Intelligence and Security Act 2017

Public Act	2017 No 10
Date of assent	28 March 2017
Commencement	see section 2

Contents

Part 5
Accessing information held by other agencies

The Parliament of New Zealand enacts as follows:

1 Title

This Act is the Intelligence and Security Act 2017.

2 Commencement

(1) The following provisions come into force on 1 April 2017:

(a) section 4, in relation to the definition of **intelligence and security agency**:

(b) subpart 6 of Part 4:

(c) section 118:

(d) section 119:

(e) subpart 2 of Part 5:

(f) sections 167 to 170:

(g) section 242(1):

(h) sections 256 to 258:

(i) sections 283 to 311:

(j) Schedule 2:

(k) Part 1 of Schedule 3:

(l) Part 3 of Schedule 3.

(2) The rest of this Act comes into force on the day that is 6 months after the date of Royal assent.

Part 1
Preliminary provisions

3 Purpose

The purpose of this Act is to protect New Zealand as a free, open, and democratic society by—

(a) establishing intelligence and security agencies that will effectively contribute to—

(i) the protection of New Zealand's national security; and

(ii) the international relations and well-being of New Zealand; and

(iii) the economic well-being of New Zealand; and

(b) giving the intelligence and security agencies adequate and appropriate functions, powers, and duties; and

(c) ensuring that the functions of the intelligence and security agencies are performed—

(i) in accordance with New Zealand law and all human rights obligations recognised by New Zealand law; and

(ii) with integrity and professionalism; and

(iii) in a manner that facilitates effective democratic oversight; and

(d) ensuring that the powers of the intelligence and security agencies are subject to institutional oversight and appropriate safeguards.

4 Interpretation

In this Act, unless the context otherwise requires,—

advisory panel means the advisory panel continued by section 167

Auditor-General means the Controller and Auditor-General appointed under section 7 of the Public Audit Act 2001

Chief Commissioner of Intelligence Warrants means the Chief Commissioner of Intelligence Warrants appointed under section 112(2)

Commissioner of Intelligence Warrants means a Commissioner of Intelligence Warrants appointed under section 112(1)

department—

(a) means a department specified in Schedule 1 of the State Sector Act 1988; and

(b) includes a departmental agency as defined in section 27A of the State Sector Act 1988

Deputy Inspector-General means the Deputy Inspector-General of Intelligence and Security appointed under section 164

designated terrorist entity has the meaning given to it by section 4(1) of the Terrorism Suppression Act 2002

Director-General of an intelligence and security agency means—

(a) the Director-General of Security:

(b) the Director-General of the Government Communications Security Bureau

Director-General of Security means the chief executive of the New Zealand Security Intelligence Service

Director-General of the Government Communications Security Bureau means the chief executive of the Government Communications Security Bureau

employee, in relation to an intelligence and security agency, means a person employed in any capacity in that agency

financial year means a period of 12 months commencing on 1 July and ending with 30 June

foreign organisation means—

(a) a Government of any jurisdiction other than New Zealand:

(b) an entity controlled by the Government of any jurisdiction other than New Zealand:

(c) a body corporate that is incorporated outside New Zealand, or any company within the meaning of the Companies Act 1993 that is, for the purposes of the Companies Act 1993, a subsidiary of any body corporate incorporated outside New Zealand:

(d) an unincorporated body of persons—

(i) that is not a body 50% or more of whose members are New Zealand citizens or permanent residents of New Zealand; and

(ii) that carries on activities wholly or in part outside New Zealand:

(e) an international organisation

foreign person means a person who is not—

(a) a New Zealand citizen; or

(b) a permanent resident of New Zealand

foreign public agency means any person or body, wherever situated, that performs any public function, duty, or power conferred on that person or body by or under the laws of a foreign country

Government Communications Security Bureau means the Government Communications Security Bureau continued by section 8

human intelligence activities means activities that involve the use of any person to gather intelligence

Human Rights Commissioners means the members of the Human Rights Commission that is continued by section 4 of the Human Rights Act 1993

Independent Police Conduct Authority means the Authority established under section 4 of the Independent Police Conduct Authority Act 1988

information assurance and cybersecurity activities means activities that are carried out proactively or reactively to ensure the availability, confidentiality, and integrity of communications and information infrastructures

information infrastructure includes electromagnetic emissions, communications systems and networks, information technology systems and networks, and any communications carried on, contained in, or relating to those emissions, systems, or networks

Inspector-General of Intelligence and Security or **Inspector-General** means the Inspector-General of Intelligence and Security holding office under section 157

intelligence and security agency means—

(a) the New Zealand Security Intelligence Service:

(b) the Government Communications Security Bureau

Intelligence and Security Committee or **Committee** means the Intelligence and Security Committee continued by section 192

intelligence warrant has the meaning given to it by section 47

ministerial policy statement means a ministerial policy statement issued under section 206, 207, or 208, and includes any amendments made to a statement under section 212

New Zealand citizen means a person who has New Zealand citizenship as provided in—

(a) the Citizenship Act 1977; or

(b) the Citizenship (Western Samoa) Act 1982

New Zealand person—

(a) means any person being—

(i) a New Zealand citizen; or

(ii) a person ordinarily resident in New Zealand; or

(iii) an unincorporated body of persons, being a body of which more than 50% of the members are New Zealand persons under subparagraphs (i), (ii), or (iv); or

(iv) a body corporate that is incorporated in New Zealand; but

(b) does not include—

(i) any company within the meaning of the Companies Act 1993 that is, for the purposes of that Act, a subsidiary of any body corporate incorporated outside New Zealand; or

(ii) any company within the meaning of the Companies Act 1993, or building society, in which—

(A) 25% or more of any class of shares is held by any overseas person or overseas persons; or

(B) the right to exercise or control the exercise of 25% or more of the voting power at any meeting of the company or building society is held by any overseas person or overseas persons; or

(iii) a person acting in his or her capacity as a nominee of an overseas person, whether or not that person is also an overseas person

New Zealand Security Intelligence Service means the New Zealand Security Intelligence Service continued by section 7

official information has the meaning given to it by section 2(1) of the Official Information Act 1982, and includes security records

Ombudsman means an Ombudsman appointed under the Ombudsmen Act 1975

overseas person has the meaning given to it by section 7 of the Overseas Investment Act 2005

permanent resident of New Zealand means a person who is the holder, or is deemed to be the holder, of a permanent resident visa under the Immigration Act 2009

Privacy Commissioner means the Privacy Commissioner appointed under section 12 of the Privacy Act 1993

public authority means a person or body that performs or exercises any public function, duty, or power conferred on that person or body by or under the law, and includes—

(a) an organisation named in—

(i) Schedule 1 of the Ombudsmen Act 1975; and

(ii) Schedule 1 of the Official Information Act 1982; and

(b) a local authority or public body named or specified in Schedule 1 of the Local Government Official Information and Meetings Act 1987; and

(c) a foreign public agency

security records—

(a) means papers, documents, and records of any kind, and whether bearing a security classification or not, that are officially made or received—

(i) by an intelligence and security agency in the conduct of its affairs; or

(ii) by any employee of an intelligence and security agency in the course of that employee's official duties; and

(b) includes registers, books, maps, plans, drawings, photographs, cinematographic films, sound recordings, and electronic storage media made or received by an agency or employee of the kind described in paragraph (a); and

(c) includes copies of papers, documents, records, and other things that are security records by virtue of paragraph (a) or (b)

signals intelligence means intelligence gathered or derived from communications and information infrastructures

State Services Commissioner means the State Services Commissioner appointed under section 3 of the State Sector Act 1988

Type 1 intelligence warrant has the meaning given to it by section 47

Type 2 intelligence warrant has the meaning given to it by section 47.

5 Transitional, savings, and related provisions

The transitional, savings, and related provisions set out in Schedule 1 have effect according to their terms.

6 Act binds the Crown

This Act binds the Crown.

Part 2
Intelligence and security agencies

7 New Zealand Security Intelligence Service

(1) There continues to be a New Zealand Security Intelligence Service that specialises in human intelligence activities.

(2) The New Zealand Security Intelligence Service is the same body as the body of that name existing immediately before the commencement of this section.

(3) The New Zealand Security Intelligence Service is a department of State.

Compare: 1969 No 24 s 3

8 Government Communications Security Bureau

(1) There continues to be a department of State called the Government Communications Security Bureau that specialises in signals intelligence and information assurance and cybersecurity activities.

(2) The Government Communications Security Bureau is the same body as the body of that name existing immediately before the commencement of this section.

Compare: 2003 No 9 s 6

Objectives

9 Objectives of intelligence and security agencies

The principal objectives of the intelligence and security agencies are to contribute to—

(a) the protection of New Zealand's national security; and

(b) the international relations and well-being of New Zealand; and

(c) the economic well-being of New Zealand.

Compare: 1969 No 24 s 4AAA(1)(a), (b); 2003 No 9 s 7

Functions

10 Intelligence collection and analysis

(1) It is a function of an intelligence and security agency to—

(a) collect and analyse intelligence in accordance with the New Zealand Government's priorities; and

(b) provide any intelligence collected and any analysis of that intelligence to 1 or more of the following:

(i) the Minister:

(ii) the Chief Executive of the Department of the Prime Minister and Cabinet:

(iii) any person or class of persons (whether in New Zealand or overseas) authorised by the Minister to receive the intelligence and any analysis of that intelligence.

(2) In performing the function referred to in subsection (1)(a), an intelligence and security agency may co-operate with, and provide advice and assistance to,—

(a) any public authority (whether in New Zealand or overseas); and

(b) any other person or class of persons (whether in New Zealand or overseas) authorised by the Minister under subsection (1)(b)(iii).

(3) Before authorising, under subsection (1)(b)(iii), the provision of intelligence and any analysis of that intelligence to any overseas person or class of persons, the Minister must be satisfied that, in providing the intelligence and analysis, the intelligence and security agency will be acting in accordance with New Zealand law and all human rights obligations recognised by New Zealand law.

(4) In this section, **Minister**, in relation to an intelligence and security agency, means the Minister responsible for the intelligence and security agency.

Compare: 2003 No 9 s 8B

11 Protective security services, advice, and assistance

(1) It is a function of an intelligence and security agency to provide protective security services, advice, and assistance to—

(a) any public authority (whether in New Zealand or overseas); and

(b) any person or class of persons (whether in New Zealand or overseas) authorised by the Minister responsible for the intelligence and security agency to receive the services, advice, and assistance.

(2) An intelligence and security agency may provide protective security services, advice, and assistance to any public authority or person or class of persons under subsection (1) in co-operation with any other such public authority or person or class of persons.

(3) In this section, **protective security services, advice, and assistance** means—

(a) services and advice relating to developing and implementing protective security arrangements, including arrangements for—

(i) personnel security (for example, security clearance assessments); and

(ii) information security (for example, information assurance and cybersecurity activities); and

(iii) physical security (for example, making premises secure and protecting classified information); and

(b) assisting with the development and implementation of the arrangements in paragraph (a); and

(c) providing advice about national security risks (for example, national security risks associated with citizenship applications and border security).

Compare: 2003 No 9 s 8B(2)

12 Information assurance and cybersecurity activities

(1) In relation to the Government Communications Security Bureau, the information assurance and cybersecurity activities referred to in paragraph (a)(ii) of the

definition of protective security services, advice, and assistance in section 11(3) are—

(a) providing information assurance and cybersecurity activities to a public authority, person, or class of persons referred to in section 11(1); and

(b) doing everything that is necessary or desirable to protect the security and integrity of communications and information infrastructures of importance to the Government of New Zealand, including identifying and responding to threats or potential threats to those communications and information infrastructures.

(2) Subsection (1)(a) is not limited by subsection (1)(b).

(3) An activity described in subsection (1)(a) may be carried out by the Government Communications Security Bureau—

(a) without an authorisation if—

(i) the activity is a lawful activity; or

(ii) the activity would otherwise be an unlawful activity but is a lawful activity because it is carried out with the lawful consent of the public authority, person, or class of persons; or

(b) with an authorisation if that activity is—

(i) not otherwise a lawful activity; and

(ii) not carried out with the consent of the public authority, person, or class of persons.

(4) An activity described in subsection (1)(b) may be carried out by the Government Communications Security Bureau—

(a) without an authorisation if that activity is lawful; or

(b) with an authorisation if that activity is otherwise unlawful.

(5) Any information obtained by the Government Communications Security Bureau in carrying out information assurance and cybersecurity activities under section 11 without an authorisation may only be used for—

(a) performing its function under section 11:

(b) producing reports related to threats to, or interference with, communications or information infrastructures of importance to the Government of New Zealand and providing those reports to any person or class of persons (whether in New Zealand or overseas) authorised by the Minister for the purpose of this subsection to receive them.

(6) Despite subsection (5), any information obtained by the Government Communications Security Bureau in carrying out information assurance and cybersecurity activities under section 11 may—

(a) be used for any other purpose authorised by an authorisation under Part 4:

(b) if publicly available, be used for any other purpose relevant to its functions.

(7) Before authorising, under subsection (5)(b), any overseas person or class of persons to receive any report or class of reports, the Minister must be satisfied that, in providing the report, the intelligence and security agency will be acting in accordance with New Zealand law and all human rights obligations recognised by New Zealand law.

(8) In this section, **Minister** means the Minister responsible for the Government Communications Security Bureau.

13 Co-operation with other public authorities to facilitate their functions

(1) It is a function of the intelligence and security agencies to—

(a) co-operate with—

(i) each other; and

(ii) the New Zealand Police; and

(iii) the New Zealand Defence Force; and

(b) provide advice and assistance to the New Zealand Police and the New Zealand Defence Force for the purpose of facilitating the performance or exercise of the functions, duties, or powers of those public authorities.

(2) An intelligence and security agency may perform the function under subsection (1)(b)—

(a) only to the extent that the advice and assistance are provided for the purpose of activities that the public authority may lawfully carry out; and

(b) subject to and in accordance with any limitations, restrictions, and protections under which those public authorities perform or exercise their functions, duties, and powers; and

(c) even though the advice and assistance might involve the exercise of powers or the sharing of capabilities that the intelligence and security agency is not, or could not be, authorised to exercise or share in the performance of its other functions.

(3) An intelligence and security agency, in relation to any advice and assistance provided to a public authority under subsection (1)(b), is subject to—

(a) the jurisdiction of any other body or authority to the same extent as the public authority's actions are subject to the other body's or authority's jurisdiction (for example, the Independent Police Conduct Authority in relation to advice and assistance provided to the New Zealand Police); and

(b) the oversight of the Inspector-General.

(4) The Director-General of an intelligence and security agency and an employee of an intelligence and security agency are immune from criminal liability for

any act done under this section in good faith in providing advice and assistance to the New Zealand Police or the New Zealand Defence Force if—

(a) the Director-General or employee reasonably believed that the act was necessary to provide the advice and assistance; and

(b) the act was carried out in a reasonable manner; and

(c) the act could have been lawfully carried out by the New Zealand Police or the New Zealand Defence Force, as the case may be.

Compare: 2003 No 9 s 8C

14 Co-operation with other entities to respond to imminent threat

(1) It is a function of the intelligence and security agencies to co-operate with, and provide advice and assistance to, a person, class of persons, or public authority (whether in New Zealand or overseas) that is responding to an imminent threat to the life or safety of—

(a) any person in New Zealand; or

(b) any New Zealand citizen who is overseas; or

(c) any permanent resident of New Zealand who is overseas; or

(d) any person in an area in respect of which New Zealand has search and rescue responsibilities under international law; or

(e) any person outside the territorial jurisdiction of any country.

(2) An intelligence and security agency may perform this function—

(a) only to the extent that the co-operation, advice, and assistance are necessary to respond to the imminent threat; and

(b) only if the activities carried out in co-operating and providing advice and assistance could not, in any circumstance, be authorised by an intelligence warrant issued for the purpose of performing a function under section 10 or 11; and

(c) subject to the restriction that any information obtained by the agencies in the performance of this function may not be used for any other purpose, except to the extent that the use for that other purpose is authorised by an intelligence warrant issued in the circumstances referred to in section 102(2)(a); and

(d) even though the co-operation, advice, and assistance might involve the exercise of powers or the sharing of capabilities that the agency is not, or could not be, authorised to exercise or share in the performance of its other functions.

(3) As soon as practicable after undertaking any activity in the performance of its function under this section, the Director-General of an intelligence and security agency must provide details of that activity to—

(a) the Minister responsible for the intelligence and security agency; and

(b) the Inspector-General.

15 Additional functions

In addition to the functions specified in sections 10 to 14, the intelligence and security agencies have any other function conferred or imposed on them by or under any other enactment.

Compare: 2003 No 9 s 8(5)

16 Functions of intelligence and security agencies do not include enforcement

It is not the function of an intelligence and security agency to enforce measures for national security except as may be required—

(a) in connection with any information assurance and cybersecurity activities that are carried out by the Government Communications Security Bureau; or

(b) in the course of performing its function under section 13; or

(c) under any other enactment.

Compare: 1969 No 24 s 4(2)

Duties

17 General duties applying when intelligence and security agency performing functions

When performing its functions, an intelligence and security agency must act—

(a) in accordance with New Zealand law and all human rights obligations recognised by New Zealand law; and

(b) in the performance of its operational functions, independently and impartially; and

(c) with integrity and professionalism; and

(d) in a manner that facilitates effective democratic oversight.

18 Specific duties of Director-General of an intelligence and security agency

The Director-General of an intelligence and security agency must take all reasonable steps to ensure that—

(a) the activities of the agency are—

(i) limited to those that are relevant to the performance of its functions; and

(ii) kept free from any influence or consideration that is not relevant to the performance of its functions; and

(iii) politically neutral (for example, the activities are not carried out for the purpose of promoting or harming the interests of any political party or candidate); and

(b) any co-operation with foreign jurisdictions and international organisations in the performance of any of the agency's functions is in accordance with New Zealand law and all human rights obligations recognised by New Zealand law.

Compare: 1969 No 24 s 4AA(1); 2003 No 9 s 8D(3)

19 Activities of intelligence and security agency not to limit freedom of expression

The exercise by any person in New Zealand or any class of persons in New Zealand of their right to freedom of expression under the law (including the right to advocate, protest, or dissent) does not of itself justify an intelligence and security agency taking any action in respect of that person or class of persons.

Compare: 1969 No 24 s 2(2)

20 Director-General of an intelligence and security agency to consult Leader of the Opposition

The Director-General of an intelligence and security agency must regularly consult the Leader of the Opposition for the purpose of keeping the Leader of the Opposition informed about matters relating to the agency's functions.

Compare: 1969 No 24 s 4AA(3); 2003 No 9 s 8D(4)

Part 3
Covert activities of intelligence and security agencies

Subpart 1—Assumed identities

21 Purpose of subpart

The purpose of this subpart is to enable an employee of an intelligence and security agency to acquire an assumed identity, use an assumed identity, or maintain an assumed identity for the purposes of—

(a) facilitating the ability of that intelligence and security agency to carry out its activities while maintaining the secrecy of those activities:

(b) protecting the identity of the employee.

22 Interpretation

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

access, in relation to information, means to do any or all of the following:

(a) inspect the information:

(b) copy the information, or any part of the information:

(c) obtain a printout of the information

acquire an assumed identity means to acquire evidence of the assumed identity, and includes taking steps towards acquiring evidence of the identity

agency includes—

(a) a Minister; and

(b) a statutory officer; and

(c) a government agency; and

(d) a private sector agency

assumed identity, in relation to an authorised person, means an identity the person assumes that—

(a) is not the person's real identity; or

(b) involves a false or misleading representation about 1 or more aspects of the person's real identity

authorised person means an employee of an intelligence and security agency who is authorised under section 23 to do 1 or more of the following:

(a) acquire an assumed identity:

(b) use an assumed identity:

(c) maintain an assumed identity

employee means any person—

(a) who is, or will be, an employee of an intelligence and security agency; and

(b) who is approved by the Director-General of an intelligence and security agency to carry out activities for that agency

evidence, in relation to an identity, means any documentation (whether physical or electronic) or thing that—

(a) has a tendency to prove, or purports to establish, the identity (for example, a birth certificate, certificate of New Zealand citizenship, passport, or driver licence); or

(b) can be used to support the proof or establishment of the identity (for example, a bank card or staff identity card)

false document includes a false document within the meaning of section 255 of the Crimes Act 1961

government agency means—

(a) a Crown entity within the meaning of section 7 of the Crown Entities Act 2004; and

(b) a department

maintain, in relation to an assumed identity, includes taking steps towards maintaining the identity

private sector agency means an entity that is not a government agency

statutory officer means a person who—

(a) holds or performs the duties of an office established by an enactment; or

(b) performs duties expressly conferred on that person by an enactment by virtue of that person's office.

(2) For the purposes of this subpart,—

(a) a record is **publicly available** if an agency, in the ordinary course of its activities, makes the record available to the public for inspection or searching; but

(b) a record is not to be treated as publicly available merely because it is or may be required to be made available under the Official Information Act 1982.

