REPUBLIC OF VANUATU

BILL FOR THE CYBERSECURITY ACT NO. OF 2026

Explanatory Note

In November 2022, a ransomware attack affected the Government of Vanuatu's broadband network. At the same time, government email systems, shared drives, and voice services failed. Critical information infrastructure (CII) within the Government, including systems supporting hospitals, government financial services and other public services, was significantly affected, preventing access to essential operational systems. As a result, revenue collection, licensing procedures, court administrative functions and many other activities came to a halt. The recovery process took several months and required support from development partners. Later, a criminal organization claimed responsibility, saying it had exfiltrated 3.2 terabytes of data.

The threat has since grown, not receded. Ransomware against small states, including Vanuatu, is now sold as a service. Hostile intrusion into government networks has become an instrument of state conduct as much as of crime. Vanuatu cannot answer either with an arrangement that rests on no legal foundation.

This Bill establishes clear and proactive legal guardrails to safeguard Vanuatu's CII, economy, and digital information, while also protecting citizens from escalating cyber threats. This initiative also aims to secure critical services and establish security benchmarks. The Bill sets clear standards, enhances threat information sharing, strengthens legal protections, and introduces mandatory reporting protocols.

The key features of this Bill are described below:

(a) The establishment of the National Cybersecurity Agency ("the Agency") as the lead national authority for cybersecurity.

(b) The Agency develops and coordinates national cybersecurity policy, issues codes of practice and technical standards, advises the Minister and the Council of Ministers, and represents Vanuatu internationally on cybersecurity and the protection of CII.

(c) The designation of CII against criteria stated on the face of the Act and linked to a Schedule of essential services. Designated operators must arrange annual cybersecurity audits, maintain risk management plans, appoint a Chief Information Security Officer or equivalent officer, report serious cyber incidents, participate in national cyber exercises and notify the Agency before making significant changes to infrastructure architecture. A system located outside Vanuatu may be designated where an essential service here depends on it.

(d) The Minister may declare a National Cyber Emergency on the advice of the Director if a serious cyber incident threatens national security, public safety, the economy or essential services and may have effects beyond the capacity of normal cybersecurity operations. A declaration ordinarily lasts 30 days but may be revoked earlier or extended. During an emergency, the Minister may direct government agencies and CII Operators to act or refrain from acting, and they must comply despite the provisions of any other Act.

(e) The Bill gives Vanuatu an authority legally accountable for the security of the systems on which the country depends. It converts an informal capability into a statutory one, places enforceable duties on those who operate critical systems, and gives the State a lawful basis to act while an attack is under way rather than only after it has ended. It gives regional and international partners a counterpart with standing to deal with them. Without it, Vanuatu's digital transformation proceeds on the assumption that nothing will fail.

Prime Minister

REPUBLIC OF VANUATU

BILL FOR THE CYBERSECURITY ACT NO. OF 2026

Arrangement of Sections

PART 1 INTERPRETATION 3
1 Interpretation 3

PART 2 NATIONAL CYBERSECURITY AGENCY AND DIRECTOR 6

Division 1 Establishment of the National Cybersecurity Agency 6
2 Establishment of National Cybersecurity Agency 6
3 Functions of the Agency 6
4 Powers of the Agency 7

Division 2 Director 7
5 Director 7
6 Functions of the Director 7
7 Powers of the Director 8

PART 3 NATIONAL CYBERSECURITY ADVISORY BOARD 9
8 Establishment of the National Cybersecurity Advisory Board 9
9 Composition of the Board 9
10 Functions of the Board 10
11 Chairperson and Deputy Chairperson of the Board 10
12 Meetings of the Board 10
13 Sitting allowances of the members of the Board 11
14 Removal of a member of the Board 11

PART 4 DECLARATION OF NATIONAL CYBER EMERGENCY 12
15 Declaration of National Cyber Emergency 12
16 Broadcasting of declaration 12
17 Duration of the National Cyber Emergency 12
18 Minister's power to direct government agencies and CII Operators 13
19 Other special powers when declaration is in force 13

PART 5 RESPONSE TO RANSOMWARE AND ESPIONAGE 14
20 Response to ransomware 14
21 Response to espionage 14

