

Cybercrime Bill 2026

№

Contents

1 Title 1
2 Commencement 1

Part 1 — Preliminary matters

3 Interpretation 1
4 Penalties 3
5 Extraterritorial application of Act 3
6 Act binds the Government 4

Part 2 — Cybercrime offences

7 Unauthorised access to computer system or computer data 4
8 Unauthorised interception 4
9 Unauthorised interference with computer data 5
10 Unauthorised hindering of, or preventing access to, computer system 5
11 Unauthorised devices 6
12 Computer-related forgery 6
13 Computer-related fraud 7
14 Computer-related identity crimes 7
15 Parties to offences and attempts 7

Part 3 — Enforcement

16 Service providers must keep details of investigation confidential 8
17 Exceptions to section 16 8
18 Search and seizure 9
19 Assistance 10
20 Production order 11
21 Preservation notice 12
22 Lawful collection and recording of electronic communications 12

23 Forensic tool 13
24 Offence—Refusing or failing to comply with warrant, order, or notice or to assist in executing warrant 14
25 Disclosure of traffic data 15
26 Collection or recording of traffic data 15
27 Offence—Refusing or failing to comply with order under section 25 or 26 16

Part 4 — Liability of bodies corporate and service providers

28 Corporate liability 16
29 Protection of service providers 17

Part 5 — Miscellaneous

30 Immunity from criminal or civil liability 17
31 Annual reporting by Chief of Police 18

Regulations

32 Regulations 19

Related amendments

33 Related amendments to Mutual Assistance in Criminal Matters Act 1998 19

Schedule Related amendments to Mutual Assistance in Criminal Matters Act 1998

A Bill for an Act to—

a. create offences and penalties for criminal activity associated with the use of computer systems and computer data, and provide for related measures, including investigative and enforcement powers; and

b. make related amendments to the Mutual Assistance in Criminal Matters Act 1998.

The Assembly enacts as follows—

1 Title

This is the Cybercrime Act 2026.

2 Commencement

This Act comes into force on the day after the date on which it becomes law in accordance with Article 34 of the Constitution.

Part 1 — Preliminary matters

3 Interpretation

(1) In this Act, unless the context otherwise requires—

authorised, in relation to conduct, means that the conduct is authorised by a person who has lawful authority to authorise it and ***unauthorised*** has a corresponding meaning;

computer data means any representation of facts, information, or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function (whether by wire or wirelessly);

computer system means a device or group of interconnected or related devices that, in accordance with a program, performs automatic processing of data;

device includes a mobile phone;

foreign country means a country other than Niue;

interception—

(a) means intercepting computer data, electromagnetic emissions, or an electronic communication not directed to the person who is intercepting it; and

(b) includes (without limitation) the acquiring, viewing, and capturing of that computer data, electromagnetic emission, or electronic communication whether by wire, wireless, electronic, optical,

magnetic, or other means during transmission through the use of any technical device;

Minister means the Minister responsible for the administration of this Act;

Niue resident means a person ordinarily resident in Niue;

Police officer means a Police officer with the Niue Police Department;

***seize*—**

(a) includes—

(i) making and retaining a copy of computer data that is on a computer system, including using onsite equipment;

(ii) rendering inaccessible or removing a computer system or part of it;

(iii) taking a printout of computer data on a computer system;

(iv) otherwise securing or maintaining the integrity of a computer system or computer data for later examination;

(b) does not include making or generating a record of the exercise of a search or seizure power by the person exercising that power or assisting with the exercise of that power, for example, taking notes, photographs, or recordings;

service provider means—

(a) any public or private entity that provides to users of its services the ability to communicate, share, or display computer data by means of a computer system; or

(b) any other entity that processes or stores computer data for those users or services;

traffic data means computer data that—

(a) relates to a communication by means of a computer system; and

(b) is generated by a computer system that is part of the chain of communication; and

(c) indicates 1 or more of the communication's origin, destination, route, time, date, size, or duration, or the type of underlying service.

unauthorised—*see* definition of 'authorised' in this subsection.