23 Assumed identity may be acquired, used, and maintained

(1) An employee of an intelligence and security agency may do 1 or more of the following if the employee is authorised to do so by the Director-General of the intelligence and security agency:

(a) acquire an assumed identity:

(b) use an assumed identity:

(c) maintain an assumed identity.

(2) The Director-General may authorise the acquiring, use, or maintenance of an assumed identity only if he or she is satisfied that the acquiring, use, or maintenance of the assumed identity is necessary for a purpose specified in section 21.

(3) An employee (as defined in section 4) may make a false document for use in supporting the use or maintenance of an assumed identity if the Director-General is satisfied that—

(a) the making and use of the false document are necessary for a purpose specified in section 21; and

(b) the document is of a kind that is not ordinarily issued or given by a Minister or government agency.

(4) Nothing in this subpart prevents 2 or more authorised persons from acquiring, using, or maintaining the same assumed identity.

24 Use of assumed identity

(1) The power for an employee to use an assumed identity includes the power to use the identity as if it were the employee's own identity, for example, to use or assume the identity—

(a) to acquire, or take steps towards acquiring, evidence of the assumed identity (with or without assistance under section 26):

(b) to establish, maintain, and operate a legal entity (with or without assistance under section 36 or 37).

(2) Subsection (1)(a) and (b) applies only to the extent that a person of that identity could lawfully do the things referred to in those paragraphs.

(3) A thing is not unlawful for the purposes of subsection (2) merely because it involves a false or misleading representation about the employee's identity.

(4) The power for an employee to use an assumed identity also includes the power to use a false document made under section 23(3).

25 Request for assistance to acquire, use, and maintain assumed identity

(1) The Director-General of an intelligence and security agency may request any other agency to assist an authorised person to do 1 or more of the following:

(a) acquire an assumed identity:

(b) use an assumed identity:

(c) maintain an assumed identity.

(2) A request must—

(a) provide details of—

(i) the authorised person that are necessary to enable the agency to provide the assistance; and

(ii) the assumed identity being acquired (or that has been acquired) for the authorised person; and

(iii) the assistance being sought from the agency; and

(iv) the specific evidence of the assumed identity that the agency is requested to issue or give; and

(b) confirm that the request is made for either or both of the purposes specified in section 21.

26 Assistance to acquire, use, and maintain assumed identity

(1) An agency that receives a request under section 25 may—

(a) grant the request; or

(b) decline the request in accordance with subsections (2) and (3).

(2) The agency may decline the request if—

(a) it is not satisfied that an authorised person will use the assumed identity appropriately; or

(b) it otherwise considers that it is appropriate to decline the request.

(3) The agency must, in considering the matter under subsection (2), have regard to—

(a) the purpose of this subpart; and

(b) every relevant ministerial policy statement, to the extent that it is known to the agency; and

(c) the protections that are or will be in place for the purpose of ensuring that an authorised person will use the assumed identity appropriately; and

(d) any other matters the agency thinks relevant.

(4) In granting the request, the agency may do anything to assist the authorised person, including—

(a) issuing or giving to the authorised person evidence of the assumed identity that is of a kind ordinarily issued or given by the agency; and

(b) omitting, amending, replacing, or inserting any information in any register or other publicly available records (including making changes to an assumed identity and, if necessary, creating other identities to support an assumed identity); and

(c) omitting, amending, replacing, or inserting operational or administrative information, as necessary, so that it supports the evidence or information described in paragraphs (a) and (b).

27 Cancellation of evidence of assumed identity

(1) An agency must cancel evidence of an assumed identity if directed in writing to do so by the Director-General of the intelligence and security agency who requested assistance in relation to the assumed identity under section 25.

(2) The cancellation must be made in the manner set out in the direction from the Director-General.

(3) The manner of cancellation may include, for example, 1 or more of the following:

(a) omitting, amending, replacing, or inserting information in a register or other publicly available records:

(b) preventing or restricting access to any information in a register or other publicly available records:

(c) omitting, amending, replacing, or inserting operational or administrative information, as necessary, so that it supports the actions under paragraphs (a) and (b).

28 Provisions do not require destruction of certain information

(1) Sections 26(4) and 27(3)—

(a) do not require an agency to destroy information if the agency is under an obligation to retain the information; and

(b) do not require or authorise the disposal of a record for the purposes of the Public Records Act 2005.

(2) Section 29 is subject to this section.

29 Non-compliance with enactments, policies, and practices

Evidence of an assumed identity may be issued, given, changed, or cancelled by an agency, and assistance may otherwise be given under this subpart, without complying with any enactment, policy, or practice that, in relation to the action taken by the agency, requires compliance with any specified or prescribed—

(a) criteria or standards:

(b) requirements:

(c) process or procedure.

30 Restrictions on access to information about process for obtaining assistance, etc

(1) The purpose of this section is to prevent access to information about the process for obtaining assistance under section 25 or 26 or compliance with a direction under section 27 where the access may compromise the secrecy relating to the acquisition, use, or maintenance of an assumed identity.

(2) An agency must not permit any person (**person A**) to access a request made under section 25, a direction given under section 27, or any other information within its possession or control relating to the process for obtaining or giving the assistance or compliance with the direction (whether or not the request has been or will be granted or the direction has been complied with).

(3) Subsection (2) does not apply if—

(a) person A is an authorised person; or

(b) person A is the Director-General of an intelligence and security agency; or

(c) person A is the Inspector-General of Intelligence and Security; or

(d) it is necessary for person A to have access to the information in order for the assistance to be given or for the direction to be complied with; or

(e) an authorised person has given the agency written consent to person A having access to the information; or

(f) the Director-General of the intelligence and security agency who made the request or gave the direction has given the agency written consent to person A having access to the information; or

(g) a court has ordered that person A be permitted access to the information for any specified purpose (for example, for the purposes of a prosecution in relation to the making of a false statement).

(4) If the agency receives an access request, the agency must, as soon as practicable, notify the Director-General of the intelligence and security agency who made the request or gave the direction.

(5) The notice must include—

(a) the date and time of the access request:

(b) the name, address, and contact details (if known) of the person who made the access request:

(c) the information sought to be accessed.

(6) Consent under subsection (3)(e) or (f) may be given for a class of persons that includes person A without referring to person A by name.

(7) In this section, **access request** means a request for access to any information referred to in subsection (2).

31 Immunity of persons assisting and of employee of agency in making false documents

(1) A person is protected from civil and criminal liability, however it may arise, in relation to any act that the person does, or omits to do, in good faith and with reasonable care in the course of complying with—

(a) a request made under section 25; or

(b) a direction given under section 27.

(2) An employee of an intelligence and security agency is protected from civil and criminal liability, however it may arise, in relation to any act that the employee does, or omits to do, in good faith and with reasonable care in the course of making a false document under section 23(3).

(3) In subsection (2), **employee** has the same meaning as in section 4.

32 Immunity of authorised persons

(1) An authorised person is protected from civil and criminal liability, however it may arise, for any act that the authorised person does, or omits to do, in good faith and with reasonable care—

(a) in the course of acquiring, using, or maintaining an assumed identity in accordance with an authorisation given under section 23; and

(b) in accordance with any protections referred to in section 26(3)(c).

(2) Subsection (1) does not apply to—

(a) anything done, or not done, by an authorised person in breach of any contractual arrangement (unless the breach is a necessary consequence of using or maintaining the assumed identity); or

(b) anything done by an authorised person if a particular qualification is needed to do the thing and the person does not have that qualification (for example, a person who is not qualified to fly a plane is not authorised to fly even though he or she has acquired a pilot's licence under an assumed identity).

(3) Subsection (2)(b) applies whether or not the authorised person has acquired, as evidence of an assumed identity, a document that indicates that he or she has that qualification.

(4) In this section, **qualification** means a qualification, licence, registration, or other approval.

Compare: Crimes Act 1914 s 15KT (Aust)

Subpart 2—Corporate identities

33 Purpose of subpart

The purpose of this subpart is to enable an intelligence and security agency to create and maintain a legal entity through which it may conduct transactions for the purpose of facilitating the ability of the agency to carry out its activities while maintaining the secrecy of those activities.

34 Interpretation

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

access, in relation to information, means to do any or all of the following:

(a) inspect the information:

(b) copy the information, or any part of the information:

(c) obtain a printout of the information

agency means—

(a) the chief executive of a department:

(b) a department:

(c) a Registrar or Deputy Registrar appointed under, or in accordance with, any enactment:

(d) a Board established under section 8 of the Charities Act 2005:

(e) a regulatory authority

entity means—

(a) an unincorporated body:

(b) a body corporate:

(c) a corporation sole:

(d) a trust

evidence, in relation to a legal identity, status, capacity, or unique identifier, means any documentation (whether physical or electronic) or thing that—

(a) has a tendency to prove, or purports to establish, the identity, status, or capacity or that the unique identifier has been allocated; or

(b) can be used to support the proof or establishment of the identity, status, or capacity or that the unique identifier has been allocated

regulatory authority means any authority having statutory functions that include any or all of the following:

(a) monitoring the business community:

(b) regulating any business sector:

(c) conducting inquiries and investigations into any business activity or practice:

(d) enforcing legislation that relates to business activities.

(2) For the purposes of this subpart,—

(a) a record is **publicly available** if an agency, in the ordinary course of its activities, makes the record available to the public for inspection or searching; but

(b) a record is not to be treated as publicly available merely because it is or may be required to be made available under the Official Information Act 1982.

35 Request for corporate identity, status, etc

(1) The Director-General of an intelligence and security agency may, if he or she is satisfied that it is necessary for the purpose specified in section 33, request any other agency to do any of the following:

(a) confer a legal identity by forming or incorporating an entity (for example, incorporate a company or a charitable trust board):

(b) confer on an entity any legal status or capacity (for example, register an entity as a charitable entity or financial service provider):

(c) allocate to an entity a unique identifier (for example, allocate an entity a New Zealand Business Number or a goods and services tax registration number):

(d) provide evidence of—

(i) any legal identity, status, or capacity having been conferred on an entity (for example, issue a certificate of incorporation):

(ii) any unique identifier having been allocated to an entity (for example, record an entity's New Zealand Business Number in the New Zealand Business Number Register):

(e) perform any action that is ancillary to, or consequential on, any of the actions specified in paragraphs (a) to (d).

(2) A request must—

(a) provide details of—

(i) the entity or proposed entity that is the subject of the request that are necessary to enable the agency to take the requested action; and

(ii) the action that the agency is being requested to take in respect of the entity or proposed entity; and

(b) confirm that the request is made for the purpose specified in section 33.

36 Conferring corporate identity, status, etc

(1) An agency that receives a request under section 35 may—

(a) grant the request; or

(b) decline the request in accordance with subsections (2) and (3).

(2) An agency may decline the request if—

(a) it is not satisfied that the intelligence and security agency will use appropriately—

(i) the legal identity, status, or capacity to be conferred on the entity or proposed entity; or

(ii) the unique identifier to be allocated to the entity or proposed entity; or

(b) it otherwise considers that it is appropriate to decline the request.

(3) The agency must, in considering the matter under subsection (2), have regard to—

(a) the purpose of this subpart; and

(b) every relevant ministerial policy statement, to the extent that it is known to the agency; and

(c) the protections that are or will be in place for the purpose of ensuring that the intelligence and security agency will use appropriately—

(i) the legal identity, status, or capacity conferred on the entity or proposed entity; or

(ii) the unique identifier allocated to the entity or proposed entity; and

(d) any other matters the agency thinks relevant.

(4) In granting the request, the agency may do anything to take an action referred to in section 35, including—

(a) omitting, amending, replacing, or inserting any information in any register or other publicly available records (including, if necessary, creating assumed identities to support the action); and

(b) omitting, amending, replacing, or inserting operational or administrative information, as necessary, so that it supports the information in paragraph (a).

37 Maintaining corporate identity, status, or capacity

(1) The Director-General of an intelligence and security agency may, for the purpose specified in section 33, request an agency to assist with maintaining the legal identity, status, or capacity that has been conferred under section 36.

(2) An agency that receives a request under subsection (1) may—

(a) grant the request; or

(b) decline the request if it is not satisfied that it is appropriate to provide the assistance.

(3) The agency must, in considering the matter under subsection (2)(b), have regard to—

(a) the purpose of this subpart; and

(b) every relevant ministerial policy statement, to the extent that it is known to the agency; and

(c) the impact on any members of the public; and

(d) any other matters the agency thinks relevant.

(4) In granting the request, the agency may do anything to give the assistance, including—

(a) omitting, amending, replacing, or inserting any information in any register or other publicly available records (including making changes to the legal identity, status, or capacity and, if necessary, creating assumed identities to support a legal identity, status, or capacity); and

(b) omitting, amending, replacing, or inserting operational or administrative information, as necessary, so that it supports the information described in paragraph (a).

38 Dissolution or deregistration, etc, of entity

(1) A Director-General of an intelligence and security agency who made a request under section 35 or 37 may, at any time, direct an agency that took any action of the kind specified in section 35(1) or 37(4) in response to his or her request to subsequently take steps necessary to—

(a) negate the effect of the earlier action (for example, remove a company from the register of companies); and

(b) expunge any record of that earlier action having been taken.

(2) The steps must be taken in the manner set out in the direction from the Director-General.

(3) The manner of taking those steps may include, for example, 1 or more of the following:

(a) omitting, amending, replacing, or inserting information in a register or any other publicly available records:

(b) preventing or restricting access to any information in a register or any other publicly available records:

(c) omitting, amending, replacing, or inserting operational or administrative information, as necessary, so that it supports the actions under paragraphs (a) and (b).

39 Provisions do not require destruction of certain information

(1) Sections 36(4), 37(4), and 38(3)—

(a) do not require an agency to destroy information if the agency is under an obligation to retain the information; and

(b) do not require or authorise the disposal of a record for the purposes of the Public Records Act 2005.

(2) Section 40 is subject to this section.

40 Non-compliance with enactments, policies, and practices

Compliance with a request made under section 35, 37, or 42 or a direction given under section 38 may be made without complying with any enactment, policy, or practice that, in relation to the action taken by the agency, requires compliance with any specified or prescribed—

(a) criteria or standards:

(b) requirements:

(c) process or procedure.

41 Restrictions on access to information about process for obtaining assistance, etc

(1) The purpose of this section is to prevent access to information about the process for obtaining assistance under sections 35 to 37, an exemption under section 42, or compliance with a direction under section 38 where the access may compromise the secrecy relating to the creation or maintenance of the legal entity.

(2) An agency must not permit any person (**person A**) to access a request made under section 35, 37, or 42, a direction given under section 38, or any other information within its possession or control relating to the process for obtaining or giving the assistance or exemption or compliance with the direction (whether or not the request or exemption has been or will be granted or the direction has been complied with).

(3) Subsection (2) does not apply if—

(a) person A is the entity; or

(b) person A is the Director-General of an intelligence and security agency; or

(c) person A is the Inspector-General of Intelligence and Security; or

(d) it is necessary for person A to have access to the information in order for the assistance to be given, for the exemption to be granted, or for the direction to be complied with; or

(e) the Director-General of an intelligence and security agency who made the request or gave the direction has consented in writing to person A having access to the information; or

(f) a court has ordered that person A be permitted access to the information for any specified purpose (for example, for the purposes of proceedings relating to a transaction entered into by the entity).

(4) If an agency receives an access request, the agency must, as soon as practicable, notify the Director-General of the intelligence and security agency who made the request or gave the direction.

(5) The notice must include—

(a) the date and time of the access request; and

(b) the name, address, and contact details (if known) of the person who made the access request; and

(c) the information sought to be accessed.

(6) Consent under subsection (3)(e) may be given for a class of persons that includes person A without referring to person A by name.

(7) In this section, **access request** means a request for access to any information referred to in subsection (2).

42 Entity or officer exempt from complying with legal requirements, etc

(1) An entity that has been conferred with any legal identity, status, or capacity under section 36, or an officer of that entity, may be exempted from complying with any requirements or duties imposed by or under any enactment that apply to an entity having that legal identity, status, or capacity or to an officer of such an entity.

(2) An exemption from complying with any requirement or duty may be granted only—

(a) by—

(i) the agency responsible for ensuring compliance with, or enforcing, that requirement or duty; or

(ii) the agency that is the department responsible for the administration of the enactment referred to in subsection (1); and

(b) on a request made by the Director-General of an intelligence and security agency.

(3) An agency may grant an exemption only if the agency is satisfied that granting the exemption—

(a) will not have a significant negative impact on any members of the public; and

(b) is otherwise appropriate.

(4) The agency must, before granting an exemption, have regard to—

(a) whether, in the circumstances, compliance with the enactment referred to in subsection (1)—

(i) would require the entity or officer to comply with a duty or requirement that is unduly onerous or burdensome; or

(ii) is not necessary in order to fulfil the purpose for which the duty or requirement was imposed; and

(b) whether the extent of the exemption is not broader than is reasonably necessary to address the matters that gave rise to the exemption; and

(c) the purposes of the enactment referred to in subsection (1); and

(d) any other matters the agency thinks relevant.

(5) An exemption must be granted by notice in writing and may be subject to any terms and conditions specified by the agency.

(6) An exemption is not—

(a) a legislative instrument for the purposes of the Legislation Act 2012; or

(b) a disallowable instrument for the purposes of the Legislation Act 2012.

(7) In this section and section 45(2)(g), **officer**, in relation to an entity, means—

(a) a director within the meaning of section 6(1) of the Financial Markets Conduct Act 2013; and

(b) a person who is not a director but who occupies a position that allows the person to exercise significant influence over the management or administration of the entity (for example, a chief executive or a chief financial officer).

43 Immunity of persons complying with request or direction

A person is protected from civil and criminal liability, however it may arise, in relation to any act that the person does, or omits to do, in good faith and with reasonable care in the course of complying with—

(a) a request made under section 35, 37, or 42; or

(b) a direction given under section 38.

44 Immunity of entity

(1) An entity that has been conferred with any legal identity, status, or capacity under section 36 is protected from civil and criminal liability, however it may arise, for any act that the entity does, or omits to do, in good faith and with reasonable care—

(a) in the course of carrying out its activities; and

(b) in accordance with any protections referred to in section 36(3)(c).

(2) Subsection (1) does not apply to—

(a) anything done, or not done, by an entity in breach of any contractual arrangement (unless the breach is a necessary consequence of creating or maintaining the relevant legal identity, status, or capacity); or

(b) anything done by an entity if a particular qualification is needed to do the thing and the entity does not have that qualification (for example, an entity that is not qualified to provide a financial service is not authorised to provide that service even though it has acquired a licence to perform that service).

(3) Subsection (2)(b) applies whether or not the entity has acquired a document that indicates that it has that qualification.

(4) In this section, **qualification** means a qualification, licence, registration, or other approval.

Subpart 3—Register of assumed identities and legal entities created or maintained

45 Register of assumed identities and legal entities created or maintained

(1) The Director-General of an intelligence and security agency must keep a register of assumed identities acquired, and legal entities created or maintained, under this Part by the agency.

(2) The register must include,—

(a) for each authorisation given by the Director-General under section 23, details of—

(i) the assumed identity that was being acquired (or that had been acquired) for the authorised person; and

(ii) the scope of the authorisation; and

(iii) the person who was authorised to acquire, maintain, or use the assumed identity; and

(iv) each false document for use in supporting the use or maintenance of the assumed identity that was created under section 23(3); and

(b) for each request for assistance under section 25, details of—

(i) the date of the request and of the agency to which the request was made; and

(ii) the authorised person to whom the request relates; and

(iii) the assumed identity that was being acquired (or that had been acquired) for the authorised person; and

(iv) the assistance that was sought from the agency; and

(v) the specific evidence of the assumed identity that the agency was requested to issue or give; and

(vi) whether the agency granted or refused the request; and

(c) for each direction given under section 27, details of—

(i) the date of the direction and of the agency to which the direction was given; and

(ii) the assumed identity to which the direction relates; and

(iii) the evidence that was required to be cancelled and the manner of cancellation that is set out in the direction; and

(d) for each request made under section 35, details of—

(i) the date of the request and of the agency to which the request was made; and

(ii) the entity or proposed entity that was the subject of the request; and

(iii) the action that the agency was requested to take in respect of the entity or proposed entity; and

(iv) whether the agency granted or refused the request; and

(e) for each request made under section 37, details of—

(i) the date of the request and of the agency to which the request was made; and

(ii) the entity or proposed entity that was the subject of the request; and

(iii) the action that the agency was requested to take in respect of the entity or proposed entity; and

(iv) whether the agency granted or refused the request; and

(f) for each direction given under section 38, details of—

(i) the date of the direction and of the agency to which the direction was given; and

(ii) the entity to which the direction relates; and

(iii) the steps required to be taken and the manner of taking those steps that is set out in the direction; and

(g) for each request made under section 42, details of—

(i) the date of the request and of the agency to which the request was made; and

(ii) the entity that was the subject of the request; and

(iii) each officer to whom the exemption relates (if any); and

(iv) the exemption that the agency was requested to grant; and

(v) whether the agency granted or refused the request; and

(vi) the terms and conditions of the exemption that was granted (if any).