PART 6 DESIGNATION OF CRITICAL INFORMATION INFRASTRUCTURE 16
22 Designation of critical information infrastructure 16
23 Urgent temporary designation 17
24 Designation of critical information infrastructure supplier 17

PART 7 CYBERSECURITY OBLIGATIONS 19
25 Obligations of government agency and reporting entity 19
26 Obligations of CII Operators 19

PART 8 ENFORCEMENT 20
27 Authorised officer 20
28 Request for disclosure of information and documents 21
29 Powers of entry 21
30 Powers on entry 22
31 Receipt for things seized 23
32 Return of things seized 23
33 Police to assist authorised officers 23
34 Warrant 23

PART 9 OFFENCES AND PENALTIES 26
35 Offences 26
36 Penalty notice 28

PART 10 MISCELLANEOUS PROVISIONS 29
37 Amendment of the Schedule 29
38 Annual report 29
39 Immunity 29
40 Regulations 29
41 Commencement 30

SCHEDULE 31

REPUBLIC OF VANUATU

BILL FOR THE CYBERSECURITY ACT NO. OF 2026

An Act to provide for the establishment, operation and management of the National Cybersecurity Agency and related matters.

Be it enacted by the President and Parliament as follows-

PART 1 INTERPRETATION

1 Interpretation

In this Act, unless a contrary intention appears:

Agency means the National Cybersecurity Agency established under section 2;

authorised officer means a person appointed as an authorised officer under section 27;

Board means the National Cybersecurity Advisory Board established under section 8;

computer system has the same meaning as in the Cybercrime Act No. 22 of 2021 and includes an operational technology system, including an industrial control system, a programmable logic controller, a supervisory control and data acquisition system and a distributed control system, whether or not the system would otherwise be a computer within that meaning;

critical information infrastructure means any computer system, infrastructure, network or associated services that, if disrupted or compromised, may have a significant impact on national security, public safety, public health, the economy or essential services;

CII Operator means a person who operates, manages or controls a designated infrastructure;

cyber incident means any event compromising the confidentiality, integrity, or availability of a computer system or data;

critical supplier means a vendor, contractor, or service provider whose goods, components, or services are essential to an organisation's core operations, safety, compliance, or business continuity, such that any failure or disruption in their delivery would cause severe economic, operational, financial, societal, or reputational damage or harm;

cyber threat means any potential occurrence or event that may cause harm to a computer system;

cybersecurity protection means the protection of computer systems, networks, and data from attack, damage, or unauthorised access;

cybersecurity risk means the likelihood and impact of a cyber incident;

cyber espionage means state-sponsored or organised unauthorised intrusion into computer systems for intelligence gathering;

designated infrastructure means a critical information infrastructure designated under section 22;

Director means the Director of the National Cybersecurity Agency;

Director General means the Director General of the Ministry responsible for cybersecurity;

essential service means an essential service classified under the Schedule;

government agency means:

(a) a Ministry; or

(b) an office or body established under the Constitution; or

(c) an office or body established under an Act of Parliament; or

(d) a prescribed agency;

Minister means the Minister responsible for cybersecurity;

ransomware means malicious software that encrypts data and demands payment for decryption;

regulated entity means an organisation, institution, business, or individual that is authorised and required to operate under specific rules and laws, subject to continuous oversight by a government agency or regulatory body that is directly bound by the statutory duties of the Act;

reporting entity means a public body, statutory body, body corporate, company, organisation, CII Operator, critical supplier or other entity that is required under this Act to submit a report to the Agency;

serious cyber incident means a cyber incident that has a significant impact on the availability, integrity or operation of a critical information infrastructure and essential services;

vulnerability means a weakness in a computer system or network that could be exploited.

PART 2 NATIONAL CYBERSECURITY AGENCY AND DIRECTOR

Division 1 Establishment of the National Cybersecurity Agency

2 Establishment of National Cybersecurity Agency

The National Cybersecurity Agency is established.

