this section must keep the notice and all its particulars confidential, unless expressly permitted otherwise by the police officer or government prosecutor or the judge.

(5) A service provider under subsection (4) must:

(a) respond expeditiously to requests for assistance; and

(b) disclose, as soon as practicable, a sufficient amount of traffic data to enable a police officer or government prosecutor to identify any other service provider involved in the transmission of the electronic communication.

(6) A person commits a felony in the third degree if the person intentionally contravenes or in any manner fails to fully comply with the obligations set forth in a written order served under this section.

§18. Production order.

(1) If a police officer or government prosecutor presents an affidavit in support of a warrant demonstrating to the satisfaction of a judge that there are reasonable grounds to believe that the disclosure of specified computer data or specified subscriber information is required for the purposes of a specific criminal investigation, the judge may order:

(a) a person in the Republic to submit the specified computer data in that person's possession or control, which is stored in a computer system or computer data storage medium; or

(b) a service provider offering its services in the Republic to submit subscriber information relating to such services in that service provider's possession or control.

(2) In this section, "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic data or content data.

(3) The judge may require that the recipient of the order and any person in possession or control of the computer system keep confidential the existence of the order or warrant and exercise of power under this section.

(4) A person commits a felony in the third degree if the person intentionally contravenes or in any manner fails to fully comply with the obligations set forth in a written order or warrant served under this section.

§19. Search and seizure of stored computer data and other things.

(1) A police officer or government prosecutor may present an affidavit in support of a warrant to demonstrate that there exist reasonable grounds to believe that there may be a specified computer system, computer data, or computer that:

(a) is reasonably required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence in proving a specifically identified offense; or

(b) has been acquired by a person as a result of the commission of an offense,

(2) Upon review of an affidavit presented in accordance with subsection (1), if the judge is satisfied that there exist reasonable grounds to support a warrant, the judge may issue such warrant authorizing a police officer or government prosecutor, with such assistance as may be necessary to:

(a) seize or similarly secure the specified computer system, program, data, or computer;

(b) make and retain copies of the specified computer system, program, or data;

(c) maintain the integrity of the relevant stored data;

(d) render inaccessible or remove the data in the specified computer system;

(e) inspect and assess the operation of any computer system to which the warrant issued under this section applies;

(f) require any person, other than the suspect, possessing knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary computer data, to enable the police officer or government prosecutor to conduct such activities as authorized under this section;

(g) require any person, other than the suspect, in possession of decryption information to grant him or her access to such decryption information necessary to decrypt data required for the purpose of the warrant issued under this section; and/or

(h) provide the police officer or government prosecutor with such reasonable technical and other assistance as the police officer or government prosecutor may require for the purposes of the warrant issued under this section.

(3) Where a police officer or government prosecutor is permitted to search or similarly access a specified computer system or computer data storage medium, under subsection (2), and has grounds to believe that the computer data sought is stored in another computer system or computer data storage medium, and such computer data is lawfully accessible from or available to the initial computer system or computer data storage medium, the police officer or government prosecutor may extend the search or similar access to such other computer system or computer data storage medium .

(4) Seized computer data may be used only for lawful purposes for which it was originally obtained, or to enforce the law.

(5) The police officer or government prosecutor must:

(a) only seize a computer system or computer data storage medium under subsection (1) when:

(i) it is not practical to seize or secure the computer data; or

(i) it is necessary to ensure that computer data will not be modified, lost, destroyed, rendered inaccessible, or otherwise interfered with; and

(b) exercise reasonable care while the computer system or computer data storage medium is retained.

(6) A person commits a felony in the third degree if the person intentionally obstructs the lawful exercise of the powers under this section or misuses the powers granted under this section.

(7) In this section:

(a) 'decryption information' means information or technology that enables a person to readily unscramble encrypted data into an intelligible format; and

(b) 'encrypted data' means data which has been transformed from its plain text or readable version to an unintelligible format, regardless of the technique utilized for such transformation and irrespective of the medium in which such data occurs or can be found for the purposes of protecting the content of such data.

§20. Real-time collection of traffic data.