(3) All information required to be kept under this section by the Director-General of an intelligence and security agency may be accessed at any time by—

(a) the Minister responsible for the intelligence and security agency:

(b) the Inspector-General.

Part 4
Authorisations

46 Purpose of Part

The purpose of this Part is to establish an authorisation regime for the intelligence and security agencies that—

(a) authorises as lawful the carrying out of an activity by an intelligence and security agency that would otherwise be unlawful, if certain criteria are satisfied; and

(b) confers on an intelligence and security agency specified powers for the purpose of giving effect to an authorisation.

47 Interpretation

In this Part, unless the context otherwise requires,—

access an information infrastructure means instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources or features of an information infrastructure (including features that provide audio or visual capability)

authorisation means—

(a) an intelligence warrant:

(b) an authorisation given under section 78:

(c) a removal warrant:

(d) a practice warrant

authorised activity means an activity that is authorised by an authorisation

authorising Minister, in relation to an application for an intelligence warrant, means,—

(a) in the case of an application under section 55, the Minister responsible for the intelligence and security agency making the application; or

(b) in the case of a joint application under section 56,—

(i) the Minister responsible for the intelligence and security agencies, if the same Minister is responsible for each agency; or

(ii) the Ministers responsible for the intelligence and security agencies, if a different Minister is responsible for each agency

communication includes signs, signals, impulses, writing, images, sounds, information, or data that a person or machine produces, sends, receives, processes, or holds in any medium

electronic tracking means the use of electronic means for the purpose of ascertaining the location, or tracking the movement, of a person or thing

incidentally obtained information means information that—

(a) is obtained in the course of performing a function under section 10 or 11; but

(b) is not relevant to either of those functions

intelligence warrant means—

(a) a Type 1 intelligence warrant; and

(b) a Type 2 intelligence warrant

intercept, in relation to a private communication, includes to hear, listen to, record, monitor, acquire, or receive the communication, or acquire its substance, meaning, or sense,—

(a) while it is taking place; or

(b) in the course of transmission

interception device means any electronic, mechanical, electromagnetic, optical, or electro-optical instrument, apparatus, equipment, or other device that is used or is capable of being used to intercept communications

practice warrant means a warrant issued under section 93

private activity means an activity that, in the circumstances, any of the participants in it ought reasonably to expect to be observed or recorded by no one except the participants

private communication—

(a) means a communication (whether in oral or written form, or in the form of a telecommunication, or otherwise) made in circumstances that may reasonably be taken to indicate that any party to the communication desires it to be confined to the parties to the communication; but

(b) does not include a communication of that kind occurring in circumstances in which any party to the communication ought reasonably to expect that the communication may be intercepted by some other person without having the express or implied consent of any party to do so

private premises means a private residence, a marae, or any other premises to which members of the public do not usually or frequently have access

remote access search means a search of a thing that does not have a physical address that a person can enter and search

removal warrant means a warrant issued under section 85

search includes a remote access search

seize includes to take, remove, and copy, and **seizing** and **seizure** have corresponding meanings

serious crime,—

(a) for the purposes of section 58, means,—

(i) in relation to New Zealand, any offence punishable by 3 or more years' imprisonment; and

(ii) in relation to any other country, any offence that, if it occurred in New Zealand, would be an offence punishable by 3 or more years' imprisonment; and

(b) for the purposes of section 104, means,—

(i) in relation to New Zealand, any offence punishable by 2 or more years' imprisonment; and

(ii) in relation to any other country, an offence that, if it occurred in New Zealand, would be an offence punishable by 2 or more years' imprisonment

situation of urgency means a situation where—

(a) there is an imminent threat to the life or safety of any person; or

(b) the delay associated with applying for the issue of an intelligence warrant in the usual way is likely to materially prejudice the protection of New Zealand's national security

surveillance includes—

(a) visual surveillance; and

(b) electronic tracking

thing includes—

(a) a vehicle:

(b) an information infrastructure (for example, a mobile phone, a website, or a data storage device)

Type 1 intelligence warrant means an intelligence warrant issued under section 58 or 59

Type 2 intelligence warrant means an intelligence warrant issued under section 60

visual surveillance means the observation of private activity in private premises, with or without the use of a visual surveillance device, and includes any recording of that observation

visual surveillance device has the meaning given to it by section 3(1) of the Search and Surveillance Act 2012.

48 Authorisation not required to carry out lawful activity

An intelligence and security agency may carry out a lawful activity in the performance or exercise of any function, duty, or power without an authorisation.

49 Authorisation required to carry out otherwise unlawful activity

(1) An intelligence and security agency may carry out an otherwise unlawful activity only if that activity is an authorised activity.

(2) An intelligence and security agency may not, without an authorisation, request a government of, or an entity in, another jurisdiction to carry out an activity that would be an unlawful activity if it were carried out by the intelligence and security agency.

(3) An authorised activity may lawfully be carried out by an intelligence and security agency despite anything to the contrary in any other enactment.

50 Duty to act only as authorised

The Director-General of an intelligence and security agency must take all reasonable steps to ensure that, in relation to the carrying out of an otherwise unlawful activity, the intelligence and security agency—

(a) acts only within the scope of an authorisation; and

(b) carries out only authorised activities; and

(c) exercises only powers necessary for carrying out authorised activities.

51 Request for assistance to give effect to authorisations

(1) The Director-General of an intelligence and security agency may request assistance with giving effect to an authorisation from—

(a) the New Zealand Police; or

(b) any other organisation; or

(c) any person.

(2) A request must—

(a) specify the assistance required; and

(b) be recorded in writing.

(3) A person who assists is subject to the control of the Director-General of the intelligence and security agency and may exercise the same powers as the intelligence and security agency.

(4) A person who assists has the same immunities as an employee of an intelligence and security agency (*see* section 86 of the State Sector Act 1988 and section 111 of this Act).

(5) In this section, **organisation** includes a body corporate, an unincorporated body, an association of persons, a department, and a Crown entity or other instrument of the Crown.

Compare: 1969 No 24 s 4D

Subpart 1—Intelligence warrants

Types of intelligence warrants

52 Types of intelligence warrant

There are 2 types of intelligence warrants, as follows:

(a) Type 1 intelligence warrants:

(b) Type 2 intelligence warrants.

53 Type 1 intelligence warrant

A Type 1 intelligence warrant authorises an intelligence and security agency to carry out an otherwise unlawful activity for the purpose of collecting information about, or to do any other thing directly in relation to,—

(a) any person who is—

(i) a New Zealand citizen; or

(ii) a permanent resident of New Zealand; or

(b) a class of persons that includes a person who is—

(i) a New Zealand citizen; or

(ii) a permanent resident of New Zealand.

54 Type 2 intelligence warrant

A Type 2 intelligence warrant authorises an intelligence and security agency to carry out an otherwise unlawful activity for the purpose of collecting information, or to do any other thing, in circumstances where a Type 1 warrant is not required.

Application and issue of intelligence warrants

55 Application for issue of intelligence warrant

(1) An application for the issue of an intelligence warrant must be made in writing by the Director-General of an intelligence and security agency and—

(a) state the type of intelligence warrant applied for; and

(b) set out details of the activity proposed to be carried out under the warrant; and

(c) set out the grounds on which the application is made (including the reasons why the legal requirements for issuing the warrant are believed to be satisfied); and

(d) contain a statement in which the Director-General making the application confirms that all of the information set out in the application is true and correct.

(2) An application for a Type 1 intelligence warrant must be made to—

(a) the authorising Minister; and

(b) the Chief Commissioner of Intelligence Warrants.

(3) An application for a Type 2 intelligence warrant must be made to the authorising Minister.

56 Joint application for intelligence warrant

The Director-General of Security and the Director-General of the Government Communications Security Bureau may jointly apply for the issue of an intelligence warrant.

57 Issue of Type 1 intelligence warrant

(1) A Type 1 intelligence warrant is issued jointly by—

(a) the authorising Minister; and

(b) a Commissioner of Intelligence Warrants.

(2) A Type 1 intelligence warrant may only be issued in accordance with section 58 or 59.

58 Issue of Type 1 intelligence warrant to contribute to protection of national security

(1) A Type 1 intelligence warrant may be issued to the Director-General of an intelligence and security agency if the authorising Minister and a Commissioner of Intelligence Warrants are satisfied—

(a) that the issue of the Type 1 intelligence warrant will enable the intelligence and security agency to carry out an activity that—

(i) is necessary to contribute to the protection of national security; and

(ii) identifies, enables the assessment of, or protects against any of the harms specified in subsection (2); and

(b) that the additional criteria in section 61 are met.

(2) The harms referred to in subsection (1)(a)(ii) are—

(a) terrorism or violent extremism:

(b) espionage or other foreign intelligence activity that—

(i) is directed at a New Zealand interest (whether or not that interest is in New Zealand):

(ii) is carried out by a person who is a New Zealand citizen or permanent resident of New Zealand (whether or not that person is in New Zealand):

(iii) occurs in New Zealand (whether or not directed at a New Zealand interest):

(c) sabotage (within the meaning of section 79 of the Crimes Act 1961):

(d) proliferation of weapons of mass destruction:

(e) anything that may be relevant to serious crime and that—

(i) originates outside New Zealand or is influenced from outside New Zealand; or

(ii) involves the movement of money, goods, or people—

(A) within a country outside New Zealand; or

(B) from a country outside New Zealand to New Zealand or to any other country; or

(iii) has the potential to damage New Zealand's international relations or economic well-being:

(f) threats to, or interference with, information (including communications) or information infrastructure of importance to the Government of New Zealand:

(g) threats to—

(i) international security that have the potential to impact adversely on New Zealand's interests:

(ii) the operations of the Government of New Zealand:

(iii) the sovereignty of New Zealand, including New Zealand's territorial and border integrity and its right to manage or control its natural resources.

59 Issue of Type 1 intelligence warrant to contribute to New Zealand's international relations or economic well-being

(1) A Type 1 intelligence warrant may be issued to the Director-General of an intelligence and security agency if the authorising Minister and a Commissioner of Intelligence Warrants are satisfied of the matters in subsection (2).

(2) The matters are—

(a) that the issue of the Type 1 intelligence warrant will enable the intelligence and security agency to carry out an activity that will contribute to—

(i) the international relations and well-being of New Zealand; or

(ii) the economic well-being of New Zealand; and

(b) that there are reasonable grounds to suspect that—

(i) a person referred to in section 53(a) in respect of whom the activity is proposed to be carried out is acting, or purporting to act, for or on behalf of—

(A) a foreign person; or

(B) a foreign organisation; or

(C) a designated terrorist entity; or

(ii) any New Zealand persons within a class of persons referred to in section 53(b) in respect of whom the activity is proposed to be carried out are employed by, or are members of,—

(A) a foreign government; or

(B) a designated terrorist entity; and

(c) that the additional criteria in section 61 are met.

60 Issue of Type 2 intelligence warrant

(1) A Type 2 intelligence warrant is issued by the authorising Minister.

(2) A Type 2 intelligence warrant may be issued to the Director-General of an intelligence and security agency only if the authorising Minister is satisfied of the matters in subsection (3).

(3) The matters are—

(a) that the issue of the Type 2 intelligence warrant will enable the intelligence and security agency to carry out an activity that—

(i) is necessary to contribute to the protection of national security; or

(ii) will contribute to—

(A) the international relations and well-being of New Zealand; or

(B) the economic well-being of New Zealand; and

(b) that the activity is not in respect of a person, or class of persons, for which a Type 1 warrant is required; and

(c) that the additional criteria in section 61 are met.

61 Additional criteria for issue of intelligence warrant

The additional criteria for the issue of an intelligence warrant referred to in sections 58(1)(b), 59(2)(c), and 60(3)(c) are that—

(a) the carrying out of the otherwise unlawful activity (a **proposed activity**) by an intelligence and security agency is necessary to enable the agency to perform a function under section 10 or 11; and

(b) the proposed activity is proportionate to the purpose for which it is to be carried out; and

(c) the purpose of the warrant cannot reasonably be achieved by a less intrusive means; and

(d) there are satisfactory arrangements in place to ensure that—

(i) nothing will be done in reliance on the intelligence warrant beyond what is necessary and reasonable for the proper performance of the function under section 10 or 11; and

(ii) all reasonably practicable steps will be taken to minimise the impact of the proposed activity on any members of the public; and

(iii) any information obtained in reliance on the intelligence warrant will be retained, used, and disclosed only in accordance with this Act or any other enactment.

Compare: 1969 No 24 s 4A(3)(b), (c); 2003 No 9 s 15A(2)(a)–(d)

62 Issue of joint intelligence warrant

(1) A joint Type 1 intelligence warrant may be issued under section 58 or 59 if the authorising Minister and a Commissioner of Intelligence Warrants consider it appropriate in the circumstances to do so.

(2) A joint Type 2 intelligence warrant may be issued under section 60 if the authorising Minister considers it appropriate in the circumstances to do so.

(3) The Director-General of Security and the Director-General of the Government Communications Security Bureau may jointly or severally—

(a) carry out all of the activities authorised by a joint intelligence warrant; and

(b) exercise all of the powers under a joint intelligence warrant.

(4) Subsection (3) applies even though an activity or a power authorised by the joint intelligence warrant is not an activity or a power that a Director-General could be authorised to carry out or exercise by an intelligence warrant that is not a joint intelligence warrant (for example, the Director-General of the Government Communications Security Bureau may exercise a power that may be exercised by the Director-General of Security).

63 Minister of Foreign Affairs to be consulted in relation to issue of intelligence warrants in certain cases

The authorising Minister must consult the Minister of Foreign Affairs before an intelligence warrant is issued authorising any activity that is likely to have implications for—

(a) New Zealand's foreign policy; or

(b) New Zealand's international relations.

64 Intelligence warrants may be issued subject to restrictions or conditions

An intelligence warrant may be issued subject to any restrictions or conditions that are considered desirable in the public interest by—

(a) the authorising Minister and a Commissioner of Intelligence Warrants, in the case of a Type 1 intelligence warrant:

(b) the authorising Minister, in the case of a Type 2 intelligence warrant.

Compare: 1969 No 24 ss 4B(2), (3), 4IC(1)(b); 2003 No 9 s 15A(4)

65 Term of intelligence warrant

(1) An intelligence warrant must specify a period not exceeding 12 months during which it is valid.

(2) The expiry of an intelligence warrant does not prevent a further application for an intelligence warrant in relation to the same activity.

Compare: 1969 No 24 s 4C

66 Matters required to be stated in intelligence warrant

An intelligence warrant must state—

(a) the type of intelligence warrant issued:

(b) the Director-General to whom the warrant is issued or, if the warrant is issued on a joint application made under section 56, that it is issued to the Director-General of Security and the Director-General of the Government Communications Security Bureau:

(c) the objective in section 9 to which the warrant relates:

(d) the purpose for which the warrant is issued:

(e) the person or class of persons (if any) in respect of whom the otherwise unlawful activity is being carried out:

(f) the particular activity or activities authorised to be carried out:

(g) any restrictions or conditions imposed under section 64:

(h) the term of the warrant:

(i) the date of issue of the warrant.

Compare: 1969 No 24 s 4B; 2003 No 9 s 15D

Authorised activities and powers

67 Authorised activities

(1) An intelligence warrant may authorise the carrying out of 1 or more of the following activities that would otherwise be unlawful:

(a) conducting surveillance in respect of 1 or more—

(i) persons or classes of persons:

(ii) places or classes of places:

(iii) things or classes of things:

(b) intercepting any private communications or classes of private communications:

(c) searching 1 or more—

(i) places or classes of places:

(ii) things or classes of things:

(d) seizing—

(i) 1 or more communications or classes of communications:

(ii) information or 1 or more classes of information:

(iii) 1 or more things or classes of things:

(e) requesting the government of, or an entity in, another jurisdiction to carry out an activity that, if carried out by an intelligence and security agency, would be an unlawful activity:

(f) taking any action to protect a covert collection capability:

(g) any human intelligence activity to be carried out for the purpose of collecting intelligence, not being an activity that—

(i) involves the use or threat of violence against a person; or

(ii) perverts, or attempts to pervert, the course of justice.

(2) An intelligence warrant issued to the Director-General of the Government Communications Security Bureau may, in addition to any of the activities specified in subsection (1), authorise the doing of any other act that is necessary or desirable to protect the security and integrity of communications and information infrastructures of importance to the Government of New Zealand (including identifying and responding to threats or potential threats to those communications or infrastructures) without the consent of any person.

68 Powers of New Zealand Security Intelligence Service acting under intelligence warrant

(1) The Director-General of the New Zealand Security Intelligence Service, or an employee of that intelligence and security agency authorised by the Director-General for that purpose, may exercise any of the following powers to give effect to an intelligence warrant:

(a) enter—

(i) any place, vehicle, or other thing that is specified in the intelligence warrant; or

(ii) any place, vehicle, or other thing that is owned or occupied by a person identified in the intelligence warrant; or

(iii) any place, vehicle, or other thing where a person identified in the intelligence warrant is, is likely to be, or has been, at any time; or

(iv) in any case where an information infrastructure is identified in the intelligence warrant, any place, vehicle, or other thing—

(A) where that information infrastructure is or is likely to be at any time; or

(B) that it is necessary to enter in order to access that information infrastructure:

(b) install, use, maintain, or remove—

(i) a visual surveillance device; or

(ii) a tracking device; or

(iii) an interception device:

(c) access an information infrastructure or a class of information infrastructures:

(d) open (by any means) or interfere with a vehicle, container, receptacle, or other thing:

(e) take photographs, sound recordings, video recordings, or drawings of the place, vehicle, or other thing entered or searched, and of any item found in or on that place or thing, if the person exercising the power has reasonable grounds to believe that the photographs or sound or video recordings or drawings may be relevant to the purposes of the activity:

(f) bring into and use in or on a place, vehicle, or other thing searched any equipment:

(g) use any equipment found in or on the place, vehicle, or other thing searched:

(h) extract and use, in the course of carrying out activities allowed by the warrant, any electricity from a place or thing:

(i) bring into and use in or on a place, vehicle, or other thing searched a dog (being a dog that is trained to undertake searching or other intelligence duties and that is under the control of its usual handler):

(j) use any force in respect of any property or thing that is reasonable for the purposes of carrying out a search or seizure:

(k) do any act that is reasonable in the circumstances and reasonably required to conceal the fact that anything has been done under the warrant and to keep the activities of the intelligence and security agency covert:

(l) do any other act that is reasonable in the circumstances and reasonably required to achieve the purposes for which the warrant was issued.

(2) Subsection (1) applies subject to any restrictions or conditions imposed under section 64 and stated in the warrant.

Compare: 1969 No 24 s 4E(1), (3); 2012 No 24 s 110(c), (e), (f), (j)

69 Powers of Government Communications Security Bureau under intelligence warrant

(1) The Director-General of the Government Communications Security Bureau, or an employee of that intelligence and security agency authorised by the Director-General for that purpose, may exercise the following powers to give effect to the intelligence warrant:

(a) access an information infrastructure, or a class of information infrastructures:

(b) install, use, maintain, or remove a visual surveillance device to maintain the operational security of any activity authorised to be carried out:

(c) install, use, maintain, or remove an interception device:

(d) extract and use, in the course of carrying out activities allowed by the warrant, any electricity from a place or thing:

(e) do any act that is reasonable in the circumstances and reasonably required to conceal the fact that anything has been done under the warrant and to keep the activities of the intelligence and security agency covert:

(f) do any other act that is reasonable in the circumstances and reasonably required to achieve the purposes for which the warrant was issued.

(2) Subsection (1) applies subject to any restrictions or conditions imposed under section 64 and stated in the warrant.

(3) In this section, **access an information infrastructure** includes—

(a) instructing, communicating with, storing data in, retrieving data from, or otherwise making use of the resources or features of the infrastructure:

(b) making photographs, videos, and sound recordings, or using the infrastructure or any part of it.

70 Privileged communications or privileged information

(1) An intelligence warrant may not authorise the carrying out of any activity or the exercise of any power for the purpose of obtaining privileged communications or privileged information of—

(a) a New Zealand citizen; or

(b) a permanent resident of New Zealand.

(2) In subsection (1), **privileged communications or privileged information** means communications or information protected by legal professional privilege or privileged in proceedings under section 54 or any of sections 56 to 59 of the Evidence Act 2006.

Compare: 1969 No 24 ss 4A(3)(d), 4IB(3)(d); 2003 No 9 s 15C

Urgent intelligence warrants

71 Urgent issue of Type 1 intelligence warrant

(1) This section applies if an application for the issue of a Type 1 intelligence warrant is made in a situation of urgency.