3 Functions of the Agency

The Agency has the following functions:

(a) to develop, review and coordinate national cybersecurity policies and strategies; and

(b) to deal with national and international cybersecurity operations; and

(c) to monitor and coordinate responses to cybersecurity incidents and threats; and

(d) to designate and oversee critical information infrastructure; and

(e) to ensure the protection of critical information infrastructure; and

(f) to carry out investigations and intelligence gathering; and

(g) to carry out cybersecurity and cybercrime research and development; and

(h) to plan and conduct national cyber drills and exercises; and

(i) to promote cyber innovation and emerging development; and

(j) to represent Vanuatu in international matters relating to cybersecurity; and

(k) to conduct public awareness and education on cybersecurity in Vanuatu; and

(l) to be the focal point for national and international cyber cooperation; and

(m) to develop technical standards; and

(n) to advise the Minister on matters relating to the administration of this Act; and

(o) to perform such other functions as may be conferred on the Agency by this Act or any other Act.

4 Powers of the Agency

(1) The Agency has the power to do all things necessary or convenient to be done for or in connection with the performance of its functions under this Act.

(2) Without limiting subsection (1), the Agency has the power to do all or any of the following:

(a) to issue guidelines; and

(b) to issue cybersecurity codes of practice; and

(c) to conduct cybersecurity audits and assessments of regulated entities.

Division 2 Director

5 Director

(1) The Director is responsible for the day-to-day management and administration of this Act.

(2) The Director must advise and assist the Minister and the Director General in matters relating to the Agency as required under this Act.

6 Functions of the Director

The Director has the following functions:

(a) to advise the Board and the Minister on matters relating to the administration of this Act; and

(b) to report to the Minister on cybersecurity threats, incidents and emerging risks affecting Vanuatu; and

(c) to advise the Minister and the Council of Ministers, after receiving advice from the Board, on cybersecurity matters; and

(d) to manage and oversee the operations of the Agency; and

(e) to develop annually a National Cybersecurity Work Programme; and

(f) to monitor and implement the National Cybersecurity Strategy and to report to the Minister on its progress; and

(g) to perform such other functions as may be conferred on the Director by this Act or any other Act.

7 Powers of the Director

(1) The Director has the power to do all things necessary or convenient to be done for or in connection with the performance of his or her functions under this Act.

(2) Without limiting subsection (1), the Director may direct a government agency, regulated entity, CII Operator or critical supplier in writing:

(a) to prevent or respond to a cyber incident or threat; or

(b) to comply with a code of practice.

PART 3 NATIONAL CYBERSECURITY ADVISORY BOARD

8 Establishment of the National Cybersecurity Advisory Board

The National Cybersecurity Advisory Board is established.

9 Composition of the Board

(1) The Board consists of the following persons:

(a) the Director of the Department of Communications and Digital Transformation; and

(b) the Director of Finance and Treasury; and

(c) the National Security Advisor; and

(d) a senior representative of the Police nominated by the Commissioner of Police; and

(e) a person representing the National University of Vanuatu nominated by the Chancellor; and

(f) a person representing the Vanuatu Chamber of Commerce nominated by the Chairperson.

(2) Subject to subsection (4), the Minister is to appoint the members under paragraphs (1)(e) and (f).

(3) The person nominated under paragraph (1)(d) must have relevant operational knowledge or experience in cybercrime, cybersecurity, digital investigations, intelligence or related law-enforcement matters.

(4) A person nominated under paragraph (1)(e) or (f) must:

(a) have a tertiary qualification in cybersecurity, digital infrastructure, risk management, computer science, information technology, engineering, law, public administration or a related field; and

(b) have not less than 5 years' experience in dealing with cybersecurity, information technology or digital safety; and

(c) not have been convicted of a serious offence involving dishonesty, corruption, cybercrime or abuse of office; and

(d) be a citizen of Vanuatu.

(5) A member appointed under paragraph (1)(e) or (f) is appointed for a term of 4 years and may be re-appointed.

10 Functions of the Board

(1) The Board has an advisory function only.

(2) The Board is to advise the Director on:

(a) any policy relating to cybersecurity; and

(b) any matter relating to critical information infrastructure; and

(c) major regulatory directions.

(3) To avoid doubt, the Board has no decision-making powers.

11 Chairperson and Deputy Chairperson of the Board

(1) The members of the Board are to elect from amongst themselves a Chairperson.

(2) The members of the Board are to elect from amongst themselves a Deputy Chairperson.

(3) The Deputy Chairperson is to hold office for a period of 1 year and may be re-elected.