(2) Notes in this Act do not form part of the Act.

4 Penalties

(1) A penalty specified at the foot of a provision of this Act indicates that an offence mentioned in the provision is punishable on conviction by a penalty not exceeding the penalty specified.

(2) A reference in a provision of this Act to a penalty of a specified number of penalty units is a reference to a fine of that number of penalty units.

Note for subsection (2)—'Penalty unit' is defined in section 5 of the Interpretation Act 2004.

(3) If the penalty for an offence is expressed to be both imprisonment and a fine, an individual who is found guilty of the offence may be—

(a) fined or imprisoned; or

(b) fined and imprisoned.

(4) If a provision prescribes a fine for an offence—

(a) the fine is the fine for an individual; and

(b) if a body corporate is found guilty of the offence, the court may impose a fine of an amount equal to 5 times the fine for an individual.

5 Extraterritorial application of Act

(1) This Act applies to an act done or an omission made—

(a) by any person within Niue; or

(b) outside Niue, by any person on a ship or aircraft registered in or operating under the laws of Niue; or

(c) except as provided in paragraphs (b) or (d), by a Niue resident outside Niue if—

(i) the person's conduct would also be an offence under a law of the country where the conduct occurs; or

(ii) if the person is outside the jurisdiction of any country; or

(d) by any person outside Niue, if it has a detrimental effect on—

(i) the security of Niue or its nationals; or

(ii) any property or any computer system or computer data located in Niue.

(2) To avoid doubt—

(a) subsection (1)(a) applies to any person present in Niue whether or not they are a Niue resident, unless, in the case of a person who is not a Niue resident, they are extradited to another country for the purposes of criminal proceedings in relation to the acts connected with the alleged offending in Niue; and

(b) subsections (1)(b) and (d) apply to any person whether or not they are a Niue resident; and

(c) this section applies to bodies corporate as well as individuals.

6 Act binds the Government

This Act binds the Government.

Part 2 — Cybercrime offences

7 Unauthorised access to computer system or computer data

(1) A person commits an offence if they—

(a) gain or attempt to gain unauthorised access to a computer system or computer data; and

(b) know the access is unauthorised or are reckless about whether it is authorised.

Penalty: (i) if the offence involves a circumstance of aggravation—1000 penalty units and 10 years' imprisonment; or

(ii) otherwise—200 penalty units and 2 years' imprisonment.

(2) It is a circumstance of aggravation for this section for a person to commit the offence with fraudulent or dishonest intent of—

(a) procuring an economic benefit for themselves or for another person; or

(b) causing loss to another person.

8 Unauthorised interception

A person commits an offence if—

(a) they intercept by technical means—

(i) any non-public transmission of computer data to, from, or within a computer system; or

(ii) electromagnetic emissions from a computer system carrying computer data; and

(b) the interception is unauthorised; and

(c) they know that the interception is unauthorised or are reckless about whether it is authorised.

Penalty: 500 penalty units and 5 years' imprisonment.

9 Unauthorised interference with computer data

(1) A person commits an offence if—

(a) they interfere with computer data by doing any of the following acts—

(i) damage computer data or take any action that results in it deteriorating;

(ii) delete computer data;

(iii) alter computer data;

(iv) render computer data meaningless, useless, or ineffective;

(v) obstruct, interrupt, or interfere with the lawful use, or a person in the lawful use, of computer data;

(vi) deny access to computer data or to any person authorised to access it; and

(b) the interference is unauthorised; and

(c) they know the interference is unauthorised or are reckless about whether it is authorised; and

(d) the interference results in serious harm.

Penalty: (i) if the offence involves a circumstance of aggravation—1500 penalty units and 14 years' imprisonment; or

(ii) otherwise—500 penalty units and 5 years' imprisonment.

(2) It is a circumstance of aggravation for this section for a person to commit the offence knowing, or reckless about whether, danger to life is likely to result.