(2) If this section applies,—

(a) the authorising Minister and a Commissioner of Intelligence Warrants may, if satisfied that a situation of urgency exists and that it is necessary to do so,—

(i) allow the application to be made orally (for example, by a telephone call) or by personal appearance, and excuse the applicant from putting all or any part of the application in writing; and

(ii) issue urgently in accordance with section 58 or 59 a Type 1 intelligence warrant; or

(b) the authorising Minister may, if satisfied that a situation of urgency exists and that it is necessary to do so without the involvement of a Commissioner of Intelligence Warrants,—

(i) allow the application to be made orally (for example, by a telephone call) or by personal appearance and excuse the applicant from putting all or any part of the application in writing; and

(ii) issue urgently in accordance with section 58 or 59 a Type 1 intelligence warrant.

(3) If a Type 1 intelligence warrant is issued under subsection (2)(b)(ii), the warrant is effective as if it had been issued by the authorising Minister and a Commissioner of Intelligence Warrants, but—

(a) the authorising Minister must immediately notify the Chief Commissioner of Intelligence Warrants; and

(b) the Chief Commissioner of Intelligence Warrants may, at any time before an application required by section 74 is determined, revoke the warrant.

72 Urgent issue of Type 2 intelligence warrant

(1) This section applies if an application for the issue of a Type 2 intelligence warrant is made in a situation of urgency.

(2) The authorising Minister may, if satisfied that a situation of urgency exists and that it is necessary to do so,—

(a) allow the application to be made orally (for example, by a telephone call) or by personal appearance and excuse the applicant from putting all or any part of the application in writing; and

(b) issue urgently in accordance with section 60 a Type 2 intelligence warrant.

73 Reasons for urgent issue of intelligence warrant to be recorded

The reasons for the urgent issue of an intelligence warrant under section 71 or 72 must be recorded as soon as practicable by—

(a) the authorising Minister; or

(b) the authorising Minister and the Commissioner of Intelligence Warrants, in the case of a warrant issued under section 71(2)(a)(ii).

74 Intelligence warrant issued under section 71 revoked unless confirmed

(1) An intelligence warrant issued under section 71 is revoked by the operation of law 48 hours after its issue unless, before the expiry of that period, the applicant has made an application under section 55 for the issue of a Type 1 intelligence warrant.

(2) On an application made under section 55, the authorising Minister and a Commissioner of Intelligence Warrants may—

(a) confirm the urgent intelligence warrant, and that warrant must then be treated as a Type 1 intelligence warrant issued under section 58 or 59 (as the case may be) on the date on which the urgent intelligence warrant was issued; or

(b) revoke the intelligence warrant issued under section 71.

75 Intelligence warrant issued under section 72 revoked unless confirmed

(1) An intelligence warrant issued under section 72 is revoked by the operation of law 48 hours after its issue unless, before the expiry of that period, the applicant has made an application under section 55 for the issue of a Type 2 intelligence warrant.

(2) On an application made under section 55, the authorising Minister may—

(a) confirm the urgent intelligence warrant, and that warrant must then be treated as a Type 2 intelligence warrant issued under section 60 on the date on which the urgent intelligence warrant was issued; or

(b) revoke the intelligence warrant issued under section 72.

76 Information to be destroyed if intelligence warrant issued under section 71 or 72 revoked

(1) If an intelligence warrant issued under section 71 is revoked under section 74(1), all information obtained under that warrant must be destroyed as soon as practicable.

(2) If an intelligence warrant issued under section 72 is revoked under section 75(1), all information obtained under that warrant must be destroyed as soon as practicable.

(3) Subsections (1) and (2) do not apply to any incidentally obtained information that may be retained under section 104.

77 Intelligence warrants issued under section 71 or 72 to be referred to Inspector-General

An intelligence warrant issued under section 71 or 72 must be referred as soon as practicable after issue to the Inspector-General for review.

Authorisations by Director-General of intelligence and security agency

78 Very urgent authorisations by Director-General of intelligence and security agency

(1) This section applies if—

(a) an application for the urgent issue of an intelligence warrant would otherwise need to be made; but

(b) the delay in making that application would defeat the purpose of obtaining the warrant.

(2) The Director-General of an intelligence and security agency may authorise the carrying out of an otherwise unlawful activity for which—

(a) a Type 1 intelligence warrant is required; or

(b) a Type 2 intelligence warrant is required.

(3) Before giving an authorisation under subsection (2)(a), the Director-General of an intelligence and security agency must be satisfied of the matters in section 58 or 59.

(4) Before giving an authorisation under subsection (2)(b), the Director-General of an intelligence and security agency must be satisfied of the matters in section 60.

79 Authorisation given under section 78(2)(a) effective as Type 1 intelligence warrant

(1) An authorisation given under section 78(2)(a) is effective as if it were a Type 1 intelligence warrant, but the Director-General of an intelligence and security agency must—

(a) immediately notify—

(i) the authorising Minister; and

(ii) the Chief Commissioner of Intelligence Warrants; and

(b) within 24 hours after giving the authorisation, make an application under section 55 for the issue of a Type 1 intelligence warrant.

(2) An authorisation given under section 78(2)(a) is revoked by the operation of law 24 hours after it is given unless, before the expiry of that period, an application under section 55 is made.

(3) The authorising Minister or the Chief Commissioner of Intelligence Warrants may, at any time before an application made under section 55 is determined, revoke an authorisation given under section 78(2)(a).

(4) If a Type 1 intelligence warrant is not issued in respect of the unlawful activity authorised by the Director-General, the authorisation is revoked.

80 Authorisation given under section 78(2)(b) effective as Type 2 intelligence warrant

(1) An authorisation given under section 78(2)(b) is effective as if it were a Type 2 intelligence warrant, but the Director-General of an intelligence and security agency must—

(a) notify the authorising Minister; and

(b) within 24 hours after giving the authorisation, make an application under section 55 for the issue of a Type 2 intelligence warrant.

(2) An authorisation given under section 78(2)(b) is revoked by the operation of law 24 hours after it is given unless, before the expiry of that period, an application under section 55 is made.

(3) The authorising Minister may, at any time before an application made under section 55 is determined, revoke an authorisation given under section 78(2)(b).

(4) If a Type 2 intelligence warrant is not issued in respect of the unlawful activity authorised by the Director-General, the authorisation is revoked.

81 Information to be destroyed if authorisation given under section 78 revoked

(1) If an authorisation given under section 78(2)(a) or (b) is revoked, all information obtained under that authorisation must be destroyed as soon as practicable.

(2) Subsection (1) does not apply to any incidentally obtained information that may be retained under section 104.

82 Authorisations given under section 78 to be referred to Inspector-General

An authorisation given under section 78 must be referred as soon as practicable after it is given to the Inspector-General for review.

Register of intelligence warrants

83 Register of intelligence warrants

(1) The Director-General of an intelligence and security agency must keep a register of intelligence warrants issued to him or her.

(2) The following information must be entered in the register in relation to every intelligence warrant:

(a) the type of warrant issued; and

(b) the particular activity or activities authorised to be carried out; and

(c) any restrictions or conditions to which the intelligence warrant is subject; and

(d) the term during which the intelligence warrant is valid; and

(e) the date on which the intelligence warrant was issued.

(3) The Director-General of an intelligence and security agency must also keep, in conjunction with the register,—

(a) a copy of every application made for an intelligence warrant; and

(b) a record of any information provided by, or a copy of any document received from, the Minister of Foreign Affairs in the course of any consultation under section 63; and

(c) the original of every intelligence warrant issued.

(4) All information required to be kept under this section by the Director-General of an intelligence and security agency may be accessed at any time by—

(a) the Minister responsible for the intelligence and security agency:

(b) the Chief Commissioner of Intelligence Warrants, in relation to Type 1 intelligence warrants:

(c) the Inspector-General.

Compare: 2003 No 9 s 19

Amendment and revocation of intelligence warrants

84 Amendment and revocation of intelligence warrants

(1) The authorising Minister and a Commissioner of Intelligence Warrants may—

(a) at any time amend or revoke a Type 1 intelligence warrant; and

(b) direct that all or any specified information obtained under the warrant before it was amended or revoked be destroyed.

(2) The authorising Minister may—

(a) at any time amend or revoke a Type 2 intelligence warrant; and

(b) direct that all or any specified information obtained under the warrant before it was amended or revoked be destroyed.

Subpart 2—Removal warrants

85 Issue of removal warrant to retrieve previously installed devices

(1) This section applies if any device or equipment that has been installed in accordance with an intelligence warrant issued to the Director-General of an intelligence and security agency (the **original intelligence warrant**) remains in a place or thing after the original intelligence warrant has ceased to be in force.

(2) The Director-General of Security may make a written application to the Minister responsible for the New Zealand Security Intelligence Service for the issue of a removal warrant authorising the removal of the device or equipment.

(3) A removal warrant may be issued to the Director-General of Security if the Minister responsible for that agency is satisfied that the issue of the warrant is necessary.

(4) A removal warrant must specify a period not exceeding 12 months during which it is valid.

Compare: 1969 No 24 s 4I(1), (3)

86 Minister of Foreign Affairs to be consulted in relation to issue of removal warrants in certain cases

The Minister responsible for an intelligence and security agency making an application under section 85 must consult the Minister of Foreign Affairs before issuing a removal warrant if that warrant is likely to have implications for—

(a) New Zealand's foreign policy; or

(b) New Zealand's international relations.

87 Powers of New Zealand Security Intelligence Service acting under removal warrant

The Director-General of Security, or an employee of the New Zealand Security Intelligence Service authorised by the Director-General for that purpose, may exercise any of the following powers to give effect to the removal warrant:

(a) enter the place, vehicle, or thing that the device or equipment to be removed under the warrant is in or on:

(b) take possession of any vehicle or thing that the device or equipment to be removed under the warrant is in or on:

(c) search any place, vehicle, or thing that the device or equipment to be removed under the warrant is in or on:

(d) remove a tracking device:

(e) open (by any means) or interfere with a vehicle, container, receptacle, or other thing:

(f) bring into and use in or on a place, vehicle, or other thing referred to in any of paragraphs (a) to (c) any equipment:

(g) use any equipment found in or on a place, vehicle, or thing referred to in any of paragraphs (a) to (c):

(h) extract and use, in the course of giving effect to the removal warrant, any electricity from a place or thing:

(i) use any force in respect of any property or thing that is reasonable for the purpose of giving effect to the removal warrant:

(j) do any act that is reasonable in the circumstances and reasonably required to conceal the fact that anything has been done under the warrant and to keep the activities of the intelligence and security agency covert:

(k) do any other act that is reasonable in the circumstances and reasonably required to achieve the purposes for which the warrant was issued.

Compare: 1969 No 24 s 4I(2)

Subpart 3—Practice warrants

88 Types of practice warrant

There are 2 types of practice warrants, as follows:

(a) testing warrants:

(b) training warrants.

89 Testing warrant

A **testing warrant** authorises an intelligence and security agency to carry out an otherwise unlawful activity that is necessary to test, maintain, or develop the capability of the agency in relation to the performance of its statutory functions.

90 Training warrant

A **training warrant** authorises an intelligence and security agency to carry out an otherwise unlawful activity that is necessary to train employees in relation to the performance of the agency's statutory functions.

91 Application for issue of practice warrant

(1) An application for a practice warrant must be made in writing by the Director-General of an intelligence and security agency to—

(a) the Minister responsible for the intelligence and security agency; and

(b) the Chief Commissioner of Intelligence Warrants.

(2) An application for the issue of a practice warrant must set out—

(a) the type of practice warrant applied for; and

(b) details of the activity proposed to be carried out under the practice warrant; and

(c) the purpose of the proposed activity; and

(d) the reasons why the criteria for issuing the practice warrant set out in section 92 are believed to be satisfied.

92 Criteria for issue of practice warrant

The criteria for the issue of a practice warrant are—

(a) the carrying out of the otherwise unlawful activity (the **proposed activity**) by an intelligence and security agency is reasonably necessary to ensure that the agency will be able to competently perform its statutory functions in the future; and

(b) the proposed activity is proportionate to the purpose for which it is to be carried out; and

(c) the purpose of the proposed activity cannot reasonably be achieved by a less intrusive means; and

(d) there are satisfactory arrangements in place to ensure that—

(i) all reasonably practicable steps will be taken to minimise the impact of the proposed activity on any members of the public; and

(ii) nothing will be done in reliance on the practice warrant beyond what is necessary and reasonable to achieve the purpose of the proposed activity; and

(iii) any information obtained in reliance on the practice warrant will be retained only for so long as is necessary to achieve the purpose of the proposed activity.

93 Issue of practice warrant

(1) A practice warrant is issued to the Director-General of an intelligence and security agency.

(2) A practice warrant is issued jointly by—

(a) the Minister responsible for the intelligence and security agency; and

(b) a Commissioner of Intelligence Warrants.

94 Minister of Foreign Affairs to be consulted in relation to issue of practice warrants in certain cases

The Minister responsible for an intelligence and security agency making an application under section 91 must consult the Minister of Foreign Affairs before a practice warrant is issued authorising any activity that is likely to have implications for—

(a) New Zealand's foreign policy; or

(b) New Zealand's international relations.

95 Practice warrants may be issued subject to restrictions or conditions

A practice warrant may be issued subject to any restrictions or conditions that are considered desirable in the public interest.

96 Term of practice warrant

(1) A practice warrant must specify a period not exceeding 12 months during which it is valid.

(2) The expiry of a practice warrant does not prevent a further application for a practice warrant in relation to the same activity.

97 Matters to be stated in practice warrant

A practice warrant must state—

(a) the type of warrant issued; and

(b) the Director-General to whom the warrant is issued; and

(c) the activity authorised to be carried out; and

(d) any restrictions or conditions imposed under section 95; and

(e) the term of the warrant; and

(f) the date on which the warrant was issued.

98 Authorised activities

A practice warrant may authorise the carrying out of 1 or more of the activities specified in section 67(1)(a) to (f) that would otherwise be unlawful.

99 Powers of New Zealand Security Intelligence Service acting under practice warrant

(1) The Director-General of the New Zealand Security Intelligence Service, or an employee of that intelligence and security agency authorised by the Director-General for that purpose, may exercise any of the powers in section 68(1)(b) to (l) to give effect to a practice warrant.

(2) Subsection (1) applies subject to any restrictions or conditions imposed under section 95 stated in the practice warrant.

100 Powers of Government Communications Security Bureau acting under practice warrant

(1) The Director-General of the Government Communications Security Bureau, or an employee of that intelligence and security agency authorised by the Director-General for that purpose, may exercise any of the powers in section 69 to give effect to a practice warrant.

(2) Subsection (1) applies subject to any restrictions or conditions imposed under section 95 stated in the practice warrant.

101 Report on practice warrant activities

As soon as practicable after the expiry or revocation of a practice warrant, the Director-General of an intelligence and security agency must provide details of all authorised activities carried out under the warrant to—

(a) the Minister responsible for the intelligence and security agency; and

(b) the Inspector-General.

Subpart 4—Unauthorised, irrelevant, and incidentally obtained information

102 Destruction of unauthorised information

(1) In this section, **unauthorised information** means—

(a) information unintentionally obtained that is outside the scope of—

(i) an authorisation; or

(ii) an authorised activity; or

(b) information obtained during the provision of co-operation, advice, and assistance under section 14 that could otherwise only be obtained during the carrying out of an authorised activity.

(2) Unauthorised information must be destroyed immediately after it is obtained unless,—

(a) on an application that is made as soon as practicable, an intelligence warrant is issued authorising collection of the information; or

(b) section 104 applies.

103 Destruction of irrelevant information

(1) In this section, **irrelevant information** means information that—

(a) is obtained by an intelligence and security agency within the scope of an authorised activity; but

(b) is not required, or is no longer required, by the agency for the performance of its functions.

(2) Irrelevant information must be destroyed as soon as practicable.

(3) Subsection (2) is subject to—

(a) any enactment requiring the retention of the information; or

(b) any order of a court that imposes a prohibition on the destruction of the information.

104 Retention of incidentally obtained information

(1) The Director-General of an intelligence and security agency may retain any incidentally obtained information that comes into the possession of the agency only for the purpose of disclosing it to a person specified in subsection (2) in the circumstances specified in subsection (3).

(2) The persons are—

(a) any employee of the New Zealand Police:

(b) any member of the New Zealand Defence Force:

(c) any public authority (whether in New Zealand or overseas) that the Director-General considers should receive the information.

(3) The circumstances are that the Director-General has reasonable grounds to believe that the disclosure of the information to a person specified in subsection (2) may assist in—

(a) preventing or detecting serious crime in New Zealand or any other country:

(b) preventing or responding to threats to the life of any person in New Zealand or any other country:

(c) identifying, preventing, or responding to threats or potential threats to the security or defence of New Zealand or any other country:

(d) preventing the death of any person who is outside the territorial jurisdiction of any country.

Compare: 2003 No 9 s 25

Return of physical items seized

105 Physical items seized to be returned after search or analysis

(1) A physical item seized under an intelligence warrant may be retained by an intelligence and security agency only for as long as is reasonably necessary to enable the agency to conduct a search or analysis of the item.

(2) The physical item must then be returned to—

(a) the place from which it was seized; or

(b) the person from whom it was seized.

(3) However, subsection (2) does not apply if—

(a) the return of the item would undermine the ability of the agency to maintain the secrecy of the search and seizure; or

(b) the person from whom the item was seized was not lawfully entitled to possession of the item; or

(c) the item was unlawfully in the place from which it was seized or was being used unlawfully in the place from which it was seized; or

(d) the person from whom the item was seized cannot be found.

Subpart 5—Offences and immunities

106 Offence to provide false or misleading information

(1) A Director-General of an intelligence and security agency or an employee of an intelligence and security agency who makes a warrant application that contains any false or misleading information commits an offence and is liable on conviction to imprisonment for a term not exceeding 1 year.

(2) It is a defence to a charge under subsection (1) that the Director-General of an intelligence and security agency to whom the charge relates did not know that he or she was providing false or misleading information and had exercised all

reasonable care and due diligence to ensure that the information provided was not false or misleading.

(3) In this section, **warrant application** means an application for the issue of any of the following:

(a) an intelligence warrant (including the urgent issue of an intelligence warrant):

(b) a removal warrant:

(c) a practice warrant.

107 Failure to destroy information

A person commits an offence and is liable on conviction to a fine not exceeding $10,000 if the person knowingly fails to comply with—

(a) section 76:

(b) section 81:

(c) section 102.

Compare: 1969 No 24 ss 4G(3), 4IB(11), 4IE(11); 2003 No 9 s 23(2)

108 Unlawful use or disclosure of information

(1) A person carrying out an authorised activity must not, other than in the performance or exercise of the person's functions, duties, or powers or with the consent of the relevant Minister,—

(a) disclose to any other person that the activity is an authorised activity; or

(b) use any information obtained from the carrying out of the authorised activity; or

(c) disclose to any other person any information obtained from the carrying out of the authorised activity.

(2) A person who contravenes this section commits an offence and is liable on conviction to a fine not exceeding $10,000.

(3) In this section, **relevant Minister** means the Minister responsible for the intelligence and security agency authorised to carry out the activity.

Compare: 1969 No 24 s 12A(1), (2), (4)

109 Unlawful disclosure of acquired information

(1) A person who acquires knowledge of any information knowing that it was gained from the carrying out of an authorised activity must not knowingly disclose that information otherwise than in the performance or exercise of his or her functions, duties, or powers.

(2) A person who contravenes this section commits an offence and is liable on conviction to a fine not exceeding $10,000.

Compare: 1969 No 24 s 12A(3), (4)

110 Immunities from criminal liability in relation to obtaining intelligence warrant

(1) The Director-General of an intelligence and security agency and an employee of an intelligence and security agency are immune from criminal liability for any act done in good faith to obtain an intelligence warrant if—

(a) the Director-General or employee reasonably believed that the act was necessary to obtain the warrant; and

(b) the carrying out of the activity was done in a reasonable manner.

(2) Subsection (1) applies even if the intelligence warrant is subsequently—

(a) revoked; or

(b) determined to have been invalidly issued or given.

(3) Subsection (2)(b) is to avoid doubt.

(4) Subsection (1) does not apply if the Director-General or employee is charged with an offence under section 106.

111 Immunities from criminal liability in relation to carrying out authorised activity

(1) A person is immune from criminal liability for any act done in good faith in carrying out an authorised activity if—

(a) the person reasonably believed that doing the act was necessary to carry out the activity; and

(b) the activity was carried out in a reasonable manner.

(2) Subsection (1) applies even if the authorisation is subsequently—

(a) revoked; or

(b) determined to have been invalidly issued or given.

(3) Subsection (2)(b) is to avoid doubt.

Subpart 6—Commissioners of Intelligence Warrants

112 Appointment of Commissioners

(1) The Governor-General must, on the recommendation of the Prime Minister, appoint up to 3 persons as Commissioners of Intelligence Warrants.

(2) The Governor-General must, on the recommendation of the Prime Minister, appoint 1 Commissioner of Intelligence Warrants as the Chief Commissioner of Intelligence Warrants.