12 Meetings of the Board

(1) The Board is to meet at least once every quarter and may hold such other meetings as are necessary for the proper performance of its functions under this Act.

(2) The Chairperson is to preside at all meetings of the Board and if the Chairperson is absent, the Deputy Chairperson is to preside at these meetings.

(3) The quorum for a meeting is 4 members of the Board present at the meeting.

(4) A member present at the meeting has 1 vote and questions arising at a meeting are to be decided by a majority of votes.

(5) If the voting at the meeting is equal, the Chairperson or the Deputy Chairperson (if he or she is presiding over the meeting) has a casting vote.

(6) The Agency is the Secretary of the Board.

(7) The Agency, after consultation with the Chairperson, is to notify the other members of the Board of the venue, time and date of the meeting.

(8) Subject to this Act, the Board may determine and regulate its own procedures.

13 Sitting allowances of the members of the Board

The Minister may, on the advice of the Director, by Order, prescribe the sitting allowances for the members of the Board.

14 Removal of a member of the Board

A member appointed under paragraph 9(1)(e) or (f) is to be removed as a member if he or she:

(a) fails to attend 3 consecutive meetings of the Board without the permission of the Board; or

(b) is suspended from his or her profession; or

(c) is incapable of performing his or her duties as a member.

PART 4 DECLARATION OF NATIONAL CYBER EMERGENCY

15 Declaration of National Cyber Emergency

(1) The Minister may, on the advice of the Director, by Order, declare that a National Cyber Emergency exists in the whole of Vanuatu or a specified part or parts of Vanuatu in relation to a cyber incident.

(2) In making a declaration under subsection (1), the Minister must be satisfied that the cyber incident:

(a) is a serious cyber incident threatening national security, public safety, the economy or essential services; and

(b) may have effects that are beyond the capacity of normal cybersecurity operations.

16 Broadcasting of declaration

After a declaration of a National Cyber Emergency under section 15, the Minister must inform the public of the declaration through the media.

17 Duration of the National Cyber Emergency

(1) A declaration of a National Cyber Emergency has effect immediately on the day it is made.

(2) The declaration of a National Cyber Emergency does not prevent the declaration of a further National Cyber Emergency in relation to the same or a different cyber incident.

(3) The declaration of a National Cyber Emergency ends 30 days after the day on which it is made, unless upon the advice of the Agency:

(a) the Minister revokes the declaration of a National Cyber Emergency sooner if it is no longer necessary; or

(b) the Minister extends the declaration of a National Cyber Emergency for a further period as recommended by the Director.

18 Minister's power to direct government agencies and CII Operators

(1) If a declaration of a National Cyber Emergency is in force, the Minister may, on the advice of the Agency, direct any government agency or CII Operator to do or refrain from doing any act or to exercise or refrain from exercising any function.

(2) If a direction is given to a government agency or CII Operator under this section, the government agency or CII Operator must comply with the direction despite the provisions of any other Act.

19 Other special powers when declaration is in force

(1) The powers in this section apply only during a National Cyber Emergency.

(2) If the Director is satisfied that it is necessary in the interest of safety, he or she may authorise an officer of the Agency:

(a) to direct a person to do any or all of the following:

(i) to leave particular premises and to move out of a National Cyber Emergency area; or

(ii) not to enter a National Cyber Emergency area; or

(iii) to disclose any information or document; or

(b) to close any public or private place during a National Cyber Emergency.

(3) If the person does not comply with the direction under subsection (2), the officer of the Agency may do all such things as are reasonably necessary to ensure compliance with it, using such force as is reasonably necessary in the circumstances.

(4) A police officer may, on the request of the Director, assist the Director in exercising his or her powers under subsection (2).

PART 5 RESPONSE TO RANSOMWARE AND ESPIONAGE

20 Response to ransomware

(1) A government agency, reporting entity or CII Operator that detects a serious cyber incident involving a ransomware attack must give an early warning to the Agency within 24 hours of detection.

(2) In addition to giving an early warning under subsection (1), the government agency, reporting entity or CII Operator must, within 72 hours after giving the early warning, determine whether there is a serious cyber incident involving a ransomware attack and notify the Agency of that determination.

(3) On request, the Agency must, within 24 hours of being notified under subsection (2), respond to the government agency, reporting entity or CII Operator by providing initial feedback and guidance on mitigation.