(3) In subsection (1)(d), ***serious harm*** means 1 or more of the following—

(a) a financial loss of more than $1000;

(b) a threat to national security;

(c) physical injury or death;

(d) a threat to public health or public safety.

10 Unauthorised hindering of, or preventing access to, computer system

A person commits an offence if they—

(a) take any action that seriously hinders the functioning of a computer system or prevents access to a computer system by any person authorised to access it; and

(b) are not authorised to hinder the functioning of the computer system or prevent access to it; and

(c) know they are not authorised to hinder the functioning of the computer system or prevent access to it or are reckless about whether they are authorised.

Penalty: 500 penalty units and 5 years' imprisonment.

11 Unauthorised devices

(1) A person commits an offence if they—

(a) produce, sell, procure for use, import, export, distribute, or otherwise make available—

(i) a device or tool, including a computer program, that is primarily designed or specifically adapted for the purpose of committing an offence against this Act; or

(ii) a password, access code, or similar data by which the whole or any part of a computer system or computer data is capable of being accessed; and

(b) intend that the device, tool, program, password, access code, or data be used by any person to commit an offence against this Act.

Penalty: 500 penalty units and 5 years' imprisonment.

(2) A person commits an offence if they possess a device, tool, program, password, access code, or data described in subsection (1)(a) with the intent that it be used by any person to commit an offence against this Act.

Penalty: 500 penalty units and 5 years' imprisonment.

12 Computer-related forgery

(1) A person commits an offence if they—

(a) input, alter, delete, or suppress computer data, resulting in inauthentic data; and

(b) do so for wrongful gain and with the intent that the inauthentic data be considered or acted upon for legal purposes as if it were authentic, regardless of whether the data is directly readable or intelligible.

Penalty: (i) if the offence involves a circumstance of aggravation—500 penalty units and 5 years' imprisonment;

(ii) otherwise—300 penalty units and 3 years' imprisonment.

(2) It is a circumstance of aggravation for this section for a person to commit the offence by sending out multiple electronic mail messages from or through computer systems.

(3) This section does not limit or affect section 207 or 208 of the Niue Act 1966 (section 94 or 95 of the Criminal Law Code).

13 Computer-related fraud

(1) A person commits an offence if they—

(a) cause a loss of property to another person by any—

(i) input, alteration, deletion, or suppression of computer data; or

(ii) interference with the functioning of a computer system; and

(b) do so with fraudulent or dishonest intent of procuring an economic benefit for themselves or for another person.

Penalty: 500 penalty units and 5 years' imprisonment.

(2) This section does not limit or affect section 191, 200, 202, 203, 207, 208, or 228A of the Niue Act 1966 (section 77, 86, 88, 89, 94, 95, or 115 of the Criminal Law Code).

14 Computer-related identity crimes

A person commits an offence if they—

(a) transfer, possess, or use a means of identification of another person; and

(b) do so with the intent to commit, or to aid or abet, or in connection with, any activity that is an offence under any law; and

(c) use a computer system for any action that is or is connected with the offence.

Penalty: 500 penalty units and 5 years' imprisonment.

15 Parties to offences and attempts

(1) Subsection (2) applies to a person who aids or abets a person to commit an offence against this Act.

(2) The person commits the same offence and is liable on conviction to the penalty provided for the offence.

(3) A person who attempts to commit or does any act preparatory to or in furtherance of the commission of an offence against this Act commits the same offence and is liable on conviction to the penalty provided for the offence.

(4) For the purposes of subsection (3), it is immaterial whether the substantive offence was actually completed.

Part 3 — Enforcement

16 Service providers must keep details of investigation confidential

(1) This section applies to a service provider that is—

(a) required to take any action or assist under a court order or notice under this Part; or

(b) in or responsible for a place subject to a search and seizure warrant issued under section 18; or

(c) required to permit or assist with search and seizure under section 19; or

(d) ordered or required to permit or assist a Police officer to do anything authorised under this Part; or

(e) subject to any other obligation that applies by operation of law to maintain confidentiality in relation to a criminal investigation.