(3) Before recommending an appointment under this section, the Prime Minister must—

(a) consult the Leader of the Opposition about the proposed appointment; and

(b) advise the Governor-General that the Leader of the Opposition has been consulted.

Compare: 1969 No 24 s 5A(1), (2)

113 Eligibility for appointment

A person may be appointed a Commissioner of Intelligence Warrants only if that person has previously held office as a Judge of the High Court.

Compare: 1969 No 24 s 5A(3)

114 Functions of Commissioners

The functions of a Commissioner of Intelligence Warrants are—

(a) to advise the authorising Minister on applications under section 55 for Type 1 intelligence warrants:

(b) to consider with the authorising Minister applications under section 55 for Type 1 intelligence warrants:

(c) to deliberate with the authorising Minister on applications under section 55 for Type 1 intelligence warrants:

(d) to issue Type 1 intelligence warrants under section 58 or 59 jointly with the authorising Minister:

(e) to consider with the authorising Minister applications made under section 136 seeking permission to access restricted information:

(f) to consider with the responsible Minister applications made under section 145 for an approval to obtain business records:

(g) to conduct reviews under section 56 of the Telecommunications (Interception Capability and Security) Act 2013 relating to significant network security risks:

(h) to conduct reviews under section 27GF of the Passports Act 1992 relating to decisions to refuse to issue, or to cancel or retain possession of, a New Zealand travel document:

(i) to perform any other functions conferred or imposed on a Commissioner of Intelligence Warrants by or under this Act or any other enactment.

Compare: 1969 No 24 s 5A(5)(a)–(d), (g)

115 Additional functions of Chief Commissioner of Intelligence Warrants

The Chief Commissioner of Intelligence Warrants has the following additional functions:

(a) to be the central point of contact for all communications with the Commissioners of Intelligence Warrants:

(b) to receive all applications for a Type 1 intelligence warrant:

(c) to allocate an application for a Type 1 intelligence warrant to himself or herself or to another Commissioner of Intelligence Warrants:

(d) to receive notice under section 71(3)(a) of the issue of a Type 1 intelligence warrant by the authorising Minister and consider whether to revoke it:

(e) to receive notice under section 79(1)(a) of an authorisation given under section 78(2)(a) and consider whether to revoke it:

(f) to receive all applications for an approval under section 145:

(g) to allocate an application for an approval under section 145 to himself or herself or to another Commissioner of Intelligence Warrants for consideration:

(h) to perform any other functions conferred or imposed on the Chief Commissioner of Intelligence Warrants by or under this Act or any other enactment.

116 Delegation of functions of Chief Commissioner of Intelligence Warrants

(1) The Chief Commissioner of Intelligence Warrants (the **Chief Commissioner**) must ensure that an appropriate delegation is at all times in place under this section to enable another Commissioner of Intelligence Warrants (a **delegate**) to act in place of the Chief Commissioner during—

(a) any absence or incapacity of the Chief Commissioner; or

(b) any vacancy in the office of the Chief Commissioner.

(2) A delegation under this section—

(a) must be in writing; and

(b) is revocable at any time, by notice in writing.

(3) A delegate may perform the functions of the Chief Commissioner in the same manner and with the same effect as if those functions had been conferred directly on him or her by this Act.

(4) A delegate who purports to act under a delegation is, in the absence of proof to the contrary, presumed to be acting in accordance with the delegation.

(5) A delegation, until it is revoked, continues to have effect even if the Chief Commissioner by whom it was made ceases to hold office.

117 Administrative provisions relating to Commissioners

Part 1 of Schedule 3 applies in relation to the Commissioners of Intelligence Warrants.

Part 5
Accessing information held by other agencies

118 Interpretation

In this Part, unless the context otherwise requires,—

agency—

(a) means any person, whether in the public sector or the private sector; and

(b) includes a department

database—

(a) means the information recording system or facility used by a holder agency to store information; and

(b) includes any system for transferring or processing information into or out of, or within, that information recording system or facility

direct access, in relation to a database, means to do either or both of the following (whether remotely or otherwise):

(a) search the database:

(b) copy any information stored on the database (including by previewing, cloning, or other forensic methods)

holder agency means an agency specified in the third column of the table in Schedule 2

information means personal information and non-personal information

non-personal information means information that is not personal information

personal information means information about an identifiable individual

responsible Minister,—

(a) in relation to an intelligence and security agency, means the Minister responsible for the intelligence and security agency; and

(b) in relation to the intelligence and security agencies, means—

(i) the Minister responsible for the intelligence and security agencies, if the same Minister is responsible for each agency; and

(ii) the Ministers responsible for the intelligence and security agencies, if a different Minister is responsible for each agency.

119 Relationship between this Part and other law relating to information disclosure

This Part does not limit the collection, use, or disclosure of personal information that—

(a) is authorised or required by or under any enactment; or

(b) is permitted by the information privacy principles in section 6 of the Privacy Act 1993.

Subpart 1—Request and disclosure of information

120 Purpose of subpart

The purpose of this subpart is—

(a) to recognise—

(i) the existing ability of an intelligence and security agency to request information held by other agencies; and

(ii) the existing ability of an agency to disclose information that it holds to an intelligence and security agency; but

(b) not to confer on an agency any legal right or obligation.

121 Requests for information

(1) The Director-General of an intelligence and security agency may request information from any other agency if the Director-General believes on reasonable grounds that the information is necessary to enable the intelligence and security agency to perform any of its functions.

(2) A request must—

(a) provide details of the information requested; and

(b) confirm that the information is necessary to enable the intelligence and security agency to perform any of its functions.

122 Disclosure of information to intelligence and security agency

(1) An agency may disclose to an intelligence and security agency any information that it holds or controls if it believes on reasonable grounds that the disclosure of information is necessary to enable the intelligence and security agency to perform any of its functions.

(2) An agency may disclose the information—

(a) on the request of an intelligence and security agency; or

(b) on its own initiative.

(3) For the purpose of enabling an agency to decide whether to disclose any information under subsection (1) (including the application of section 6 of the Privacy Act 1993), the Director-General of an intelligence and security agency may certify that he or she believes on reasonable grounds that the disclosure of the information is necessary for the performance of any of the agency's functions.

(4) This section is subject to—

(a) a provision contained in any other enactment that—

(i) prohibits or restricts the disclosure of the information to an intelligence and security agency; or

(ii) regulates the manner in which the information may be obtained or made available to an intelligence and security agency; and

(b) a provision contained in any contract, agreement, or other document relating to the disclosure of the information; and

(c) any obligation of confidence.

Register of section 122 certificates

123 Register of section 122 certificates

(1) The Director-General of an intelligence and security agency must keep a register of all certificates issued by him or her under section 122(3) (a **section 122 certificate**).

(2) The register must include, for each section 122 certificate issued, details of—

(a) the date on which the certificate was issued; and

(b) the agency to which the certificate was issued; and

(c) the information to which the certificate relates; and

(d) the circumstances in which the certificate was issued.

(3) The register may be accessed at any time by—

(a) the Minister responsible for the intelligence and security agency:

(b) the Inspector-General.

Subpart 2—Direct access to database information

124 Purpose of subpart

The purpose of this subpart is to enable an intelligence and security agency to have direct access to databases storing specified public sector information.

125 Direct access to certain information

(1) An intelligence and security agency specified in the first column of Schedule 2 may have direct access to the information specified in the second column of Schedule 2 that is opposite its name and held by the holder agency specified in the third column of Schedule 2.

(2) However, that access must be in accordance with a written direct access agreement entered into between—

(a) the Minister responsible for the holder agency; and

(b) the Minister responsible for the intelligence and security agency.

126 Matters to which Ministers must have regard before entering into direct access agreement

Before entering into a direct access agreement, the Ministers referred to in section 125(2) must be satisfied that—

(a) direct access to the information is necessary to enable the intelligence and security agency to perform any of its functions; and

(b) there are adequate safeguards to protect the privacy of individuals, including that the proposed compliance and audit requirements for the direct access, use, disclosure, and retention of the information are sufficient; and

(c) the agreement will include appropriate procedures for direct access, use, disclosure, and retention of the information.

127 Consultation with Privacy Commissioner before entering into direct access agreement

(1) Before entering into a direct access agreement, the Ministers referred to in section 125(2) must consult with, and invite comment from, the Privacy Commissioner on the proposed agreement.

(2) When consulted on a direct access agreement, the Privacy Commissioner must have particular regard to the matters that the Ministers need to be satisfied of before entering into the agreement that are specified in section 126(b) and (c).

(3) The Ministers must have regard to any comments received from the Privacy Commissioner on the proposed agreement.

128 Consultation with Inspector-General before entering into direct access agreement

(1) Before entering into a direct access agreement, the Ministers referred to in section 125(2) must also consult with, and invite comment from, the Inspector-General on the proposed agreement.

(2) The Ministers must have regard to any comments received from the Inspector-General on the proposed agreement.

129 Content of direct access agreements

An agreement must specify—

(a) the database or databases that may be accessed:

(b) the particular information that may be accessed:

(c) the particular purpose or purposes for which the information may be accessed:

(d) the particular function, duty, or power being, or to be, performed or exercised by the intelligence and security agency for which the information is required:

(e) the mechanism by which the information is to be accessed:

(f) the position held by the person or persons in the intelligence and security agency who may access the information:

(g) the records to be kept in relation to each occasion on which a database is accessed:

(h) the safeguards that are to be applied for protecting particular information (for example, personal information or information that is commercially sensitive):

(i) the requirements relating to storage, retention, and disposal of information obtained from the database or databases:

(j) the circumstances (if any) in which the information may be disclosed to another agency (whether in New Zealand or overseas), and how that disclosure may be made:

(k) the apportionment of the costs incurred by the holder agency and the intelligence and security agency under the agreement.

130 Variation of direct access agreement

Sections 126, 127, and 128 apply with any necessary modifications in respect of a proposal to enter into an agreement varying a direct access agreement.

131 Publication of direct access agreements

(1) An agreement, and all variations to the agreement, must be published on—

(a) an Internet site maintained by or on behalf of the holder agency; and

(b) an Internet site maintained by or on behalf of the relevant intelligence and security agency.

(2) However, subsection (1) does not apply to—

(a) an agreement or a variation of an agreement that may be withheld on a request under the Official Information Act 1982:

(b) a provision of an agreement or a variation of an agreement that may be withheld on a request under the Official Information Act 1982.

(3) If, in reliance on subsection (2)(a), an agreement or a variation of an agreement is not published, a summary of the agreement or variation of an agreement must be published on—

(a) an Internet site maintained by or on behalf of the holder agency; and

(b) an Internet site maintained by or on behalf of the relevant intelligence and security agency.

132 Review of agreements

(1) The Ministers who have entered into an agreement must review the agreement every 3 years.

(2) In conducting a review, the Ministers must—

(a) consult—

(i) the Privacy Commissioner; and

(ii) the Inspector-General; and

(b) have regard to any comments received from—

(i) the Privacy Commissioner; and

(ii) the Inspector-General.

133 Relationship between subpart and other law

This subpart does not prevent or limit any disclosure of information that may be required or authorised by or under—

(a) any other provision of this Act; or

(b) any other enactment.

Subpart 3—Access to restricted information

134 Purpose of subpart

The purpose of this subpart is to enable an intelligence and security agency to access restricted information.

135 Meaning of restricted information

In this subpart, **restricted information** means—

(a) information that an Inland Revenue officer must maintain, and must assist in maintaining, the secrecy of under section 81 of the Tax Administration Act 1994:

(b) information relating to national student numbers assigned by the Secretary of Education under section 343 of the Education Act 1989 to students enrolled with a tertiary education provider:

(c) information relating to an adoption held by the Registrar-General appointed under section 79(1) of the Births, Deaths, Marriages, and Relationships Registration Act 1995:

(d) photographic images used for driver licences that are stored under section 28(5) of the Land Transport Act 1998.

136 Application for permission to access restricted information

(1) The Director-General of an intelligence and security agency seeking access to restricted information in relation to a person must apply for permission.

(2) An application for permission must be made to—

(a) the responsible Minister and the Chief Commissioner of Intelligence Warrants, if the person is—

(i) a New Zealand citizen; or

(ii) a permanent resident of New Zealand; or

(b) the responsible Minister, if the person is not—

(i) a New Zealand citizen; or

(ii) a permanent resident of New Zealand.

(3) An application must state the particular restricted information to which access is sought.

137 Permission to access restricted information granted on application made under section 136(2)(a)

The responsible Minister and a Commissioner of Intelligence Warrants may grant an application made under section 136(2)(a) and permit access to specified restricted information if they are satisfied—

(a) that—

(i) access to the restricted information is necessary to contribute to the protection of national security and to assist in protecting against any of the harms specified in section 58(2); and

(ii) the further criteria in section 139 are met; or

(b) that—

(i) access to the restricted information will contribute to achieving the objective in section 9(b) or (c); and

(ii) there are reasonable grounds to suspect that the person referred to in section 136(2)(a) is acting, or purporting to act, for or on behalf of—

(A) a foreign person; or

(B) a foreign organisation; or

(C) a designated terrorist entity; and

(iii) the further criteria in section 139 are met.

138 Permission to access restricted information granted on application made under section 136(2)(b)

The responsible Minister may grant an application made under section 136(2)(b) and permit access to specified restricted information if the responsible Minister is satisfied that—

(a) access to the restricted information—

(i) is necessary to contribute to the protection of national security; or

(ii) will contribute to—

(A) the international relations and well-being of New Zealand; or

(B) the economic well-being of New Zealand; and

(b) the further criteria in section 139 are met.

139 Further criteria for permitting access to restricted information

The further criteria for permitting access to restricted information referred to in sections 137 and 138 are that—

(a) access to the restricted information is necessary for the purpose of enabling the intelligence and security agency to perform a function under section 10 or 11; and

(b) the privacy impact of permitting access is proportionate to that purpose; and

(c) the restricted information cannot be accessed by any other means.

140 Permission must specify restricted information that may be accessed

A permission given under section 137 or 138 must specify the particular restricted information that the intelligence and security agency may access.

141 Access to restricted information must be provided if permitted

An agency must provide to the Director-General of an intelligence and security agency named in the permission access to any restricted information specified in the permission if that information is held by or is within the control of that agency.

142 Use, retention, and disclosure of restricted information

Restricted information accessed by an intelligence and security agency may be used, retained, and disclosed by the intelligence and security agency only in the performance of its functions.

Subpart 4—Obtaining business records of telecommunications network operators and financial service providers

143 Purpose of subpart

The purpose of this subpart is to enable an intelligence and security agency to obtain business records of telecommunications network operators and financial service providers.

144 Interpretation

In this subpart, unless the context otherwise requires,—

approval means an approval given under section 147 to obtain business records from business agencies

business agencies means—

(a) telecommunications network operators:

(b) financial service providers

business records means,—

(a) in relation to a business agency that is a telecommunications network operator, all information in the possession or under the control of the telecommunications network operator that is generated or received in the course of the operator's business,—

(i) including—

(A) customer information (for example, names and contact details):

(B) subscriber information (for example, names and contact details):

(C) bank account number details:

(D) credit card number details:

(E) IP addresses:

(F) billing information and records:

(G) call associated data (within the meaning of section 3(1) of the Telecommunications (Interception Capability and Security) Act 2013):

(H) device-related information:

(I) details of mobile data usage:

(J) information on linked accounts:

(K) details of any persons communicating with the network operator; but

(ii) excluding—

(A) personal information about the network operator's employees and directors:

(B) the content of telecommunications:

(C) any information relating to the business operations of the network operator (including finances, budgets, plans, and strategies):

(D) the content of any other communications or files held by the network operator in providing any service to a customer (for example, cloud storage servers or insurance):

(E) web browsing history:

(b) in relation to a business agency that is a financial service provider, all information in the possession or under the control of the financial service provider that is generated or received in the course of the provider's business,—

(i) including—

(A) customer information (for example, names and contact details):

(B) bank account number details:

(C) credit card number details:

(D) statement and account information:

(E) transaction information and other information related to a specific account; but

(ii) excluding—

(A) personal information about the provider's employees and directors:

(B) the content of communications:

(C) any information relating to the business operations of the financial service provider (including finances, budgets, plans, and strategies):

(D) the content of any other communications or files held by the financial service provider in providing any service to a customer (for example, cloud storage servers or insurance)

business records direction means a direction issued under section 150

financial service provider has the meaning given to it by section 4 of the Financial Service Providers (Registration and Dispute Resolution) Act 2008

telecommunication has the meaning given to it by section 5 of the Telecommunications Act 2001

telecommunications network operator means a network operator as defined in section 3(1) of the Telecommunications (Interception Capability and Security) Act 2013.

Approval to obtain business records

145 Application for approval to obtain business records

(1) The Director-General of an intelligence and security agency may apply for an approval to obtain business records from business agencies under business records directions.

(2) An application for an approval must be made to—

(a) the responsible Minister; and

(b) the Chief Commissioner of Intelligence Warrants.

(3) An application must be in writing and state—

(a) the circumstances giving rise to the need to rely on the approval to issue business records directions to obtain business records; and

(b) the business records or class of business records sought to be obtained under each business records direction issued under the approval (including, to avoid doubt, the time period to which those records or classes of records relate); and

(c) the function under section 10, 11, or 14 that the intelligence and security agency would be performing in those circumstances; and

(d) that applying for an intelligence warrant to obtain the business records is likely to be impractical in those circumstances, or the reason why it would otherwise not be appropriate in those circumstances to apply for an intelligence warrant to obtain the business records.

146 Joint application for approval

The Director-General of Security and the Director-General of the Government Communications Security Bureau may jointly apply for an approval.

147 Approval to obtain business records

(1) An application for an approval to obtain business records from business agencies is granted jointly by—

(a) the responsible Minister; and

(b) a Commissioner of Intelligence Warrants.

(2) An application for an approval may be granted to the Director-General of an intelligence and security agency if the responsible Minister and a Commissioner of Intelligence Warrants are satisfied that—

(a) obtaining business records from business agencies in the circumstances stated in the application is necessary to enable the intelligence and security agency to perform a function under section 10, 11, or 14; and

(b) the privacy impact of obtaining the business records in those circumstances does not outweigh the importance of performing that function; and

(c) it would not be more appropriate for the Director-General to apply for the issue of an intelligence warrant authorising the seizing of the business records; and

(d) there are satisfactory arrangements in place to ensure that nothing will be done in reliance on the approval beyond what is necessary and reasonable for the proper performance of a function of an intelligence and security agency; and

(e) there are satisfactory arrangements in place to ensure that any information obtained in reliance on the approval will be retained, used, and disclosed only in accordance with this Act or any other enactment.

(3) An approval must state—

(a) the Director-General to whom the approval is granted; and

(b) the circumstances in which those business records may be obtained from business agencies by the issue of a business records direction under the approval; and

(c) the business records or class of business records that the Director-General may obtain from business agencies under a business records direction; and

(d) any restrictions or conditions to which the approval is subject; and

(e) the date on which the approval was granted.

148 Duration of approval

(1) An approval takes effect on the date on which it is granted and expires 6 months after that date.

(2) The Director-General of an intelligence and security agency may, either before or after the date on which an approval expires, apply for a subsequent approval that is the same as the earlier approval.

(3) Despite subsection (1), if an application for a subsequent approval is made before the earlier approval expires, the subsequent approval may take effect from the date on which the earlier approval expires.

149 Amendment and revocation of approvals

The responsible Minister and a Commissioner of Intelligence Warrants may—

(a) at any time amend or revoke an approval; and

(b) direct that all or any specified business records obtained under the approval before it was amended or revoked be destroyed.

Issue of business records direction

150 Director-General of intelligence and security agency may issue business records direction

(1) The Director-General of an intelligence and security agency who has been granted an approval may issue a business records direction in writing to a named business agency requiring that agency to provide to the Director-General copies of—

(a) specified business records relating to an identifiable person or thing:

(b) any specified class of business records relating to an identifiable person or thing.

(2) A business records direction may be issued by a Director-General only—

(a) in respect of business records, or a class of business records, that the Director-General may obtain under a current approval; and

(b) in the circumstances stated in the approval; and

(c) in accordance with any restrictions or conditions stated in the approval.

(3) Before issuing a business records direction, the Director-General of an intelligence and security agency must be satisfied that the extent of business records required to be provided under that direction is justified and is no more than is necessary to enable the performance of the agency's functions.

(4) In this section,—

current approval means an approval that has not expired

thing includes—

(a) a number (for example, a telephone number, bank account number, or credit card number); and

(b) an address (for example, an Internet protocol address).

151 Compliance with business records direction

(1) A business agency to which a business records direction is issued must comply with the direction not later than 30 days after receiving it, or comply at any later time permitted by the Director-General who issued the request.

(2) A business agency commits an offence if the agency, without reasonable excuse, fails to comply with a business records direction.