(4) The Agency must, after it is determined that a serious cyber incident involving a ransomware attack has occurred:

(a) conduct an initial risk assessment; and

(b) coordinate containment and recovery actions; and

(c) provide technical guidance; and

(d) request relevant information; and

(e) coordinate with the Police, national security bodies and other relevant authorities where necessary.

(5) The Agency is to provide a report within 30 days after it is determined that a ransomware attack has occurred.

21 Response to espionage

(1) If a person becomes aware of:

(a) unauthorised access to a computer system; or

(b) unauthorised use of a computer system,

in circumstances that reasonably suggest that information is being gathered for the benefit of a foreign State or an organised group, that person must report the matter to the Agency as soon as reasonably practicable.

(2) A person who makes a report under subsection (1) in good faith does not incur any civil or criminal liability or liability for breach of duty, or suffer any detriment in employment, for making the report.

(3) Subject to subsection (2), the identity of the person making the report must be protected except with the person's consent or by order of the Court.

(4) The Agency must, after receiving a report under subsection (1), conduct an investigation into the alleged cyber espionage.

(5) The Agency, on completing an investigation, is to provide a report to the National Security Council.

PART 6 DESIGNATION OF CRITICAL INFORMATION INFRASTRUCTURE

22 Designation of critical information infrastructure

(1) The Minister may, by Order, on the recommendation of the Director after consultation with relevant sector regulators and operators, designate a critical information infrastructure.

(2) The Minister, in making a designation under subsection (1), must be satisfied that:

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

(b) the loss, disruption or compromise of the computer system or network would be likely to have a deliberate effect on the availability, integrity or delivery of that service in Vanuatu; and

(c) it is located wholly or partly in Vanuatu or is used to deliver an essential service in Vanuatu.

(3) The Director, prior to making a recommendation under subsection (1), must notify the operator of the intention to designate the critical information infrastructure.

(4) A notice under subsection (3) must inform the operator of the following:

(a) the critical information infrastructure that is to be designated; and

(b) the purpose for designating the critical information infrastructure; and

(c) that the operator of the critical information infrastructure has 14 working days to provide written representations to the Director.

(5) The Director is to consider the representations of the operator and must:

(a) recommend designation of the whole or a specified part of the computer system or decide not to recommend designation; and

(b) give written notice of the decision with reasons to everyone who received the notice of intention.

(6) If a critical information infrastructure is designated under this section, the person who owns or controls that critical information infrastructure is the designated CII Operator.

(7) The Agency is to establish and maintain a register for the designation of critical information infrastructure.

23 Urgent temporary designation

(1) For the purpose of protecting national security or dealing with a serious cyber incident affecting an essential service, the Director may, by written notice, designate a person as a critical supplier in relation to a critical information infrastructure.

(2) The Director, in designating a person as a critical supplier, must be satisfied that:

(a) the person supplies goods or services to the CII Operator; and

(b) the serious cyber incident may have a deliberate effect on the availability, integrity or delivery of the essential service to which the critical information infrastructure relates.

(3) A critical supplier must:

(a) comply with any code of practice expressed to apply to critical suppliers; and

(b) report to the Director a serious cyber incident affecting the goods or services supplied; and

(c) notify the CII Operator and the Director of a material change to the goods or services supplied that affects their security.

24 Designation of critical information infrastructure supplier

(1) The Minister may, by Order, on the recommendation of the Director after consultation with relevant sector regulators and operators, designate a critical information infrastructure supplier.

(2) The Director, in making a recommendation under subsection (1), must be satisfied that:

(a) the goods and services are necessary for the operation or security of the critical information infrastructure; and

(b) a serious cyber incident affecting those goods or services may disrupt the delivery of essential services.

(3) The Director, prior to making a recommendation under subsection (1), must notify the supplier of the intention to designate the supplier.

(4) A notice under subsection (3) must inform the supplier of the following:

(a) the critical information infrastructure goods and services that are to be designated; and

(b) the purpose for designating the critical information infrastructure supplier.

(5) The Director is to consider the representations of the supplier and must either recommend designation of the whole or a specified part of the computer system or decide not to recommend designation and must give written notice of the decision with reasons to everyone who received the notice of intention.