(2) Except as provided in section 17, the service provider commits an offence if it intentionally discloses any of the following to any person—

(a) the fact that an order has been made, a warrant or notice has been issued, an authorisation or requirement has been given, or the obligation exists;

(b) details of anything done under the order, warrant, notice, authorisation, requirement, or obligation;

(c) details of any electronic communications or computer data obtained under the order, warrant, notice, authorisation, requirement, or obligation.

Penalty: 300 penalty units and 3 years' imprisonment.

(3) In this section, ***service provider*** includes an officer or a person involved in the management of the service provider, or an employee, an agent, or a contractor of the service provider.

17 Exceptions to section 16

(1) This section applies to an order, warrant, notice, authorisation, requirement, or obligation referred to in section 16 (the ***order***).

(2) A service provider may disclose 1 or more of the things listed in section 16(2) relating to the order to the following persons, but only in accordance with this section—

(a) a Police officer, but only for the purpose of the performance of the officer's duties;

(b) an officer or a person involved in the management of the service provider or an employee, an agent, or a contractor of the service provider, but only for the purposes of, and to the extent necessary for, ensuring that the order is complied with;

(c) a lawyer, but only for the purposes of obtaining legal advice or representation in relation to the order.

(3) A Police officer referred to in subsection (2)(a) must not disclose the existence of the order or details of anything done under it to any other person except for the purpose of performing their duties.

(4) A person referred to in subsection (2)(b) must not disclose the existence of the order or details of anything done under it to any other person except a person referred to in subsection (2)(a), (b) or (c), and only for the purposes of, and to the extent necessary for—

(a) assisting a Police officer; or

(b) ensuring that the order is complied with; or

(c) obtaining legal advice or representation in relation to the order.

(5) A lawyer referred to in subsection (2)(c) must not disclose the existence of the order or details of anything done under it to any other person except for the purposes of providing legal advice or representation in relation to it.

(6) A person who is the other person in subsections (3) or (4) must not disclose the existence of the order or details of anything done under it to any other person unless—

(a) subsection (2)(a), (b) or (c) would have applied if the service provider had made the disclosure to them directly; and

(b) they make the disclosure as permitted by subsection (2)(a), (b) or (c).

(7) Nothing in section 16 or this section prevents the disclosure of the existence or operation of an order in connection with, or in the course of, proceedings before a court.

(8) A person who contravenes this section commits an offence.

Penalty: 300 penalty units and 3 years' imprisonment.

18 Search and seizure

(1) If the High Court, on application by a Police officer, is satisfied on the basis of a sworn statement that there are reasonable grounds to suspect that there may be, in a place, a computer system or computer data—

(a) that may be material as evidence in proving an offence against this Act; or

(b) that has been acquired by a person as a result of such an offence,

the court may issue a warrant authorising a Police officer, with such assistance as may be necessary, to enter the place to search for and seize the computer system or parts of it or computer data.

(2) A person who seizes anything under the warrant must, either at the time of seizure or as soon as practicable—

(a) make a list of what has been seized, with the date and time of seizure; and

(b) give a copy of that list to—

(i) the occupier of the premises; or

(ii) the person in control of the computer system or computer data.

(3) Subject to subsection (4), any Police officer may, on request—

(a) permit a person who had the custody or control of the computer system or computer data, or someone acting on their behalf, to access and copy the computer data; or

(b) give the person a copy of the computer data.

(4) The Police officer may refuse to give access or provide a copy if they have reasonable grounds for believing that doing so may—

(a) constitute a criminal offence or assist with the commission of a criminal offence; or

(b) prejudice—

(i) an investigation in connection with which the search was carried out; or

(ii) another ongoing criminal investigation; or

(iii) any criminal proceeding that is pending or that may be brought in relation to any of those investigations.

(5) If the Police officer undertaking a search under the warrant has reasonable grounds to believe that the computer data sought is stored in another computer system in Niue, and that the system is accessible from another place, they may extend the search to the other system in the other place.