(1) If a police officer or government prosecutor presents an affidavit in support of a warrant demonstrating to the satisfaction of a judge that there are reasonable grounds to believe that traffic data associated with specified electronic communications, and related to or connected with a person under investigation, is required for the purposes of a specific criminal investigation or prosecution, a judge may issue a warrant:

(a) to allow a law enforcement officer to collect or record traffic data in real-time by technical means;

(b) requiring a service provider to with existing technical capability to:

(i) collect or record traffic data in real-time; and

(ii) provide only the traffic data to the police officer or government prosecutor.

(2) Real-time collection or recording of traffic data must be limited in time and may not be ordered for a period exceeding 90 days. This period may be extended by the judge upon application for a further specified period of time, not exceeding an additional 90 days.

(3) When issuing a warrant under subsection (1), the judge must be satisfied that:

(a) the extent of interception is adequate, proportionate, and necessary for the purposes of a specific criminal investigation or prosecution;

(b) measures are taken to ensure that, as the traffic data is intercepted, the privacy of other users, customers and third parties is maintained and data of any party not part of the investigation is not disclosed; and

(c) the investigation may be frustrated or seriously prejudiced unless the interception is permitted.

(4) A judge must require the service provider to keep confidential the warrant and execution of any power provided for under this section.

(5) A service provider commits a felony in the third degree if the service provider intentionally contravenes or in any manner, including by an act or omission, fails to fully comply with the obligations set forth in a written order or warrant served under this section.

§21. Interception of content data of electronic communications.

(1) If a police officer or government prosecutor presents an affidavit in support of a warrant demonstrating to the satisfaction of a judge that there are reasonable grounds to authorize the interception of content data and associated traffic data of specified electronic communications, related to or connected with a person or premises under criminal investigation or to give effect to a mutual assistance request, the judge may issue a warrant:

(a) to allow a law enforcement officer to collect or record content data of specified electronic communications in real-time by technical means;

(b) requiring a service provider with existing technical capability to:

(i) collect or record content data of specified electronic communications in real-time; and

(ii) provide that content data and associated traffic data to the police officer or government prosecutor as soon as reasonably practicable.

(2) Real-time collection or recording of content data and associated traffic data must be limited in time and may not be ordered for a period exceeding 90 days. This period may be extended by the judge upon application for a further specified period of time, not exceeding an additional 90 days.

(3) When issuing a warrant under subsection (1), the judge must be satisfied that:

(a) the extent of interception is adequate, proportionate, and necessary for the purposes of a specific criminal investigation or prosecution;

(b) measures are taken to ensure that, as the content data is intercepted, the privacy of other users, customers and third parties is maintained and data of any party not part of the investigation is not disclosed; and

(c) the investigation may be frustrated or seriously prejudiced unless the interception is permitted.

(4) A judge must require the service provider to keep confidential the warrant and execution of any power provided for under this section.

(5) A service provider commits a felony in the third degree if the service provider intentionally contravenes or in any manner, including by an act or omission, fails to fully comply with the obligations set forth in a written order or warrant served under this section.

PART VI – INTERNATIONAL COOPERATION ON CYBERCRIMES

§22. General principles relating to international cooperation.

(1) This Part applies in addition to, and not in derogation from, the Criminal Extradition Act (32 MIRC Ch. 2) and the Mutual Assistance in Criminal Matters Act (32 MIRC Ch. 4).

(2) The Attorney General may make a request for mutual legal assistance in any criminal matter to the appropriate authority of a foreign country for the purpose of:

(a) undertaking investigations or proceedings concerning offenses related to computer systems, electronic communications, or computer data;

(b) collecting evidence in electronic form of any offense established under law, including offenses under this Chapter; or

(c) obtaining expeditious preservation and disclosure of computer data, including traffic data, real-time collection of traffic data associated with specified electronic communications or interception of computer data or any other means, power, function, or provisions under this Chapter.

(3) For any of the purposes listed in subsection (2), a requesting foreign country may make a request for mutual legal assistance to the Attorney General in any crininal matter.

(4) The Attorney General may require a foreign country making a request in accordance with subsection (3) to:

(a) keep the contents, computer data, and materials provided in a confidential manner;

(b) only use the contents, computer data, and materials provided for the purpose of the criminal matter specified in the request; and

(c) use the contents, computer data, and materials subject to such conditions as may be specified.