(6) The power to designate part only is what allows a scope objection to be met.

PART 7 CYBERSECURITY OBLIGATIONS

25 Obligations of government agency and reporting entity

A government agency or reporting entity must:

(a) comply with the National Cybersecurity Framework issued by the Agency; and

(b) appoint a designated cybersecurity focal point; and

(c) conduct annual cybersecurity risk assessments; and

(d) enforce baseline security controls as prescribed under the Cybersecurity Code of Practice; and

(e) report any cyber incident to the Agency within 72 hours of detection.

26 Obligations of CII Operators

A CII Operator must:

(a) comply with sector-specific Cybersecurity Codes of Practice; and

(b) arrange for annual cybersecurity audits to be conducted by an auditor approved by the Agency and submit the audit reports to the Agency; and

(c) maintain an up-to-date cybersecurity risk management plan; and

(d) appoint a Chief Information Security Officer (CISO) or an equivalent officer; and

(e) report serious cyber incidents to the Agency within 6 hours of detection; and

(f) participate in national cyber exercises; and

(g) notify the Agency before making significant changes to the architecture of critical information infrastructure.

PART 8 ENFORCEMENT

27 Authorised officer

(1) The Director may appoint:

(a) a senior officer of the Agency; or

(b) any other person,

to be an authorised officer for the purposes of this Act.

(2) A person appointed under paragraph (1)(b) must satisfy the following criteria:

(a) the person has relevant qualifications, training, technical knowledge or experience in cybersecurity, information and communications technology, digital forensics, compliance, investigations or law enforcement; and

(b) the person is not an officer, employee or agent of a CII Operator, a critical supplier, a reporting entity, or a person who provides cybersecurity services on a commercial basis in Vanuatu.

(3) The Director must give an identity card to a person who is appointed as an authorised officer.

(4) The identity card must be signed by the Director and include a photograph of the authorised officer and his or her signature.

(5) An authorised officer must, in performing his or her functions or exercising his or her powers under this Act, produce his or her identity card, if requested to do so.

(6) An authorised officer must notify the Director if he or she has a conflict of interest in performing his or her functions or exercising his or her powers under this Act.

(7) The Director, after being informed under subsection (6), must replace the authorised officer and disregard any decision taken by the authorised officer.

28 Request for disclosure of information and documents

(1) An authorised officer may, in writing, request a person to disclose any information or document if he or she is satisfied that the disclosure is necessary for a cybersecurity investigation.

(2) A person must comply with the request under subsection (1) within 14 days after receiving the request.

(3) A person who fails to comply with subsection (2) commits an offence and is liable on conviction to a fine not exceeding VT1,000,000.

29 Powers of entry

(1) An authorised officer may enter:

(a) any premises at any time with the consent of the occupier of the premises; or

(b) business premises during business hours; or

(c) premises when open to the public.

(2) An authorised officer, prior to entering premises, must give one day's notice to the occupier of the premises and seek the consent of the occupier of the premises before entering the premises.

(3) An authorised officer, after receiving the consent of an occupier of premises under subsection (2), must:

(a) produce his or her identity card; and

(b) inform the occupier of the premises:

(i) of the purpose of the entry; and

(ii) that anything found and seized may be used as evidence in Court; and

(iii) that the occupier may refuse consent.

(4) In carrying out an inspection, an authorised officer must:

(a) avoid any damage or inconvenience; and

(b) not remain on the premises any longer than is reasonably necessary; and

(c) leave the premises, so far as practicable, in the same condition as they were found prior to the inspection being carried out.

30 Powers on entry

(1) In exercising a power of entry under section 29, an authorised officer may do all or any of the following:

(a) access, inspect and examine a computer system on the premises and make copies or an image of data held in or accessible in the computer system; or

(b) search the premises and anything on the premises; or

(c) inspect an electronic record or a document kept on the premises, and make copies of or take extracts from it; or

(d) take photographs, make video recordings or make sketches of the premises or of anything on the premises; or

(e) seize anything on the premises that the authorised officer believes on reasonable grounds is necessary to be seized in order to prevent its concealment, loss, alteration or destruction; or

(f) bring onto the premises any equipment or material the authorised officer reasonably needs to exercise a power under this Part; or

(g) require the occupier of the premises, or a person on the premises, to give the authorised officer reasonable help to exercise a power under this Part.