19 Assistance

(1) This section applies to a person who—

(a) is not suspected of committing an offence against this Act; but

(b) is in possession or control of a computer system or computer data that is the subject of a search under a warrant issued under section 18.

(2) The person must, at their own cost, permit the Police officer doing the search to do any of the following and, if required, assist the officer to do so—

(a) access or use that computer system or computer data, including by providing passwords or access codes;

(b) obtain or copy the computer data;

(c) use a device to make the copies;

(d) obtain output from a computer system in a usable format.

(3) This section applies to a computer system or computer data to which the person has access whether it belongs to them or to another person. To avoid doubt, this includes a service provider that has access to those things belonging to a person to whom it provides services.

20 Production order

(1) If the High Court, on application by a Police officer, is satisfied on the basis of a sworn statement that specified computer data in a computer system, or the information referred to in paragraph (b), is reasonably required for the purposes of a criminal investigation or a criminal proceeding for an offence against this Act, the court may order (a ***production order***)—

(a) a person in possession or control of the computer system to produce the specified computer data or a copy of it; and

(b) a service provider to provide information about relevant persons who subscribe to or use its services.

(2) If necessary, a Police officer may require the person producing the data or information to reproduce, or to assist any person nominated by the Police officer to reproduce, the data or information in a usable form.

(3) The person receiving the production order must take the steps specified in the order without delay.

(4) A production order is in force for the period specified in the order (which may not exceed 30 days after the date the order is made).

(5) In this section, ***information*** means any information contained in the form of computer data (other than content data) that is held by a service provider and that relates to a subscriber of its services, for example—

(a) the type of service used by the subscriber;

(b) their identity, postal or geographic address, or telephone or other access number;

(c) their billing and payment information;

(d) details of the service agreement or arrangement with them;

(e) information about the site of the installation of any relevant equipment.

21 Preservation notice

(1) This section applies if a Police officer is satisfied that—

(a) computer data stored in a computer system is reasonably required for the purpose of a criminal investigation or a criminal proceeding for an offence against this Act; and

(b) there is a risk that the data may be destroyed, modified, or rendered inaccessible.

(2) The Police officer may, by written notice given to a person in possession or control of the computer system, require the person to ensure that the data specified in the notice is preserved for a period of up to 90 days as specified in the notice.

(3) The High Court may, upon application, authorise an extension of the notice period not exceeding 90 days.

(4) The person receiving the notice must take the steps specified in the notice without delay.

(5) If the data is traffic data, it is immaterial if the data is or may be under the control of more than 1 person or available through more than 1 computer system.

22 Lawful collection and recording of electronic communications

If the High Court, on application by a Police officer, is satisfied on the basis of a sworn statement that content of specified electronic communications is reasonably required for the purposes of a criminal investigation or a criminal proceeding for an offence against this Act, the court may—

(a) order a service provider whose service is available in Niue to, through application of technical means, collect or record, or permit or assist a Police officer with the collection or recording of, computer data associated with specified electronic communications transmitted by means of a computer system; or

(b) authorise a Police officer to collect or record that computer data through application of technical means.

23 Forensic tool

(1) If the High Court, on application by a Police officer, is satisfied on the basis of a sworn statement of the matters specified in subsection (2), the court may authorise any Police officer or authorised person to—

(a) utilise a remote forensic tool for a specified task related to the collection of material evidence for an investigation; and

(b) install it on the suspect's computer system in order to collect that evidence.

(2) For subsection (1), the High Court must be satisfied that—

(a) the investigation concerns an offence against this Act; and

(b) there are reasonable grounds to believe that material evidence cannot be collected by other means under this Part; and

(c) that evidence is reasonably required for the purposes of the investigation.