(5) If the requesting foreign country cannot comply with requirements made under subsection (4), it shall notify the Attorney General accordingly, which shall then determine whether the computer data should nevertheless be provided.

(6) Where the foreign country accepts the computer data, it must comply with the conditions specified by the Attorney General.

§23. Spontaneous information.

(1) The Attorney General may, without prior request, forward to a foreign country any computer data lawfully obtained during an investigation

undertaken within the Republic when it considers that the disclosure of such computer data may:

(a) assist the foreign country in initiating or carrying out investigations or proceedings; or

(b) lead to a request for cooperation by the foreign country under this Chapter.

(2) Prior to providing computer data under subsection (1), the Attorney General may request that the computer data be kept confidential or disclosed only subject to such conditions as may be specified by the Attorney General.

(3) If the foreign country is unable to comply with such conditions specified under subsection (2), it must promptly notify the Attorney General. The Attorney General must then determine whether the computer data may still be provided.

§24. Expedited preservation of stored computer data.

(1) A foreign country may submit to the Attorney General or the 24/7 network a request for mutual legal assistance for the search, seizure, access to, securing of, or disclosure of computer data and to obtain the expeditious preservation of such computer data stored by means of a computer system located within the territory of the Republic.

(2) A request for preservation made under subsection (1) must specify:

(a) the authority seeking the preservation;

(b) the offense that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

(c) the stored computer data to be preserved and its relationship to the offense;

(d) any available information identifying the custodian of the stored computer data or the location of the computer system;

(e) the necessity of the preservation; and

(f) the intention to submit a request for mutual legal assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

(3) Upon receiving the request under subsection (1), the Attorney General or the 24/7 network must take appropriate measures to preserve the

specified data in accordance with the procedures and powers provided under this Chapter.

(4) Any preservation effected in response to the request referred to under this section must be for a period not exceeding 120 days, in order to enable the foreign country to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data and following the receipt of such a request.

(5) The data must continue to be preserved until a final decision is made on the request made under subsection (4).

(6) Notwithstanding the requirement set forth in subsection (3), a request under subsection (1) may be refused if the Attorney General considers that the execution of the request is likely to prejudice the sovereignty, security, public order, or public interest of the Republic.

§25. Expedited preservation of stored computer data.

(1) Where, during the course of executing a request under section 24 with respect to a specified electronic communication, the investigating agency discovers that a service provider in another country was involved in the transmission of the electronic communication, the Attorney General or the 24/7 network must expeditiously disclose to the requesting foreign country a sufficient amount of traffic data to identify that service provider and the path through which the electronic communication was transmitted.

(2) Disclosure of traffic data under subsection (1) may be withheld if the Attorney General considers that such disclosure is likely to prejudice the sovereignty, security, public order, or public interest of the Republic.

§26. Mutual assistance regarding access to stored computer data.

(1) A foreign country may request the Attorney General to search or similarly access, seize, or similarly secure and disclose computer data stored by means of a computer system or computer located within the Republic, including computer data that has been preserved in accordance with section 24.

(2) A request under subsection (1) must, as far as practicable, specify:

(a) the name of the authority conducting the investigation or proceedings to which the request relates;

(b) describe the nature of the criminal matter and a statement setting out a summary of the relevant facts and laws;

(c) describe the purpose of the request and the nature of the assistance being sought;

(d) in the case of a request to seize property, computer system or computer believed, on reasonable grounds, to be located in the Republic, give details of the offense, particulars of any investigation or proceedings commenced in respect of the offense, and be accompanied by a copy of any relevant warrant or seizure order issued in the foreign country;

(e) details of any procedure that the foreign country wishes to be followed by the Republic in giving effect to the request, particularly in the case of a request to take evidence;

(f) a statement setting out any demands of the requesting foreign country concerning any confidentiality relating to the request and the reasons for those demands;

(g) details of the period within which the requesting foreign country wishes the request to be complied with;

(h) details, where applicable, of the property, computer system or computer to be seized, and of the grounds for believing that the property, computer system or computer is the Republic;

(i) details of the stored computer data to be seized and its relationship to the offense;

(j) any available information that may identify the custodian of the stored computer data or the location of the property, computer system or computer;

(k) agreement on the question of the payment of the damages or costs of fulfilling the request; and

(l) any other information that may assist in giving effect to the request.