(3) A business agency who commits an offence against subsection (2) is liable on conviction,—

(a) in the case of an individual, to imprisonment for a term not exceeding 1 year:

(b) in the case of a body corporate, to a fine not exceeding $40,000.

(4) Subsection (1) applies despite the expiry of the approval under which the direction was issued.

Compare: 2012 No 24 s 174

152 Business records to be destroyed if not required by intelligence and security agency

(1) All business records obtained by a Director-General of an intelligence and security agency under a business records direction must be destroyed as soon as practicable if the records are not required, or are no longer required, by the agency for the performance of its functions.

(2) Subsection (1) is subject to—

(a) any enactment requiring the retention of the information contained in the business records; or

(b) any order of a court that imposes a prohibition on the destruction of the information contained in the business records.

Register of business records directions

153 Register of business records directions

(1) The Director-General of an intelligence and security agency must keep a register of all business records directions issued by him or her.

(2) The register must include, for each business records direction issued, details of—

(a) the approval under which the direction was issued; and

(b) the date on which the direction was issued; and

(c) the business agency to whom the direction was issued; and

(d) the circumstances in which the direction was issued; and

(e) the function being performed by the intelligence and security agency to which the direction relates; and

(f) the business records or class of business records sought to be obtained under the direction; and

(g) the date on which the business agency complied with the direction.

(3) The register may be accessed at any time by—

(a) the Minister responsible for the intelligence and security agency:

(b) the Inspector-General.

154 Subpart does not create any new obligation to create or maintain records

Nothing in this subpart requires a financial service provider or a telecommunications network operator to create information or maintain a record of information that would not, apart from this subpart, have been created or maintained.

Relationship with other law

155 Relationship between subpart and other law

This subpart does not prevent or limit the disclosure of business records to an intelligence and security agency that may be required, authorised, or permitted by or under—

(a) any other provision of this Act; or

(b) any other enactment.

Part 6
Oversight of intelligence and security agencies

156 Purpose of Part

(1) The purpose of this Part is to provide for the independent oversight of intelligence and security agencies to ensure that those agencies act with propriety and operate lawfully and effectively.

(2) To achieve this purpose,—

(a) the office of the Inspector-General of Intelligence and Security is continued, with the Inspector-General having functions, duties, or powers to—

(i) ensure that the intelligence and security agencies conduct their activities lawfully and with propriety; and

(ii) ensure that complaints relating to the intelligence and security agencies are independently investigated; and

(iii) advise the New Zealand Government and the Intelligence and Security Committee on matters relating to the oversight of the agencies:

(b) the Intelligence and Security Committee is continued to provide parliamentary scrutiny of the policies, administration, and expenditure of the intelligence and security agencies.

Subpart 1—Inspector-General of Intelligence and Security

Appointment, functions, duties, and powers of Inspector-General

157 Appointment of Inspector-General

(1) There continues to be an office called the Inspector-General of Intelligence and Security.

(2) The Inspector-General is appointed by the Governor-General on the recommendation of the House of Representatives.

(3) Before a recommendation may be made under subsection (2), the Prime Minister must—

(a) consult the Intelligence and Security Committee about the proposed appointment; and

(b) advise the House of Representatives on the outcome of that consultation.

(4) The Inspector-General must hold a government-sponsored security clearance of a level determined by the Prime Minister.

Compare: 1996 No 47 s 5(1)(a), (2)

158 Functions of Inspector-General

(1) The functions of the Inspector-General are—

(a) to conduct an inquiry into any matter relating to an intelligence and security agency's compliance with New Zealand law, including human rights law, if that inquiry is requested by—

(i) the Minister responsible for the intelligence and security agency; or

(ii) the Intelligence and Security Committee:

(b) to conduct an inquiry into any matter where it appears that a New Zealand person has been or may be adversely affected by an act, omission, practice, policy, or procedure of an intelligence and security agency, if that inquiry is requested by—

(i) the Minister responsible for the intelligence and security agency; or

(ii) the Intelligence and Security Committee:

(c) to conduct an inquiry into the propriety of particular activities of an intelligence and security agency, if that inquiry is requested by—

(i) the Minister responsible for the intelligence and security agency; or

(ii) the Intelligence and Security Committee; or

(iii) the Prime Minister:

(d) to conduct an inquiry of the type referred to in paragraph (a), (b), or (c) on the Inspector-General's own initiative:

(e) to deal with complaints received under section 171:

(f) to conduct reviews, at intervals of not more than 12 months, of the effectiveness and appropriateness of—

(i) the procedures of each intelligence and security agency to ensure compliance with this Act in relation to the issue and execution of an authorisation; and

(ii) the compliance systems of each intelligence and security agency for operational activities, including all supporting policies and practices of an intelligence and security agency relating to—

(A) administration:

(B) information management:

(C) risk management:

(D) legal compliance generally:

(g) to conduct a review, on the Inspector-General's own initiative, of any activity carried out by an intelligence and security agency in the performance of its function under section 14:

(h) to conduct unscheduled audits of the procedures and compliance systems described in paragraph (f):

(i) to conduct a review in relation to either or both of the following:

(i) the issue of an authorisation:

(ii) the carrying out of an authorised activity:

(j) to conduct a review in relation to a permission granted under section 137 or 138:

(k) to conduct a review in relation to the issue of—

(i) approvals under section 147:

(ii) business records directions under section 150:

(l) to undertake all work programmes published under section 159:

(m) to perform any other functions conferred or imposed on the Inspector-General by or under this Act or any other enactment.

(2) In conducting any inquiry or review, the Inspector-General must take into account—

(a) any relevant ministerial policy statement; and

(b) the extent to which an intelligence and security agency has had regard to that statement.

(3) In this section, **authorisation** and **authorised activity** have the meanings given to them by section 47.

Compare: 1996 No 47 s 11(1)(a), (c), (ca), (d), (da), (f), (3)

159 Inspector-General to prepare and publish annual work programme

(1) At least 60 days before the beginning of each financial year, the Inspector-General must—

(a) prepare a draft proposed work programme for that year; and

(b) consult the Ministers on that proposed work programme.

(2) The Inspector-General, after having regard to any comments received from the Ministers, must finalise the annual work programme.

(3) As soon as practicable after the annual work programme is finalised, the Inspector-General—

(a) must give a copy to the Ministers; and

(b) may publish it on an Internet site maintained by or on behalf of the Inspector-General.

(4) In this section, **Ministers** means—

(a) the Minister responsible for the New Zealand Security Intelligence Service; and

(b) the Minister responsible for the Government Communications Security Bureau.

Compare: 1996 No 47 s 11(1)(e)

160 Disclosures to Inspector-General or Deputy Inspector-General

(1) This section applies if an employee of an intelligence and security agency brings any matter to the attention of the Inspector-General or Deputy Inspector-General.

(2) The employee must not be subjected by the intelligence and security agency to any penalty or discriminatory treatment of any kind in relation to his or her employment by reason only of having brought the matter to the attention of the Inspector-General or Deputy Inspector-General.

(3) However, subsection (2) does not apply if the Inspector-General determines that the employee did not act in good faith.

Compare: 1996 No 47 ss 5(4), 18

161 Consultation by Inspector-General

(1) In carrying out his or her functions, the Inspector-General must have regard to the functions of the Auditor-General in relation to an intelligence and security agency and may consult the Auditor-General about any matter with a view to avoiding inquiries being conducted into that matter by both the Inspector-General and the Auditor-General.

(2) The Inspector-General may—

(a) consult any of the persons specified in subsection (3) about any matter relating to the functions of the Inspector-General; and

(b) despite section 218(1), disclose to any of the persons consulted any information that the Inspector-General considers necessary for the purpose of the consultation.

(3) The persons are—

(a) the Auditor-General:

(b) an Ombudsman:

(c) the Privacy Commissioner:

(d) a Human Rights Commissioner:

(e) the Independent Police Conduct Authority:

(f) the State Services Commissioner.

(4) Nothing in this section limits the functions, duties, or powers of the Auditor-General, an Ombudsman, the Privacy Commissioner, a Human Rights Commissioner, the Independent Police Conduct Authority, or the State Services Commissioner under any enactment.

Compare: 1996 No 47 ss 12, 15(3)

162 Jurisdiction of courts and other agencies not affected

(1) To avoid doubt, the carrying out of the Inspector-General's functions does not limit the jurisdiction of any court.

(2) The carrying out by the Inspector-General of his or her functions does not affect the exercise by any Police employee of any powers that the Police employee may lawfully exercise in relation to—

(a) an intelligence and security agency; or

(b) the Director-General or any employee of an intelligence and security agency.

Compare: 1996 No 47 s 15(1), (2)

163 Reviews relating to authorisations and authorised activities

(1) If a review conducted under section 158(1)(i)(i) identifies any irregularity in the issue of an authorisation to an intelligence and security agency (an **irregular authorisation**),—

(a) the finding does not—

(i) invalidate the authorisation; or

(ii) invalidate any action taken by the intelligence and security agency, or any other person, in reliance on the authorisation or any information obtained under it; or

(iii) require any information obtained under the authorisation to be destroyed:

(b) the Inspector-General may report the irregular authorisation to—

(i) the Minister responsible for the intelligence and security agency and to the Chief Commissioner of Intelligence Warrants, in the case of an authorisation that—

(A) is a Type 1 intelligence warrant; or

(B) is given under section 78(2)(a); or

(ii) the Minister responsible for the intelligence and security agency, in the case of any other kind of authorisation.

(2) If a review conducted under section 158(1)(i)(ii) identifies any irregularity in the carrying out of an authorised activity by an intelligence and security agency (an **irregular activity**),—

(a) the finding does not—

(i) invalidate the authorisation that authorised the activity; or

(ii) make the activity unlawful; or

(iii) require any information obtained during the carrying out of the activity to be destroyed:

(b) the Inspector-General may report the irregular activity to—

(i) the Minister responsible for the intelligence and security agency and to the Chief Commissioner of Intelligence Warrants, in the case of an activity authorised by—

(A) a Type 1 intelligence warrant; or

(B) an authorisation given under section 78(2)(a); or

(ii) the Minister responsible for the intelligence and security agency, in the case of an activity authorised by any other kind of authorisation.

(3) The Inspector-General may include in his or her report under subsection (1)(b) or (2)(b) a recommendation that all or any specified information obtained under an irregular authorisation or as a result of irregular activity be destroyed.

Appointment, functions, duties, and powers of Deputy Inspector-General

164 Appointment of Deputy Inspector-General

(1) There continues to be an office called the Deputy Inspector-General of Intelligence and Security.

(2) The Deputy Inspector-General is appointed by the Governor-General on the recommendation of the House of Representatives.

(3) Before a recommendation may be made under subsection (2), the Prime Minister must—

(a) consult the Intelligence and Security Committee about the proposed appointment; and

(b) advise the House of Representatives on the outcome of that consultation.

(4) The Deputy Inspector-General must hold a government-sponsored security clearance of a level determined by the Prime Minister.

Compare: 1996 No 47 s 5(1)(b), (2)

165 Functions, duties, and powers of Deputy Inspector-General

(1) The Deputy Inspector-General has and may perform or exercise, to the same extent as the Inspector-General, all the functions, duties, and powers of the Inspector-General.

(2) The performance by the Deputy Inspector-General of the Inspector-General's functions and duties, and the exercise by the Deputy Inspector-General of the Inspector-General's powers, is subject to the control of the Inspector-General.

(3) If there is a vacancy in the office of the Inspector-General, or if the Inspector-General is absent from duty for any reason, the Deputy Inspector-General has and may perform or exercise all the functions, duties, and powers of the Inspector-General for as long as the vacancy or absence continues.

(4) The fact that the Deputy Inspector-General performs or exercises any function, duty, or power of the Inspector-General is, in the absence of evidence to the contrary, conclusive evidence of the Deputy Inspector-General's authority to do so.

Compare: 1996 No 47 s 5(3), (5), (6)

Administrative provisions

166 Administrative provisions relating to offices of Inspector-General and Deputy Inspector-General

Part 2 of Schedule 3 applies in relation to the offices of Inspector-General and Deputy Inspector-General.

Advisory panel

167 Advisory panel

There continues to be an advisory panel.

Compare: 1996 No 47 s 15A

168 Functions of advisory panel

(1) The functions of the advisory panel are—

(a) to provide advice to the Inspector-General—

(i) on request from the Inspector-General; or

(ii) on its own initiative:

(b) to report to the Prime Minister on any matter relating to intelligence and security if the advisory panel considers that the matter should be drawn to the attention of the Prime Minister.

(2) To assist the advisory panel to perform its functions, the Inspector-General may on his or her own initiative, or on request, provide any information to the advisory panel.

Compare: 1996 No 47 s 15B

169 Membership of advisory panel

(1) The advisory panel consists of 2 members appointed by the Governor-General on the recommendation of the Prime Minister made after consulting the Intelligence and Security Committee.

(2) Both members appointed under subsection (1) must hold a government-sponsored security clearance of a level determined by the Prime Minister.

Compare: 1996 No 47 s 15C(1)–(4)

170 Administrative provisions relating to advisory panel

Part 3 of Schedule 3 applies in relation to the membership and procedure of the advisory panel.

Complaints

171 Complaints that may be made to Inspector-General

(1) A complaint may be made to the Inspector-General under subsection (2), (3), or (4).

(2) A New Zealand person (not being a person referred to in subsection (3)) may complain that he or she has, or may have, been adversely affected by any act, omission, practice, policy, or procedure of an intelligence and security agency.

(3) An employee, or a former employee, of an intelligence and security agency may complain that he or she has, or may have, been adversely affected by any

act, omission, practice, policy, or procedure of an intelligence and security agency if—

(a) all established internal remedies have been exhausted; or

(b) the Director-General of the relevant intelligence and security agency agrees in writing.

(4) The Speaker of the House of Representatives on behalf of 1 or more members of Parliament may complain about any act, omission, practice, policy, or procedure of an intelligence and security agency.

Compare: 1996 No 47 s 11(1)(b), (ba), (5)

172 Form of complaint

(1) A complaint may be made orally or in writing.

(2) A complaint made orally must be put in writing as soon as practicable.

Compare: 1996 No 47 s 16(1)

173 Procedure on receipt of complaint

(1) As soon as practicable after receiving a complaint, the Inspector-General must consider the complaint and—

(a) decide to conduct an inquiry into the complaint; or

(b) decide, in accordance with section 174, not to conduct an inquiry into the complaint.

(2) As soon as practicable after making a decision under subsection (1), the Inspector-General must advise the complainant of that decision.

Compare: 1993 No 28 s 70

174 Inspector-General may decide not to inquire or continue to inquire into complaint

(1) The Inspector-General may decide not to conduct an inquiry into a complaint if it appears to the Inspector-General that,—

(a) under the law or existing administrative practice, the complainant has an adequate remedy or right of appeal (other than the right to petition the House of Representatives) and it is, or would have been, reasonable for the complainant to pursue that remedy or right of appeal; or

(b) the complaint relates to an act, omission, practice, policy, or procedure that the complainant has known about for more than 12 months; or

(c) the subject matter of the complaint is trivial; or

(d) the complaint is frivolous or vexatious or not made in good faith; or

(e) the complainant does not have a sufficient personal interest in the subject matter of the complaint; or

(f) having regard to all the circumstances of the case, and following preliminary inquiries, an inquiry is unnecessary.

(2) The Inspector-General may decide not to continue to conduct an inquiry into a complaint if, in the course of his or her inquiries, it appears to the Inspector-General that—

(a) any of the circumstances in subsection (1) apply; or

(b) having regard to all the circumstances of the case, the further conduct of the inquiry is unnecessary; or

(c) the matter that is the subject of the complaint is one that should be heard by a court or tribunal constituted by statute.

(3) As soon as practicable after making a decision under subsection (1) or (2), the Inspector-General must advise the complainant of that decision.

Compare: 1975 No 9 s 17; 1996 No 47 s 17

Procedure for inquiries

175 Commencing of inquiry

(1) After commencing an inquiry, the Inspector-General must notify the Director-General of the relevant intelligence and security agency of—

(a) the commencement of the inquiry; and

(b) the nature of the inquiry.

(2) If the inquiry relates to a complaint, the Inspector-General must also give to the Director-General of the relevant intelligence and security agency a copy of the complaint.

(3) If the inquiry is initiated by the Inspector-General in reliance on section 158(1)(d), the Inspector-General must advise the Minister responsible for the relevant intelligence and security agency of—

(a) the commencement of the inquiry; and

(b) the nature of the inquiry.

(4) In this section, **relevant intelligence and security agency** means the intelligence and security agency that the inquiry relates to.

Compare: 1996 No 47 s 19(1), (2)

176 Evidence

(1) The Inspector-General must conduct an inquiry in private.

(2) The Inspector-General may receive in evidence any statement, document, information, or matter that may, in the Inspector-General's opinion, assist him or her with the inquiry, whether or not the statement, document, information, or matter would be admissible in a court of law.

(3) The Inspector-General must allow a complainant to be heard, to be represented by counsel or any other person, and to have any other persons testify to the complainant's record, reliability, and character.

(4) If, at any time during an inquiry, it appears to the Inspector-General that there may be sufficient grounds for making any report or recommendation that may adversely affect an intelligence and security agency, any employee of an intelligence and security agency, or any other department or person, the Inspector-General must give that agency, employee, or person an opportunity to be heard.

(5) Subject to the provisions of this Act, the Inspector-General may regulate his or her procedure in the manner that he or she thinks fit.

Compare: 1996 No 47 s 19(4)–(8)

177 Evidence of breach of duty or misconduct by employee of intelligence and security agency

If, during the course of an inquiry, the Inspector-General forms the opinion that there is evidence of a breach of duty or misconduct by an employee of an intelligence and security agency, the Inspector-General must immediately advise—

(a) the Director-General of the intelligence and security agency; and

(b) the Minister responsible for the intelligence and security agency.

Compare: 1996 No 47 s 25(3)

178 Power to summon persons

(1) The Inspector-General may summon and examine on oath any person who the Inspector-General considers is able to give information relevant to the inquiry, and may for that purpose administer an oath to any person.

(2) Every examination by the Inspector-General under subsection (1) is to be treated as a judicial proceeding within the meaning of section 108 of the Crimes Act 1961 (which relates to perjury).

(3) Witnesses' fees, allowances, and expenses according to the scales for the time being prescribed by regulations made under the Criminal Procedure Act 2011—

(a) must be paid by the Inspector-General to any person who appears as a witness before the Inspector-General under a summons; and

(b) may, if the Inspector-General so decides, be paid by the Inspector-General to any other person who appears as a witness before the Inspector-General.

(4) The Inspector-General may disallow the whole or any part of a sum payable under subsection (3)(a).

Compare: 1996 No 47 s 23(2), (3), (6)

179 Power to require information and documents

The Inspector-General may require any person to provide—

(a) any information that the Inspector-General considers may be relevant to an inquiry; and

(b) any documents or things in the possession or under the control of that person that the Inspector-General considers may be relevant to an inquiry.

Compare: 1996 No 47 s 23(1)

180 Disclosure of information may be required despite obligation of secrecy

(1) A person who is obliged by the provisions of an enactment or otherwise to maintain secrecy in relation to, or not to disclose, any matter may be required to do the following even if compliance with the requirement would otherwise breach the obligation of secrecy or non-disclosure:

(a) give evidence to, or answer questions put by, the Inspector-General:

(b) provide information, documents, or things to the Inspector-General.

(2) Compliance with a requirement under subsection (1) is not a breach of the relevant obligation of secrecy or non-disclosure or of any enactment by which that obligation is imposed.

(3) This section is subject to section 181.

Compare: 1996 No 47 s 23(5)

181 Protection and privileges of witnesses

Every person who does the following has the same privileges as witnesses have in a court of law:

(a) gives evidence to, or answers questions put by, the Inspector-General:

(b) provides information, documents, or things to the Inspector-General.

Compare: 1996 No 47 s 23(4)

182 Information disclosed to Inspector-General privileged

Any information, document, or thing produced by any person in the course of an inquiry conducted by the Inspector-General is privileged in the same manner as if the inquiry were a proceeding in a court.

Compare: 1996 No 47 s 24(1)(b), (2), (3)

183 Inspector-General, etc, not compellable witnesses

(1) The following persons may not be required to give evidence in any court, or in proceedings of a judicial nature, in respect of anything that comes to their knowledge when they are performing or exercising their functions, duties, or powers:

(a) the Inspector-General, or any person who has held office as Inspector-General:

(b) the Deputy Inspector-General, or any person who has held office as Deputy Inspector-General:

(c) a person who is, or has been, employed by the Inspector-General:

(d) a person who is, or has been, a member of the advisory panel.

(2) Nothing in subsection (1) applies in respect of proceedings for—

(a) an offence against section 219; or

(b) an offence against section 78, 78AA(1), 78A(1), 105, 105A, or 105B of the Crimes Act 1961; or

(c) an offence of conspiring to commit an offence against any of those sections of the Crimes Act 1961; or

(d) an offence of attempting to commit an offence against any of those sections of the Crimes Act 1961.