(3) The application must contain the following information—

(a) the identity of the suspect of the offence and their service provider (with names and addresses, if possible);

(b) the offence being investigated;

(c) a description of the targeted computer system;

(d) a description of the intended tool, task, and extent and duration of the utilisation;

(e) if the installation requires physical access to a place, a description of how it is proposed that the access will be achieved;

(f) reasons why the evidence cannot be collected by other means under this Part;

(g) if the application seeks the Court's authorisation for an authorised person to utilise the remote forensic tool, that the Chief of Police has—

(i) authorised the person to do so in Niue, but must not include any identifying particulars of the authorised person; and

(ii) authorised use of the remote forensic tool in Niue.

(4) Any modifications to the computer system of the suspect must be limited to those essential for the investigation and, if possible, be able to be undone after the end of the investigation.

(5) During the investigation, the Police officer or authorised person must log the following—

(a) the technical means used as the remote forensic tool and time and date of the utilisation; and

(b) the identification of the computer system and details of the modifications undertaken to it; and

(c) any information or evidence obtained.

(6) Any information or evidence obtained must be protected against any modification, unauthorised deletion, and unauthorised access.

(7) An authorisation under this section is limited to a maximum of 3 months.

(8) If the conditions of an authorisation are no longer met, action under the authorisation must stop immediately.

(9) A Police officer may, when applying for an order under subsection (1), request that the court also order a service provider to assist with the installation process.

(10) In this section—

***authorised person*—**

(a) means a person—

(i) who is authorised by the Chief of Police to utilise a remote forensic tool in Niue; and

(ii) who the Chief of Police is satisfied has the appropriate skills and experience to do so; and

(b) includes a person from another jurisdiction who is authorised by the Chief of Police under paragraph (a);

remote forensic tool is a remote forensic tool authorised for use in Niue by the Chief of Police and includes a tool operated from outside of Niue;

suspect includes a suspect's service provider.

24 Offence—Refusing or failing to comply with warrant, order or notice, or to assist in executing warrant

A person commits an offence if they intentionally refuse or fail to comply with any of the following—

(a) a search and seizure warrant under section 18;

(b) a requirement under section 19 to permit or assist with the execution of a search and seizure warrant issued under section 18;

(c) a production order issued under section 20;

(d) a preservation notice issued under section 21;

(e) an order under section 22 to collect or record, or permit or assist with the collection or recording of, computer data associated with electronic communications;

(f) an order under section 23 to assist with the installation of a remote forensic tool.

Penalty: 300 penalty units and 3 years' imprisonment.

25 Disclosure of traffic data

The High Court may, on the application of a Police officer that includes reasons for the application, order a person to disclose traffic data if—

(a) the person has possession or control of the traffic data or a computer system on which the traffic data is stored; and

(b) the court is satisfied that the traffic data is required for the purpose of a criminal investigation or a criminal proceeding for an offence against this Act.

26 Collection or recording of traffic data

(1) If the High Court, on application by a Police officer, is satisfied on the basis of a sworn statement that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation or a criminal proceeding for an offence against this Act, the court may order the person in control of the data—

(a) to collect or record traffic data associated with the specified communication during a specified period and disclose it to the Police officer; or

(b) to permit and assist the Police officer to collect or record that data.

(2) If the High Court, on application by a Police officer, is satisfied on the basis of a sworn statement that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation or a criminal proceeding for an offence against this Act, the court may authorise any Police officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means.

(3) A Police officer may, when applying for an order under subsection (2), request that the court also order a service provider to assist with the collection or recording of the traffic data.

27 Offence—Refusing or failing to comply with order under section 25 or 26

A person commits an offence if they intentionally refuse or fail to comply with—

(a) an order under section 25 to make disclosure of traffic data; or

(b) an order under section 26 relating to the collection, recording, or disclosure of traffic data.

Penalty: 300 penalty units and 3 years' imprisonment.

Part 4 — Liability of bodies corporate and service providers

28 Corporate liability

(1) This section applies to a person (***person A***) that is not an individual, if either of the following commits an offence against this Act for the benefit of person A—

(a) an individual described in subsection (3) who is associated with person A (an ***associated individual***);

(b) subject to subsection (4), any other person acting under the authority of person A.