(2) An authorised officer must obtain a warrant before exercising the powers under subsection (1).

(3) A person who refuses or fails, without reasonable excuse, to comply with a requirement under paragraph (1)(g) commits an offence and is liable on conviction to a fine not exceeding VT1,000,000.

31 Receipt for things seized

(1) Immediately after seizing a thing from a person, an authorised officer must give the person a written receipt for the thing seized.

(2) If, for any reason, it is not practicable to comply with subsection (1), the authorised officer must leave the written receipt secured in a place where it is visible to the occupier of the premises.

32 Return of things seized

(1) If an authorised officer seizes a thing, the authorised officer must take reasonable steps to return it to the person from whom it was seized if the reason for its seizure no longer exists.

(2) If the item has not been returned within 14 days after it is seized, the authorised officer must take reasonable steps to return it unless:

(a) proceedings have commenced and those proceedings have not been completed; or

(b) the Court makes an order under subsection (4), extending the period of 14 days.

(3) An authorised officer may apply to the Court before the expiration of the 14-day period or within a period extended by the Court for an extension of that period.

(4) The Court may order an extension if satisfied that the retention of the thing is necessary for the purposes of an investigation into whether an offence has been committed or to enable evidence of an offence to be obtained for the purposes of a prosecution.

(5) The authorised officer must notify the person of any application made under subsection (3).

33 Police to assist authorised officers

An authorised officer may request the assistance of a police officer to take any action authorised by this Act.

34 Warrant

(1) The following persons may apply to the Court for a search warrant:

(a) the Director; or

(b) an authorised officer with the approval of the Director.

(2) An application under subsection (1) may seek a warrant authorising a person specified in the warrant to:

(a) enter the premises; or

(b) search the premises and take copies of, or remove, any document, equipment or material from the premises.

(3) The application under subsection (1) may specify:

(a) premises belonging to, or in the possession or control of, a CII Operator; or

(b) any other premises that the Director or authorised officer has reasonable grounds to believe contain documents relevant to an investigation.

(4) The Court may issue a search warrant if it is satisfied on reasonable grounds that:

(a) there is a particular thing ('the evidence') at the premises connected with an offence against this Act; or

(b) failure to obtain the search warrant would prejudice an investigation; or

(c) there is a reasonable likelihood that the documents sought are on the premises and could be altered, destroyed or removed.

(5) If an authorised officer removes a document from the premises under a search warrant, the authorised officer must leave a copy of the document at the premises.

(6) A warrant is valid for the period specified in the warrant, being a period not exceeding 90 days.

(7) Subject to subsection (6), the Court may grant an extension of a warrant upon an application made before the warrant expires.

(8) An application for an extension of a search warrant must:

(a) state the reason for the extension and the period for which it is required; and

(b) be supported by any other information that the Court may consider necessary.

(9) The Court may extend a warrant if it is satisfied that the circumstances described under subsection (4) still apply.

PART 9 OFFENCES AND PENALTIES

35 Offences

(1) A person who fails to report a cyber incident within the timeframe required under this Act commits an offence and is liable on conviction:

(a) in the case of an individual- to a fine not exceeding VT3,000,000 or to a term of imprisonment not exceeding 3 years, or both; or

(b) in the case of a body corporate- to a fine not exceeding VT20,000,000.

(2) A person who fails to comply with a direction of the Director commits an offence and is liable on conviction:

(a) in the case of an individual- to a fine not exceeding VT3,000,000 or to a term of imprisonment not exceeding 3 years, or both; or

(b) in the case of a body corporate- to a fine not exceeding VT20,000,000.

(3) A person who fails to comply with a direction of the Minister during a National Cyber Emergency commits an offence and is liable on conviction:

(a) in the case of an individual- to a fine not exceeding VT3,000,000 or to a term of imprisonment not exceeding 3 years, or both; or

(b) in the case of a body corporate- to a fine not exceeding VT20,000,000.

(4) A person who contravenes a provision of this Act commits an offence and is liable on conviction:

(a) in the case of an individual- to a fine not exceeding VT10,000,000 or to a term of imprisonment not exceeding 5 years, or both; or

(b) in the case of a body corporate- to a fine not exceeding VT20,000,000.