Compare: 1996 No 47 s 24(1)(b), (2), (3)

184 Power of entry

(1) For the purposes of an inquiry, the Inspector-General may enter, at any reasonable time, any premises or place occupied or used by an intelligence and security agency.

(2) The Inspector-General must give prior notice to the Director-General of the intelligence and security agency of his or her intention to exercise the power in subsection (1).

Compare: 1996 No 47 s 21

Procedure on completion of inquiry

185 Inspector-General to prepare report on completion of inquiry

(1) On the completion of an inquiry, the Inspector-General must prepare a written report containing his or her conclusions and recommendations.

(2) In the case of an inquiry conducted in relation to a complaint, the report may include any recommendations for the redress of that complaint that the Inspector-General considers appropriate (including remedies that involve the payment of compensation).

(3) The Inspector-General must send the report to—

(a) the Minister responsible for the intelligence and security agency to which the inquiry relates; and

(b) the Director-General of the intelligence and security agency to which the inquiry relates; and

(c) the Prime Minister, if the inquiry was conducted at the request of the Prime Minister; and

(d) the Intelligence and Security Committee, if the inquiry was conducted at the request of the Committee.

(4) If the inquiry was not conducted at the request of the Intelligence and Security Committee, the Inspector-General may send the report to the Committee if—

(a) the inquiry was conducted on the Inspector-General's own initiative and the responsible Minister agrees to the report being sent to the Intelligence and Security Committee; or

(b) the inquiry was conducted at the request of a Minister responsible for the intelligence and security agency, and the Minister agrees to the report being sent to the Intelligence and Security Committee; or

(c) the inquiry was conducted at the request of the Prime Minister, and the Prime Minister agrees to the report being sent to the Intelligence and Security Committee.

(5) In the case of an inquiry conducted in relation to a complaint, the Inspector-General must advise the complainant of his or her conclusions in terms that will not prejudice—

(a) the security or defence of New Zealand; or

(b) the international relations of the Government of New Zealand.

(6) The Inspector-General may, after consulting the Director-General of the intelligence and security agency concerned, determine the security classification of the report.

(7) Despite subsection (6), if a report quotes or summarises any matter that has a security classification, then the quote or summary of that matter in the report must not be given a lower security classification.

Compare: 1996 No 47 ss 11(6), 25(1), (2), (8)

186 Advice on compliance with Inspector-General's recommendations

The Inspector-General may advise the Minister who received a report under section 185(3)(a) on—

(a) the compliance by an intelligence and security agency with the recommendations in that report; and

(b) the adequacy of any remedial or preventative measures taken by an intelligence and security agency following an inquiry.

Compare: 1996 No 47 s 25(5)

187 Minister to respond to Inspector-General's report

(1) As soon as practicable after receiving a report from the Inspector-General under section 185(3)(a), the Minister must provide his or her response to—

(a) the Inspector-General; and

(b) the Director-General of the intelligence and security agency concerned.

(2) If the report relates to an inquiry that was conducted at the request of the Intelligence and Security Committee, the Minister must also provide his or her response to the Committee.

(3) If the report relates to an inquiry that was not conducted at the request of the Intelligence and Security Committee, the Minister may provide his or her response to the Committee.

(4) This section does not apply to the extent that a report relates to an employment matter or a security clearance issue.

Compare: 1996 No 47 s 25(6), (7)

188 Publication of Inspector-General's report

(1) As soon as practicable after sending a report in accordance with section 185(3), the Inspector-General must make the report publicly available on an Internet site maintained by or on behalf of the Inspector-General.

(2) However, the Inspector-General must not, in the report made publicly available under subsection (1), disclose—

(a) information that, if publicly disclosed, would be likely to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence—

(i) by the Government of any other country or any agency of such a Government; or

(ii) by an international organisation; or

(b) information that, if publicly disclosed, would be likely to endanger the safety of any person; or

(c) the identity of any person who is or has been an officer, employee, or agent of an intelligence and security agency other than the Director-General, or any information from which the identity of such a person could reasonably be inferred; or

(d) information that, if publicly disclosed, would be likely to prejudice—

(i) the continued performance of the functions of an intelligence and security agency; or

(ii) the security or defence of New Zealand or the international relations of the Government of New Zealand; or

(e) any information about employment matters or security clearance issues.

Compare: 1996 No 47 s 25A

189 Return of documents, etc, after inquiry

(1) On completion of an inquiry, the Inspector-General must return to the intelligence and security agency concerned all information, documents, and things relating to the inquiry that the Inspector-General obtained from that agency.

(2) All other information, documents, and things relating to the inquiry in the possession of the Inspector-General must be—

(a) kept by the Inspector-General in safe custody in accordance with the requirements for the safe custody of documents applying to intelligence and security agencies; or

(b) disposed of by the Inspector-General in accordance with the requirements for the disposal of documents applying to intelligence and security agencies.

Compare: 1996 No 47 s 25(4)

190 Proceedings not to be questioned or reviewed

No proceeding, report, or finding of the Inspector-General may be challenged, reviewed, quashed, or called into question in any court except on the ground of lack of jurisdiction.

Compare: 1996 No 47 s 19(9)

191 Offence to publish information relating to inquiry

(1) A person commits an offence if the person, without the written consent of the relevant Minister, publishes or broadcasts, or causes to be published or broadcast, or otherwise distributes or discloses,—

(a) any complaint that is before the Inspector-General; or

(b) any decision of the Inspector-General relating to a complaint or an inquiry; or

(c) any report or account of any inquiry conducted by the Inspector-General; or

(d) any decision of the relevant Minister relating to a complaint or an inquiry.

(2) Subsection (1) does not apply to the publication, broadcast, distribution, or disclosure of—

(a) advice provided to a complainant by the Inspector-General under section 185(5); or

(b) a report made publicly available by the Inspector-General under section 188(1) or 222(7); or

(c) any material that the Inspector-General has approved for release (the approval being given in writing after the Inspector-General has consulted, in relation to security requirements, the Director-General of the intelligence and security agency to which the inquiry or complaint relates); or

(d) the fact only that an inquiry has been conducted by the Inspector-General.

(3) A person who commits an offence against this section is liable on conviction to—

(a) a term of imprisonment not exceeding 2 years; or

(b) a fine not exceeding $10,000.

(4) A prosecution for an offence under this section may not be commenced without the leave of the Attorney-General.

(5) Nothing in this section restricts—

(a) the communication of proceedings in Parliament; or

(b) the reporting of proceedings in Parliament.

(6) In this section,—

communication has the meaning given to it by section 5(1) of the Parliamentary Privilege Act 2014

proceedings in Parliament has the meaning given to it by section 10 of the Parliamentary Privilege Act 2014

relevant Minister means the Minister responsible for the intelligence and security agency to which the complaint or inquiry relates.

Compare: 1996 No 47 s 29

Subpart 2—Intelligence and Security Committee

Continuation of Intelligence and Security Committee

192 Intelligence and Security Committee

There continues to be an Intelligence and Security Committee.

Compare: 1996 No 46 s 5

193 Functions of Committee

(1) The functions of the Committee are—

(a) to examine the policy, administration, and expenditure of each intelligence and security agency:

(b) to receive and consider the annual report of each intelligence and security agency:

(c) to conduct each year, following receipt of the annual report of an intelligence and security agency, an annual review of the agency for the immediately preceding financial year:

(d) to consider any Bill, petition, or other matter in relation to an intelligence and security agency referred to the Committee by the House of Representatives:

(e) to request the Inspector-General to conduct an inquiry into—

(i) any matter relating to an intelligence and security agency's compliance with New Zealand law, including human rights law:

(ii) the propriety of particular activities of an intelligence and security agency:

(f) to consider any matter (not being a matter relating directly to the activities of an intelligence and security agency) referred to the Committee by the Prime Minister because of that matter's intelligence or security implications:

(g) to consider and discuss with the Inspector-General his or her annual report.

(2) However, the functions of the Committee do not include—

(a) inquiring into any matter within the jurisdiction of the Inspector-General; or

(b) inquiring into any matter that is operationally sensitive, including any matter that relates to intelligence collection and production methods, or sources of information; or

(c) inquiring into complaints by individuals concerning the activities of an intelligence and security agency that are capable of being resolved under any other enactment.

Compare: 1996 No 46 s 6

194 Membership of Committee

(1) The size of the Committee must be determined by the Prime Minister in consultation with the Leader of the Opposition, but the Committee must comprise—

(a) a minimum of 5 members; and

(b) a maximum of 7 members.

(2) The membership of the Committee must comprise—

(a) the Prime Minister; and

(b) the Leader of the Opposition; and

(c) members of the House of Representatives nominated by the Leader of the Opposition, with the agreement of the Prime Minister, after consultation with the leader of each party that is not in government or in coalition with a Government party; and

(d) members of the House of Representatives nominated by the Prime Minister after consultation with the leader of each party in government.

(3) If it is determined that the Committee should comprise 5 members,—

(a) 1 member must be nominated under subsection (2)(c); and

(b) 2 members must be nominated under subsection (2)(d).

(4) If it is determined that the Committee should comprise 6 or 7 members,—

(a) 2 members must be nominated under subsection (2)(c); and

(b) the balance of the members must be nominated under subsection (2)(d).

(5) When nominating a person for membership of the Committee, the Leader of the Opposition and the Prime Minister must have regard to security requirements and the proportional representation of political parties in the House of Representatives.

(6) When performing the Committee's functions, a member of the Committee acts in his or her official capacity as a member of Parliament.

Compare: 1996 No 46 s 7(1), (2), (4)

195 Filling vacancy in membership of Committee

(1) If the office of a member nominated under section 194(2)(c) becomes vacant, the Leader of the Opposition must nominate, in accordance with section 194(2)(c), another member of the House of Representatives to fill that vacancy.

(2) If the office of a member nominated under section 194(2)(d) becomes vacant, the Prime Minister—

(a) must nominate, in accordance with section 194(2)(d), another member of the House of Representatives to fill that vacancy, if the vacancy leaves the Committee with fewer than 6 members:

(b) may nominate, in accordance with section 194(2)(d), another member of the House of Representatives to fill that vacancy, if the vacancy leaves the Committee with 6 members.

Compare: 1996 No 46 s 11

196 Endorsement of nominated members

(1) The Prime Minister must, as soon as practicable after the commencement of each Parliament, present to the House of Representatives, for endorsement as members of the Committee, the names of the members of the House of Representatives nominated under—

(a) section 194(2)(c) and (d); and

(b) section 195 (if any).

(2) If the House of Representatives declines to endorse any nomination, the Prime Minister must present to the House of Representatives, for endorsement as a member of the Committee, the name of another member of the House of Representatives nominated by the Leader of the Opposition under section 194(2)(c), or the Prime Minister under section 194(2)(d), as the case requires.

Compare: 1996 No 46 s 8(1), (2)

197 Committee not to transact business until nominated members endorsed

The Committee must not transact any business until the required number of nominations for the membership under section 194(2)(c) and (d) has been endorsed.

Compare: 1996 No 46 s 8(3)

198 Chairperson of Committee

(1) The Committee is chaired by—

(a) the Prime Minister; or

(b) another member of the Committee from time to time appointed by the Prime Minister.

(2) The Prime Minister must not chair a meeting of the Committee, and must appoint one of the members referred to in section 194(2)(d) to act as chairperson of that meeting, if—

(a) the Committee is, in the course of conducting a financial review of an intelligence and security agency, discussing any matter relating to the performance of that agency; and

(b) the Prime Minister is the Minister responsible for that agency.

(3) The chairperson may appoint either of the following (if not already a member of the Committee) as an alternative chairperson in his or her absence at a meeting of the Committee:

(a) the Deputy Prime Minister:

(b) the Attorney-General.

Compare: 1996 No 46 ss 7(3), 7A(1)–(3)

199 Privilege

(1) The proceedings of the Committee are proceedings in Parliament for the purposes of Article 9 of the Bill of Rights 1688 and the Parliamentary Privilege Act 2014.

(2) Anything said, any information supplied, or any document, paper, or thing produced by any person in the course of any inquiry or proceedings of the Committee under this Act is privileged as proceedings in Parliament (as defined in section 10 of the Parliamentary Privilege Act 2014).

Compare: 1996 No 46 s 16

200 Administrative provisions relating to Committee

Part 4 of Schedule 3 applies in relation to the Committee.

Evidence

201 Attendance before Committee

(1) The Director-General of an intelligence and security agency must appear before the Committee if requested by the Committee.

(2) The Committee may request any person other than the Director-General of an intelligence and security agency—

(a) to attend and give evidence before the Committee; or

(b) to produce any document or other information that is relevant to the proceedings of the Committee.

(3) A request made to a person under subsection (1) or (2) must, wherever practicable, be given to that person by the Committee at least 5 working days before the date on which the person is requested—

(a) to appear; or

(b) to attend and give evidence; or

(c) to produce any document or other information.

Compare: 1996 No 46 s 14

202 Meaning of sensitive information

(1) In sections 203 and 204, **sensitive information** means information of a kind specified in subsection (2) that, if disclosed, would be likely—

(a) to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand; or

(b) to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by—

(i) the Government of any other country or any agency of such a Government; or

(ii) any international organisation; or

(c) to prejudice the maintenance of the law, including the prevention, investigation, and detection of offences and the right to a fair trial; or

(d) to endanger the safety of any person.

(2) The kinds of information are as follows:

(a) information that might lead to the identification of, or contain details of,—

(i) sources of information available to an intelligence and security agency; or

(ii) other assistance or operational methods available to an intelligence and security agency; and

(b) information about particular operations that have been undertaken, or are being or are proposed to be undertaken, in performing any of the functions of an intelligence and security agency; and

(c) information that has been provided to an intelligence and security agency by another department or agency of the Government of New Zealand and is information that cannot be disclosed by the intelligence and security agency without the consent of the department or agency of the Government of New Zealand that provided that information; and

(d) information that has been provided to an intelligence and security agency by the Government of any other country or by an agency of such a Government and is information that cannot be disclosed by the intelligence and security agency without the consent of the Government or agency that provided that information.

203 Provision of information to Committee

(1) If the Director-General of an intelligence and security agency or any other person is asked by the Committee to disclose any document or other information in his or her possession that is relevant to the matters being considered by the Committee, the Director-General or other person must, subject to subsections (2) and (3),—

(a) arrange for that document or information to be made available to the Committee; or

(b) inform the Committee that the document or information cannot be disclosed because, in the opinion of the Director-General of the relevant intelligence and security agency, that document or information is sensitive information.

(2) The fact that any particular document or information is sensitive information does not prevent the disclosure of the document or information under subsection (1)(a) if,—

(a) in any case where the document or information is in the possession or under the control of the Director-General of an intelligence and security agency, the Director-General considers it safe to disclose it; or

(b) in any case where the document or information is in the possession or under the control of any other person, the Director-General of the relevant intelligence and security agency considers it safe to disclose it.

(3) If any document or information is sensitive information within the meaning of that term in section 202(1) and (2)(a), (b), or (c), that document or information must be disclosed to the Committee if the Prime Minister considers that the disclosure is desirable in the public interest.

(4) If any document or other information that has a security classification is provided to the Committee, the Committee must ensure that the document or information—

(a) is kept in safe custody in accordance with the requirements applying to the safe custody of documents in the intelligence and security agencies; and

(b) is returned to the originating intelligence and security agency when no longer required by the Committee.

(5) If the Committee is responsible for the production of a document that has a security classification, the Committee must ensure that the document is kept in

safe custody in accordance with the requirements applying to the safe custody of documents in the intelligence and security agencies.

Compare: 1996 No 46 s 17

204 Secrecy of information disclosed to Committee

(1) A person who has been appointed to assist the Committee or who has appeared before the Committee in any capacity must not disclose or publish, or cause to be disclosed or published,—

(a) any sensitive information disclosed to the Committee under section 203(2) or (3); or

(b) any other information provided to the Committee by an intelligence and security agency the further disclosure of which would be likely to prejudice any of the interests protected by—

(i) section 224(2)(a) to (c); or

(ii) section 224(3).

(2) Subsection (1) does not apply if the disclosure or publication of the information—

(a) is in the performance of the person's functions or duties under this Act; or

(b) is in accordance with the rules and practice of the House of Representatives; or

(c) is in the exercise of the person's powers under this Act; or

(d) is authorised in writing by the Committee or its chairperson.

(3) A person must not disclose to any other person any minutes or other record relating to the proceedings of any meeting of the Committee unless—

(a) the disclosure of the minutes or record is necessary for the purposes of—

(i) a report to the House of Representatives (being a report that complies with section 222); or

(ii) the conduct of the business of the Committee; or

(b) the disclosure is authorised in writing by the Committee or its chairperson.

Compare: 1996 No 46 s 19

205 Committee's records may be copied to House of Representatives

(1) The House of Representatives may require the Committee to provide to it a copy of any or all records held by the Committee in relation to the performance of its functions under section 193(1)(a) to (d).

(2) Before providing a copy of any record to the House of Representatives, the Committee must remove any protected information.

(3) In this section,—

protected information means information that, under section 224, may not be disclosed by the Committee in a report to the House of Representatives

records means the records of the proceedings of the Committee, including records of reports, evidence, and advice received by the Committee during the course of proceedings.

Part 7
Miscellaneous provisions

Ministerial policy statements

206 Issue of ministerial policy statements

The Minister responsible for an intelligence and security agency must issue 1 or more ministerial policy statements that provide guidance to the intelligence and security agency in relation to the following matters:

(a) providing information assurance and cybersecurity activities under section 11 with consent (*see* section 12):

(b) acquiring, using, and maintaining an assumed identity under subpart 1 of Part 3:

(c) creating and maintaining a legal entity under subpart 2 of Part 3:

(d) collecting information lawfully from persons without an intelligence warrant or authorisation given under section 78:

(e) conducting surveillance in a public place:

(f) obtaining and using publicly available information:

(g) requesting information from agencies under section 121:

(h) the management of information obtained by an intelligence and security agency, including the retention and destruction of that information:

(i) making false or misleading representations under section 228 about being employed with an intelligence and security agency:

(j) conducting activities in accordance with an exemption from the Land Transport (Road User) Rule 2004 that is conferred by section 231.

207 Issue of ministerial policy statements relating to co-operating, etc, with overseas public authorities

(1) The Minister responsible for an intelligence and security agency must issue 1 or more ministerial policy statements providing guidance to the intelligence and security agency in relation to the following matters:

(a) co-operating with an overseas public authority:

(b) providing advice and assistance to an overseas public authority:

(c) sharing intelligence with an overseas public authority.

(2) The Minister must provide to the Intelligence and Security Committee a copy of a ministerial policy statement issued under subsection (1).

208 Issue of additional ministerial policy statements

The Minister responsible for an intelligence and security agency may, if the Minister considers it necessary or desirable, issue 1 or more ministerial policy statements that provide guidance to the intelligence and security agency in relation to any other matter.

209 Effect of ministerial policy statement

In making any decision or taking any action, the Director-General of an intelligence and security agency and every employee of that agency must have regard to any relevant ministerial policy statement.

210 Content of ministerial policy statements

A ministerial policy statement must, without limitation, state—

(a) the procedures of an intelligence and security agency for authorising the carrying out of an activity relating to a matter (if applicable); and

(b) the protections that need to be in place in relation to the matter (if any); and

(c) the restrictions in relation to the matter (if any).

211 Consultation on proposed ministerial policy statements

Before issuing a ministerial policy statement, a Minister must—

(a) consult—

(i) the Inspector-General; and

(ii) any other Minister of the Crown whose area of responsibility, in the Minister's opinion, includes an interest in the proposed ministerial policy statement; and

(iii) any other person that the Minister considers appropriate; and

(b) have regard to any comments received under paragraph (a).

212 Amending, revoking, or replacing ministerial policy statements

(1) The Minister who issued a ministerial policy statement may, at any time, amend, revoke, or replace the ministerial policy statement.

(2) However, before amending, revoking, or replacing a ministerial policy statement, the Minister must—

(a) consult with, and invite comment from,—

(i) the Inspector-General; and

(ii) any other Minister of the Crown whose area of responsibility, in the Minister's opinion, includes an interest in the ministerial policy statement; and

(iii) any other person that the Minister considers appropriate; and

(b) have regard to any comments received under paragraph (a).

213 Ministerial policy statements applying to both intelligence and security agencies

(1) A ministerial policy statement that provides guidance to both intelligence and security agencies may be issued.

(2) If there is a different Minister responsible for each intelligence and security agency,—

(a) the ministerial policy statement must be jointly issued by the Ministers; and

(b) sections 211 and 212 apply with all necessary modifications.

214 Duration of ministerial policy statement

A ministerial policy statement—

(a) takes effect from the date on which it is signed by the Minister who issued it; and

(b) continues in effect for a period not exceeding 3 years.