(3) Upon receiving the request under subsection (1), and provided the Attorney General is satisfied that the requirements set forth in section 19(1) are present, the Attorney General must take appropriate measures to obtain the necessary authorization, including any

warrants, to execute the request in accordance with this Chapter and any other relevant law.

(4) Where the Attorney General obtains the necessary authorization in accordance with subsection (3), including any warrants, to execute the request, the Attorney General may seek the support and cooperation of the requesting foreign country during such search and seizure.

(5) For the purpose of conducting the search and seizure request, the Attorney General must provide to the requesting foreign country, the results of the search and seizure and the electronic or physical evidence seized.

§27. Transborder access to stored computer data with consent or where publicly available.

(1) A police officer or government prosecutor may, subject to this Chapter:

(a) access publicly available stored computer data, regardless of where the data is located geographically; or

(b) access or receive, through a computer system in the Republic, stored computer data located in another country, if a police officer or government prosecutor obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data through that computer system.

§28. Mutual assistance in real-time collection of traffic data.

(1) A foreign country may request the Attorney General to provide assistance in real-time collection of traffic data associated with specified electronic communications in the Republic, transmitted by means of a computer system.

(2) A request under subsection (1) must, as far as practicable, specify:

(a) the authority seeking the use of powers under this section;

(b) the offense that is the subject of a criminal investigation or proceeding and a brief summary of the related facts;

(c) the name of the service provider which has access to the relevant traffic data;

(d) the location at which the traffic data may be held;

(e) the intended purpose of requiring the traffic data;

(f) such information as may be required to identify the traffic data;

(g) any further details relevant to the traffic data;

(h) the reason for using powers under this section;

(i) the terms and conditions for the use and disclosure of the traffic data to third parties; and

(j) any other information that may assist in giving effect to the request.

(3) Upon receiving the request under subsection (1), and provided the Attorney General is satisfied that the requirements set forth in section 20(1) are fulfilled, the Attorney General must take appropriate measures to obtain the necessary authorization, including any warrants, to execute the request in accordance with this Chapter and any other relevant law.

(4) Where the Attorney General obtains the necessary authorization in accordance with subsection (3), including any warrants, to execute the request, the Attorney General may seek the support and cooperation of the requesting foreign country during the collection.

(5) The Attorney General must, upon conducting the measures under this section, provide the results of such measures and real-time collection of traffic data associated with specified communications to the requesting foreign country.

§29. Mutual assistance regarding interception of content data.

(1) A foreign country may request the Attorney General to provide assistance in the real-time collection or recording of content data of specified electronic communications in the Republic transmitted by means of a computer system.

(2) A request under subsection (1) must, as far as practicable, specify:

(a) the authority seeking the use of powers under this section;

(b) the offense that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

(c) the name of the service provider with access to the relevant communication;

(d) the nature of the communication;

(e) the intended purpose for the required communication;

(f) sufficient information to identify the communication;

(g) details of the data of the relevant interception;

(h) the recipient of the communication;

(i) the intended duration of the interception;

(j) the reason for using powers under this section;

(k) the terms and conditions of the use and disclosure of the communication to third parties; and

(l) any other information that may assist in giving effect to the request.

(3) Upon receiving the request under subsection (1), and provided the Attorney General is satisfied that the requirements set forth in section 21(1) are fulfilled, the Attorney General must take appropriate measures to obtain the necessary authorization, including any warrants, to execute the request in accordance with this Chapter and any other relevant law.

(4) Where the Attorney General obtains the necessary authorization in accordance with subsection (3), including any warrants, to execute the request, the Attorney General may seek the support and cooperation of the requesting foreign country during the interception.

(5) The Attorney General must, upon conducting the measures under this section, provide the results of such measures and real-time collection or recording of content data of specified communications to the requesting foreign country.

§30. 24/7 network.