(5) A person who recklessly or negligently makes any representation under this Act that the person knows to be false or misleading commits an offence and is liable on conviction:

(a) for an individual- to a fine not exceeding VT3,000,000 or imprisonment for a term not exceeding 3 years, or both; or

(b) for a body corporate- to a fine not exceeding VT20,000,000.

(6) A person who obstructs the Director or any person authorised by the Director in performing any of his or her duties under this Act commits an offence and is liable on conviction to a fine not exceeding VT10,000,000 or imprisonment for a term not exceeding 5 years or both.

(7) A person who:

(a) gives false or misleading information to an authorised officer that the person knows to be false or misleading; or

(b) produces a document to an authorised officer that the person knows to be false or misleading,

commits an offence and is liable on conviction to a fine not exceeding VT10,000,000 or to imprisonment for a term not exceeding 5 years, or both.

(8) If a person without reasonable excuse obstructs or hinders an authorised officer in exercising any power under this Act, the person commits an offence and is liable on conviction to a fine not exceeding VT10,000,000, or to imprisonment for a term not exceeding 5 years, or both.

(9) If a person impersonates an authorised officer, the person commits an offence and is liable on conviction to a fine not exceeding VT10,000,000, or to imprisonment for a term not exceeding 5 years, or both.

(10) A person who intentionally obstructs a person in the execution of a search warrant issued under this Act commits an offence and is liable on conviction to a fine not exceeding VT10,000,000.

36 Penalty notice

(1) The Director may serve a penalty notice on a person if it appears to the Director that the person has committed an offence under any provision of this Act.

(2) A penalty notice is a notice to the effect that, if the person served does not wish to have the matter determined by a Court, the person may, within the time specified in the notice, pay the amount of the penalty stated in the notice to the person specified in the notice.

(3) A penalty notice may be served personally, by post or by email.

(4) If the amount of penalty prescribed for the purposes of this section for an alleged offence is paid under this section, no person is liable to any further proceedings for the alleged offence.

(5) Payment under this section is not to be regarded as an admission of liability for the purposes of any civil proceedings arising out of the same occurrence, nor does it in any way affect or prejudice any such proceedings.

(6) The Regulations may prescribe the amount of penalty payable for the offence if dealt with under this section.

(7) The amount of a penalty prescribed under this section for an offence must not exceed the maximum amount of penalty provided for in this Act.

PART 10 MISCELLANEOUS PROVISIONS

37 Amendment of the Schedule

The Minister may, by Order, on the recommendation of the Director:

(a) add to, vary or replace the Schedule; or

(b) remove any of the essential services specified in the Schedule.

38 Annual report

(1) The Director must, within 2 months after the end of each year:

(a) provide the Director General with a report of the activities of the Agency for that year; and

(b) provide the Director General with any additional information that he or she may require about a matter contained in the report.

(2) The Director General must include the Director's report in the annual report as required under the Public Service Act [CAP 246].

39 Immunity

(1) Civil or criminal proceedings must not be brought against any staff member of the Agency, an authorised officer, the Director or a member of the Board for anything done or omitted to be done in good faith in performing his or her functions or exercising his or her powers under this Act.

(2) Subsection (1) does not apply if any staff member of the Agency, an authorised officer, the Director or a member of the Board acted in bad faith in performing his or her functions or exercising his or her powers under this Act.

40 Regulations

The Minister may, on the advice of the Director, make Regulations prescribing matters:

(a) required or permitted by this Act to be prescribed; or

(b) that are necessary or convenient to be prescribed for the better carrying out or giving effect to the provisions of this Act.

41 Commencement

This Act commences on the day on which it is published in the Gazette.

SCHEDULE

The following are classified as essential services:

(a) Energy and utilities;

(b) Water and sanitation;

(c) Telecommunications and digital infrastructure;

(d) Banking, payments and finance, insurance, payroll, and core accounting functions;

(e) Aviation;

(f) Maritime and ports;

(g) Land transport and logistics;

(h) Healthcare and medical services;

(i) Emergency services and disaster management;

(j) Government administration;

(k) Border management and national security;

(l) Elections;

(m) Food security;

(n) Education;

(o) Courts.