(2) Person A is to be treated as having committed the same offence as the associated individual or other person and is liable to a separate penalty for the offence.

(3) Person A is liable under subsection (1)(a) if the associated individual is a person who in the course of their duties has—

(a) a leading role within person A with the authority to act as its representative; and

(b) the authority to take decisions on behalf of person A; and

(c) the authority to exercise control within person A.

(4) Person A is liable under subsection (1)(b) if—

(a) person A knew the other person was involved in the offending; or

(b) a lack of reasonable supervision or reasonable control of the other person on the part of person A or an associated individual allowed the offending to occur.

(5) The conviction of a person that is not an individual under this section does not absolve the individual who committed the offence from criminal liability.

(6) To avoid doubt, section 5 applies to a person to whom this section applies.

29 Protection of service providers

(1) In the absence of intent to facilitate, aid or abet, a service provider is not subject to any criminal liability under this Act solely because the service provider's service or computer system is used in connection with a contravention of this Act by a person not subject to the authority, direction, or control of the service provider.

(2) Subsection (1) does not absolve the service provider from its liability—

(a) to act in accordance with an order from a court to take down or disable access to an electronic communication; or

(b) to expeditiously take appropriate action if it becomes aware of specific information or activity that appears to be illegal, for example—

(i) by taking down or disabling access to the information or activity; or

(ii) by informing the relevant public authority (to enable the authority to evaluate the nature of the information or activity).

(3) If the service provider takes action as contemplated by subsection (2), it is exempt from any contractual obligation to its subscriber to ensure the availability of the service.

(4) Despite subsection (2)(b), a service provider is not required to monitor the information that it transmits or stores on behalf of another person, nor does it have a general obligation to actively seek facts or circumstances indicating illegal activity to avoid criminal liability.

Part 5 — Miscellaneous

30 Immunity from criminal or civil liability

The following people are immune from criminal or civil liability for anything done or omitted to be done in good faith when carrying out or intending to carry out their duties under this Act—

(a) the Solicitor-General;

(b) an officer or employee of the Crown Law Office;

(c) the Chief of Police;

(d) a Police officer;

(e) a person assisting a Police officer (at the request of a Police officer) in relation to their duties under this Act.

31 Annual reporting by Chief of Police

(1) The Chief of Police must report annually to the Minister on all of the following for the period covered in the report—

(a) the number of applications made under Part 3 that were granted or refused;

(b) the numbers of orders made, warrants or notices issued, or authorisations or requirements given under Part 3;

(c) the nature and number of any criminal investigations undertaken in Niue relating to offences against this Act;

(d) the nature and number of any criminal proceedings taken in Niue relating to offences against this Act, including the number of convictions.

(2) The report must not include any information relating to—

(a) details of anything done under this Act that the Minister considers must be kept confidential for reasons of national security; or

(b) requests made under the Mutual Assistance in Criminal Matters Act 1998 (*see* section 51 of that Act).

(3) In this section, ***nature***—

(a) includes, in each case, reference to the relevant provisions in this Act and other details the Chief of Police considers should be reported to the Minister;

(b) does not include identifying particulars of any individuals or service providers or any details the Chief of Police considers should be withheld—

(i) to avoid a detrimental effect on the security of Niue or its nationals; or

(ii) to avoid prejudice to—

(A) any criminal investigation; or

(B) any criminal proceeding that is pending or that may be brought in relation to any investigation; or

(iii) in the public interest.

Regulations

32 Regulations

Cabinet may make regulations as it thinks fit for the purposes of this Act and in particular for providing for the following—

(a) prescribing procedures and requirements for undertaking any functions under this Act;

(b) prescribing forms to be used for the purposes of this Act;

(c) providing for any other matters contemplated by this Act, necessary for its full administration, or necessary for giving it full effect.

Related amendments

33 Related amendments to Mutual Assistance in Criminal Matters Act 1998

The Mutual Assistance in Criminal Matters Act 1998 is amended as set out in the Schedule.