(1) The Attorney General must designate a point of contact available on a twenty-four-hour, seven-days-a-week basis (referred to as the 24/7 network) in order to provide immediate assistance for the purpose of investigations or proceedings concerning criminal offenses related to computer systems and computer data, or for the collection of evidence in electronic form of a criminal offense.

(2) Within expeditious timelines to be defined by regulations under this Chapter, such assistance includes the following measures:

(a) providing technical advice;

(b) preserving data pursuant to section 24 and section 25; or

(c) collecting evidence, the provision of legal information, and locating suspects,

(3) The point of contact has the authority and is empowered to coordinate and enable access, on an expedited basis, to international mutual assistance under this Chapter or extradition procedures, if applicable.

§31. Protection of personal data.

(1) The Attorney General shall only transfer personal data under this Chapter in a manner that is compliant with applicable personal data protection principles and obligations under law.

(2) Where the Attorney General is satisfied that a transfer of personal data under this Chapter would not comply with subsection (1), the Attorney General shall condition the transfer of personal data to such safeguards as the Attorney General may deem necessary to ensure compliance with applicable personal data protection principles and obligations under law.

(3) The Attorney General shall take measures to ensure that personal data received from a foreign country in accordance with this Chapter is subject to appropriate safeguards to comply with applicable personal data protection law.

(4) The Attorney General may transfer personal data obtained in accordance with this Chapter to a third country or an international organization only with the prior authorization of the original transferring foreign country.

(5) For purposes of this section, "personal data" means any information relating to an identified or identifiable natural person that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, whether directly or indirectly, with a particular natural person, including by reference to an identifier, such as name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

PART VII – AMENDMENTS

§32. Consequential Amendment.

(1) Section 250.4 of the Criminal Code is hereby amended with the underlined text as follows:

"§250.4 Harassment.

A person commits a petty misdemeanor if, with intent to harass, annoy, or alarm another, the person:

(1) repeatedly makes a telephone call, facsimile, ~~or~~ electronic mail transmission, or any other contact via electronic communications without purpose of legitimate communication; or

(2) insults, taunts, or challenges another in a manner reasonably likely to provoke immediate violent or disorderly response; or

(3) makes repeated communications, including electronic communications, anonymously or at extremely inconvenient hours; or

(4) subjects another to an offensive and unwanted touching; or

(5) repeatedly makes communications, including electronic communications, after being advised by the person to whom the communication is directed that further communication is unwelcome; or

(6) makes a communication, including electronic communications, using offensively coarse language that would cause the recipient to reasonably believe that the actor intends to cause bodily injury to the recipient or another or damage to the property of the recipient or another."

2. *Section 250.5 of the Criminal Code is hereby amended with the underlined text as follows:*

"§250.5 Stalking.

A person is guilty of stalking, a misdemeanor, if the person intentionally engages in a course of conduct that places another person in reasonable fear of the death of, or serious bodily injury to, or causes substantial emotional distress to that person or an immediate family member of that person.

"Course of conduct" means repeatedly establishing and maintaining visual or physical proximity to another person or repeatedly

conveying verbal or written threats or threats implied by conduct directed at or toward another person. A course of conduct may include contact via electronic communications.

"Immediate family" means a spouse, parent, child, sibling, or any other person who regularly resides in the household."

PART VIII – MISCELLANEOUS

§33. Liability of a corporation.

A corporation, as defined in this Chapter, may be convicted of the commission of an offense under this Chapter in accordance with the requirements of section 2.07(1) of the Criminal Code Act, 2011.

§34. Rules, regulations, and policies.

The Attorney General may prescribe such rules and regulations and adopt such policies as the Attorney General may deem necessary to implement the provisions of this Chapter.

§35. Effective date.

This Chapter will take effect on the date of certification in accordance with Article IV, section 21 of the Constitution.

CERTIFICATE

I hereby certify:

1. That Nitijela Bill No: 64ND1 was passed by the Nitijela of the Republic of the Marshall Islands on the 29th day of September 2025; and

2. That I am satisfied that Nitijela Bill No: 64ND1 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 6th day of October 2025.

Hon. Brenson S. Wase
Speaker
Nitijela of the Marshall Islands

Attest:

Morean S. Watak
Clerk
Nitijela of the Marshall Islands