Schedule Related amendments to Mutual Assistance in Criminal Matters Act 1998

Section 33

1 Section 3 amended *(Interpretation)*

In section 3, insert in their appropriate alphabetical order—

"article" includes computer data and traffic data;

"computer data" has the meaning given in section 3 of the Cybercrime Act;

"Cybercrime Act" means the Cybercrime Act 2026;

"thing" includes computer data and traffic data;

"traffic data" has the meaning given in section 3 of the Cybercrime Act;

2 New section 10AA

After section 10, in Part 1, insert—

10AA Urgent or expedited requests for assistance

(1) If the Attorney-General is satisfied, on reasonable grounds, that a request by a foreign country for assistance in a criminal matter is urgent, or needs to be expedited, they must notify the relevant authorities in Niue, in writing, and those authorities must respond to the request in an urgent or expedited manner (as relevant).

(2) The Attorney-General may seek further information from the foreign country about the request if they consider this is needed in order to decide whether or not the request is urgent or needs to be expedited.

3 Section 10A amended *(Requests by Niue)*

After section 10A(2), insert—

(3) If subsection (1) applies, the Attorney-General may also request the appropriate authority of the foreign country to serve documents relating to the criminal matter on the person.

4 New section 13A

After section 13, insert—

13A Requests by Niue for computer data or traffic data

If an investigation of or proceeding for a criminal matter has commenced in Niue relating to a serious offence involving computer data or traffic data, the Attorney-General may request the appropriate authority of a foreign country to obtain the issue of an instrument similar in nature to a warrant, order, notice, or authorisation under section 18, 20, 21, 22, 23 or 26 of the Cybercrime Act.

5 New section 14A

After section 14, in Part 3, insert—

14A Requests by foreign countries for computer data or traffic data

(1) This section applies to a request by a foreign country to the Attorney-General to locate and obtain computer data or traffic data relevant to an investigation of or proceeding for a criminal matter in that country.

(2) If there are reasonable grounds to believe that the data can be located and obtained in Niue, the Attorney-General may authorise a Police officer to make an application to the High Court under section 18, 20, 21, 22, 23, 25 or 26 of the Cybercrime Act in relation to that data.

(3) If an application is made under subsection (2), sections 16, 17, 19, 24 and 27 of the Cybercrime Act apply.

(4) Section 14(4) to (6) apply to data located or obtained under an application made under subsection (2) with any necessary modifications.

6 Section 50 replaced *(Restriction on use of information)*

Replace section 50 with—

50 Restriction on use of evidence, documents, articles, or things obtained from foreign countries

(1) This section applies to any evidence, documents, articles, or things (***material***) taken or produced in, or obtained from, a foreign country by a request made under this Act.

(2) The material may be used only for the purposes of, or in connection with, the criminal matter for which the request was made unless—

(a) the foreign country consents to the use of the material for another purpose or proceeding; and

(b) the Attorney-General gives written approval for the use of the material for that purpose or proceeding.

(3) The material must not be disclosed for any other purpose and is inadmissible in any proceeding without the consent of the Attorney-General.

(4) A person who contravenes this section commits an offence and is liable on conviction—

(a) in the case of an individual, to a fine not exceeding 120 penalty units or imprisonment not exceeding 2 years, or both;

(b) in any other case, to a fine not exceeding 600 penalty units.

Note for section 50—Section 19 provides limitations on the use of evidence given by a person brought to Niue under Part 4.

50A Custody and destruction of evidence, documents, articles, or things obtained from foreign country

(1) The law and procedures that apply in Niue to the custody and destruction of evidence, documents, articles, or things (***material***) held by the Niue Police or a court for a criminal investigation or criminal proceeding apply to anything taken or produced in, or obtained from, a foreign country under this Act.

(2) However, if the government of the foreign country wishes the material to be returned to it, the Chief of Police must arrange for its safe return to that government following the conclusion of the investigation or the proceeding for which it was obtained.

(3) In this section, ***investigation*** includes a proceeding arising out of that investigation.