215 Publication of ministerial policy statements

(1) As soon as practicable after a ministerial policy statement is issued, amended, or replaced, the Director-General of the intelligence and security agency to which the statement applies or, if the statement applies to both intelligence and security agencies, the Director-General of each agency—

(a) must make the statement publicly available on an Internet site maintained by or on behalf of the Director-General; and

(b) may make copies of the statement available in any other way that the Director-General considers appropriate in the circumstances.

(2) However, a Director-General must not, in the statement made publicly available under subsection (1), disclose any information that, if publicly disclosed, would be likely to prejudice—

(a) the carrying out of the activity to which the statement relates; or

(b) the security and defence of New Zealand; or

(c) the international relations of the Government of New Zealand.

216 Status of ministerial policy statements

A ministerial policy statement is—

(a) not—

(i) a legislative instrument for the purposes of the Legislation Act 2012; or

(ii) a disallowable instrument for the purposes of the Legislation Act 2012; and

(b) not required to be presented to the House of Representatives under section 41 of the Legislation Act 2012.

Security records

217 Powers in relation to security records

(1) For the purpose of performing his or her functions and duties, the Inspector-General must be given access to all security records—

(a) that are in the custody or control of an intelligence and security agency; and

(b) that the Inspector-General considers to be relevant to his or her functions or duties.

(2) The Inspector-General must ensure that all security records accessed under subsection (1) and held by him or her are kept in safe custody in accordance with the requirements for the safe custody of documents applying to intelligence and security agencies.

(3) If the Inspector-General is responsible for the production of any security records that have a security classification, the Inspector-General must ensure that the security records are kept in safe custody in accordance with the requirements for the safe custody of documents applying to intelligence and security agencies.

Compare: 1996 No 47 s 20

218 Disclosure of information relating to activities of intelligence and security agency

(1) The following persons must not, other than in the performance of their functions or duties, disclose to any other person any security records or other official information relating to the activities of an intelligence and security agency:

(a) the Inspector-General:

(b) the Deputy Inspector-General:

(c) an employee of the Inspector-General:

(d) a member of the advisory panel.

(2) Subsection (1) does not limit the disclosure of information concerning the activities of an intelligence and security agency to the Minister responsible for the intelligence and security agency.

(3) The Inspector-General must act in accordance with any certificate given by the Minister responsible for an intelligence and security agency that certifies—

(a) that the disclosure by the Inspector-General of any security records or any other official information would be likely—

(i) to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand; or

(ii) to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by the Government of any other country or any agency of such a Government; or

(iii) to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by any international organisation; or

(iv) to endanger the safety of any person; and

(b) that such disclosure—

(i) should not be made; or

(ii) should be made only on any terms and conditions that are, in the Minister's opinion, necessary in the interests of security.

(4) A Minister may not exercise his or her power under subsection (3) until the Minister has consulted—

(a) the Director-General of the relevant intelligence and security agency; and

(b) any other person (not being, in the case of a complaint, the complainant) capable of assisting in determining the circumstances and information that are relevant to the inquiry, being circumstances and information that should not, in the interests of security, be disclosed in the course of or in relation to the inquiry.

Compare: 1996 No 47 s 26

Confidentiality

219 Duty of confidentiality

(1) This section applies to any person who is, or has at any time been,—

(a) appointed as—

(i) Inspector-General:

(ii) Deputy Inspector-General:

(iii) Director-General of Security:

(iv) Director-General of the Government Communications Security Bureau:

(v) a member of the advisory panel:

(vi) a person assisting the Inspector-General:

(vii) a reviewer:

(b) employed or engaged by—

(i) the Inspector-General:

(ii) the Director-General of Security:

(iii) the Director-General of the Government Communications Security Bureau.

(2) Unless otherwise authorised by a Minister responsible for an intelligence and security agency, a person—

(a) must keep confidential all information that comes to his or her knowledge in the performance or exercise of his or her functions, duties, and powers; and

(b) must not make a record of or use or disclose that information except for the purpose of carrying out his or her functions or duties under, or for the purpose of giving effect to, this Act.

(3) A person who contravenes subsection (2) commits an offence and is liable on conviction to—

(a) a term of imprisonment not exceeding 2 years; or

(b) a fine not exceeding $10,000.

(4) The leave of the Attorney-General must be obtained before an offence against subsection (2) is prosecuted.

(5) A person to whom this section applies is an **official** for the purposes of sections 105 and 105A of the Crimes Act 1961.

(6) In this section, **reviewer** means a reviewer appointed under section 236(1).

Compare: 1969 No 24 s 12A; 1996 No 46 s 19; 1996 No 47 s 28; 2003 No 9 s 11; 2004 No 38 s 19

Security clearance information

220 Use of information provided for security clearance assessment

(1) Any information obtained by or disclosed to the New Zealand Security Intelligence Service for the purpose of a security clearance assessment may be used only for the following purposes:

(a) the security clearance assessment:

(b) any other security clearance assessment:

(c) counter-intelligence.

(2) Subsection (1) applies despite anything in information privacy principle 10 in section 6 of the Privacy Act 1993.

(3) In this section,—

counter-intelligence means the intelligence activities carried out to identify and counteract the threat, or potential threat, of unauthorised disclosure of official information by a person who holds, or has held, a New Zealand Government-sponsored national security clearance

security clearance assessment means an assessment conducted by the New Zealand Security Intelligence Service in the performance of its function under section 11 for the purpose of making a recommendation as to an individual's suitability to hold a New Zealand Government-sponsored national security clearance.

Annual reports

221 Annual reports of intelligence and security agencies

(1) As soon as practicable after the end of each financial year, the Director-General of each intelligence and security agency must provide to the Minister responsible for that intelligence and security agency a report (an **annual report**) on the activities of the agency during that year.

(2) An annual report must contain the information required by section 45 of the Public Finance Act 1989 and, additionally, include—

(a) a statement as to the number of occasions on which the agency has provided assistance under section 13(1)(b) to—

(i) the New Zealand Police; and

(ii) the New Zealand Defence Force; and

(b) a statement as to the number of occasions on which the agency has provided assistance under section 14; and

(c) a statement as to the number of applications made by the agency for the following:

(i) a Type 1 intelligence warrant; and

(ii) a Type 2 intelligence warrant; and

(iii) the urgent issue of a Type 1 intelligence warrant under section 71; and

(iv) the urgent issue of a Type 2 intelligence warrant under section 72; and

(v) a joint Type 1 intelligence warrant under section 56; and

(vi) a joint Type 2 intelligence warrant under section 56; and

(d) a statement as to the number of applications referred to in each of subparagraphs (i) to (vi) of paragraph (c) that were—

(i) approved; and

(ii) declined; and

(e) a statement as to the number of authorisations given by the Director-General under section 78; and

(f) a statement as to the number of applications made by the agency under section 136 for permission to access restricted information; and

(g) a statement as to the number of applications referred to in paragraph (f) that were—

(i) approved; and

(ii) declined; and

(h) a statement as to the number of business records directions issued by the agency to business agencies under section 150; and

(i) a statement setting out—

(i) a summary of the agency's equal employment opportunities programme for the year; and

(ii) an account of the extent to which the agency was, during the year, able to meet that programme.

(3) As soon as practicable after receiving an annual report, the Minister must give a copy to the Intelligence and Security Committee.

(4) Within 30 working days after receiving an annual report, the Minister must present a copy of the report to the House of Representatives in which—

(a) the financial statements are replaced with a statement recording the total of the actual expenses and capital expenditure incurred by the agency for the year against the agency's appropriation for that financial year; and

(b) information may be deleted in accordance with a direction of the Minister under subsection (5).

(5) Before presenting a copy of an annual report to the House of Representatives, the Minister may direct that any information (other than the statements referred to in subsections (2) and (4)(a)) be excluded from the report if the Minister considers that the information, if publicly disclosed, would be likely—

(a) to prejudice the security or defence of New Zealand or international relations of the Government of New Zealand; or

(b) to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by the Government of any other country or any agency of such a Government; or

(c) to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by any international organisation; or

(d) to endanger the safety of any person; or

(e) to prejudice the privacy of an individual.

(6) As soon as practicable after an annual report has been presented to the House of Representatives, the agency must make a copy of the report (as presented to

the House of Representatives) publicly available on an Internet site maintained by or on behalf of the agency.

(7) In this section,—

equal employment opportunities programme has the meaning given to it by section 58(3) of the State Sector Act 1988

working day has the meaning given to it by section 2(1) of the Public Finance Act 1989.

Compare: 1969 No 24 s 4J; 1989 No 44 ss 44(4), 45E(1)(c)(ii); 2003 No 9 s 12

222 Annual report of Inspector-General

(1) As soon as practicable after the end of each financial year, the Inspector-General must provide a report of the Inspector-General's operations during that year to—

(a) each Minister responsible for an intelligence and security agency; and

(b) the Prime Minister.

(2) The report must—

(a) specify the number of inquiries undertaken by the Inspector-General during the year; and

(b) contain a brief description of the outcome of each inquiry; and

(c) certify the extent to which each intelligence and security agency's compliance systems are sound; and

(d) contain any other information that the Inspector-General believes is necessary.

(3) The Prime Minister must, as soon as practicable after receiving a report under subsection (1), present a copy of the report to the House of Representatives, together with a statement as to whether any matter has, under subsection (4), been excluded from that copy.

(4) The Prime Minister may exclude from the copy of the report to be presented to the House of Representatives any matter that the Prime Minister, after consultation with the Inspector-General, considers is likely, if disclosed,—

(a) to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand; or

(b) to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by the Government of any other country or any agency of such a Government; or

(c) to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by any international organisation; or

(d) to endanger the safety of any person.

(5) The Prime Minister must, as soon as practicable, provide the Leader of the Opposition with a copy of a report that he or she has received under subsection (1).

(6) If the copy supplied to the Leader of the Opposition under subsection (5) contains any matter excluded by the Prime Minister from the copy presented to the House of Representatives, the Leader of the Opposition must not disclose that matter to any other person.

(7) As soon as practicable after a copy of a report is presented to the House of Representatives under subsection (3), the Inspector-General must make a copy of the report (as presented to the House of Representatives) publicly available on an Internet site maintained by or on behalf of the Inspector-General.

(8) The Inspector-General may at any time, with the agreement of the Prime Minister, report either generally or in respect of any particular matter to the Intelligence and Security Committee.

Compare: 1996 No 47 s 27

223 Annual report of Intelligence and Security Committee

(1) The Intelligence and Security Committee must present an annual report to the House of Representatives on the activities of the Committee.

(2) Subsection (1) is subject to section 224.

Compare: 1996 No 46 s 6(1)(e)(i)

224 Restrictions on reports to House of Representatives

(1) The Intelligence and Security Committee must, when presenting an annual report or any other report to the House of Representatives, have regard generally to security requirements.

(2) The Intelligence and Security Committee must not disclose in a report to the House of Representatives—

(a) any information that, if publicly disclosed, would be likely to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence—

(i) by the Government of any other country or any agency of such a Government; or

(ii) by any international organisation; or

(b) any information that, if publicly disclosed, would be likely to endanger the safety of any person; or

(c) any sensitive information disclosed to the Committee in accordance with section 203(2) or (3).

(3) The Intelligence and Security Committee must not disclose in a report to the House of Representatives the following information unless the Committee considers that there are compelling reasons in the public interest to do so:

(a) the identity of any person who is or has been an officer, employee, or agent of an intelligence and security agency, other than the Director-General, or any information from which the identity of such a person could reasonably be inferred; or

(b) any information that, if publicly disclosed, would be likely—

(i) to prejudice the continued performance of the functions of an intelligence and security agency; or

(ii) to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand.

Compare: 1996 No 46 s 18

Offences

225 Obstructing, hindering, resisting, or deceiving Inspector-General

(1) A person commits an offence and is liable on conviction to a fine not exceeding $5,000 if the person,—

(a) without lawful justification or excuse,—

(i) wilfully obstructs, hinders, or resists the Inspector-General in the exercise of his or her powers under this Act or any other enactment; or

(ii) refuses or wilfully fails to comply with any lawful requirement of the Inspector-General; or

(b) wilfully makes any false statement to, or misleads or attempts to mislead, the Inspector-General in the exercise of his or her powers under this Act or any other enactment.

(2) In this section, **Inspector-General** includes the Deputy Inspector-General.

Compare: 1996 No 47 s 23(8)

226 Personation

(1) A person commits an offence if the person, without reasonable excuse and in circumstances likely to lead another person to believe that the person is an employee of an intelligence and security agency,—

(a) pretends to be an employee of an intelligence and security agency by his or her words, conduct, or demeanour; or

(b) assumes the name, designation, or description of an employee of an intelligence and security agency.

(2) A person who commits an offence against this section is liable on conviction to—

(a) a term of imprisonment not exceeding 12 months; or

(b) a fine not exceeding $15,000; or

(c) both (a) and (b).

Compare: 1969 No 24 s 13; 2008 No 72 s 48

227 Restriction on publication and broadcasting of information regarding employees

(1) A person commits an offence if the person, without the written consent of the relevant Minister, publishes in a newspaper or other document, or broadcasts by radio or television, the fact that any person—

(a) is an employee of an intelligence and security agency, not being—

(i) the Director-General of Security; or

(ii) the Director-General of the Government Communications Security Bureau; or

(b) is connected in any way with an employee of an intelligence and security agency.

(2) Nothing in this section restricts—

(a) the communication of proceedings in Parliament; or

(b) the reporting of proceedings in Parliament.

(3) The written consent of the Minister in relation to any proceedings in any court may be filed in the court, and when so filed is sufficient authority to all persons to act in accordance with that consent.

(4) In this section,—

broadcast includes cause or allow to be broadcast

communication has the meaning given to it by section 5(1) of the Parliamentary Privilege Act 2014

proceedings in Parliament has the meaning given to it by section 10 of the Parliamentary Privilege Act 2014

publish includes cause or allow to be published

relevant Minister means the Minister responsible for the intelligence and security agency referred to in subsection (1).

(5) A person who commits an offence against this section is liable on conviction,—

(a) in the case of an individual, to a fine not exceeding $5,000:

(b) in the case of a body corporate, to a fine not exceeding $20,000.

Compare: 1969 No 24 s 13A

False or misleading representations about employment and identity

228 Employee may make false or misleading representations about employment

(1) An employee of an intelligence and security agency may make a false or misleading representation to any person in connection with any aspect of his or her employment if the representation is made—

(a) for the purpose of keeping secret the fact that he or she is an employee of the agency; and

(b) in accordance with any requirements of the Director-General of the agency.

(2) A false or misleading representation may be made by omitting or failing to disclose information.

(3) This section does not apply to representations made to any of the following:

(a) the intelligence and security agency:

(b) the Inspector-General of Intelligence and Security:

(c) the Intelligence and Security Committee:

(d) a court:

(e) a Minister of the Crown:

(f) the Leader of the Opposition:

(g) an Office of Parliament (as defined in section 2(1) of the Public Finance Act 1989):

(h) a chief executive of a department:

(i) the Chief of Defence Force:

(j) the Commissioner of Police:

(k) the Privacy Commissioner:

(l) a Human Rights Commissioner:

(m) the Independent Police Conduct Authority.

229 Protections relating to representations about identity

(1) An employee is protected from civil and criminal liability, however it may arise, for any act that the employee does, or omits to do, in good faith and with reasonable care in the course of making a representation in accordance with section 228.

(2) Nothing done (or omitted to be done) under section 228—

(a) places the employee in breach of contract or of any enactment or rule of law; or

(b) entitles any person to terminate or cancel a contract or an arrangement, or to accelerate the performance of an obligation, or to impose a penalty or an increased charge.

Exceptions and immunities

230 Exception from criminal liability under section 246 of Crimes Act 1961 in certain circumstances

(1) An employee does not commit an offence against section 246 of the Crimes Act 1961 (which relates to receiving) if—

(a) the employee receives unsolicited information from another person; and

(b) the employee has no reason to believe that the information has been obtained through the use of torture or any other abuse of human rights.

(2) Subsection (1) does not apply if it is proposed in advance to obtain information (whether or not on a continuing basis) and the obtaining of that information could have been authorised by an intelligence warrant.

(3) An intelligence and security agency that obtains information in circumstances where subsection (1) applies—

(a) must not disclose that information to another entity unless that entity is otherwise lawfully authorised to receive it; but

(b) may prepare a report using that information and, in the performance of its function under section 10 or 11, may disseminate that report to another agency.

231 Exceptions to Land Transport (Road User) Rule 2004

(1) An employee of the New Zealand Security Intelligence Service does not commit an offence against the following Parts of the Land Transport (Road User) Rule 2004 (the **Rule**) if subsection (2) applies:

(a) Part 3 (which sets out requirements about traffic signs and signals):

(b) Part 5 (which relates to speed limits):

(c) Part 6 (which relates to stopping and parking).

(2) This subsection applies if—

(a) the employee is carrying out visual surveillance from a vehicle on a public road; and

(b) the employee who takes the action that would otherwise constitute an offence considers that taking the action is reasonably necessary in order to continue the visual surveillance; and

(c) the employee takes all reasonable steps to ensure that his or her actions do not cause injury or damage, or interfere with any other person.

(3) The references in subsection (1) to Parts of the Rule include references to the corresponding Parts or provisions of any enactment that replaces the Rule.

232 Burden of proof to establish immunity and relationships between immunities

(1) If any question arises as to whether an immunity under any provision of this Act applies, the employee or entity, as the case requires, must establish, on the balance of probabilities, that the immunity applies.

(2) If there is any inconsistency between any of sections 31, 32, 43, 44, 110, 111, and 229 and the provisions of any other enactment conferring, regulating, or limiting a privilege or immunity, then the provisions of this Act prevail.

Intelligence functions of Chief Executive of Department of the Prime Minister and Cabinet

233 Functions of Chief Executive of DPMC in relation to intelligence and assessments

(1) The Chief Executive of the DPMC is responsible for the performance of the following functions:

(a) providing intelligence assessments on events and developments of significance to New Zealand's national security, international relations and well-being, and economic well-being to—

(i) Ministers; and

(ii) departments; and

(iii) any other person who the Chief Executive of the DPMC considers appropriate; and

(b) advising Ministers on the setting of priorities for intelligence collection and analysis; and

(c) advising departments on best practice in relation to the assessment of intelligence.

(2) However, the Chief Executive of the DPMC must not carry out the functions specified in subsection (1)(a) and (c) personally but must designate an employee of the DPMC to carry out those functions.

(3) The Chief Executive of the DPMC may at any time revoke a designation made under subsection (2) and designate an employee of the DPMC to carry out the functions specified in that subsection.

(4) In this section and in section 234, **DPMC** means the Department of the Prime Minister and Cabinet.

234 Duty to act independently

In matters relating to functions specified in section 233, the employee designated by the Chief Executive of the DPMC must act independently.

Periodic reviews

235 Requirement to hold periodic reviews

A review of the intelligence and security agencies and this Act must, in accordance with the terms of reference specified under section 236(3)(a), be—

(a) commenced as soon as practicable after the expiry of the period of 5 years beginning on the commencement of this section; and

(b) afterwards, held at intervals not shorter than 5 years and not longer than 7 years.

Compare: 1996 No 46 s 21

236 Appointment of reviewers and related matters

(1) A review under section 235 must be conducted by 2 persons (**reviewers**) appointed by the Prime Minister.

(2) The reviewers appointed under subsection (1) must hold a government-sponsored security clearance of a level determined by the Prime Minister.

(3) The Prime Minister must specify—

(a) the terms of reference for the review, which may include any matter relevant to the functions, effectiveness, and efficiency of the intelligence and security agencies and their contribution to national security; and

(b) any matters that he or she considers the reviewers should take into account in determining how to conduct the review; and

(c) the date by which the review is to be concluded.

(4) Before doing anything under this section, the Prime Minister must consult the Intelligence and Security Committee.

(5) The following must be notified in the *Gazette* as soon as practicable after the appointment of the reviewers:

(a) the persons appointed as reviewers; and

(b) the terms of reference of the review; and

(c) any matters specified in relation to the conduct of the review; and

(d) the date by which the review must be concluded.

Compare: 1996 No 46 s 22

237 Provision of information

To assist the reviewers to conduct their review,—

(a) the reviewers may ask the Director-General of an intelligence and security agency and the Inspector-General to provide information; and

(b) the Director-General of an intelligence and security agency or the Inspector-General may provide information to the reviewers, whether in response to a request under paragraph (a) or on his or her own initiative.

Compare: 1996 No 46 s 23

238 Report of reviewers

(1) After completing a review, the reviewers must prepare a report containing the results of their review.

(2) The report must be provided to the Intelligence and Security Committee by the date specified for the completion of the review.

(3) After the Intelligence and Security Committee has considered the report, the Committee must present the report to the House of Representatives.

(4) For the purposes of subsection (3), section 224 applies, with all necessary modifications, as if the report had been prepared by the Intelligence and Security Committee.

Compare: 1996 No 46 s 24

239 Remuneration of reviewers

(1) A reviewer is entitled—

(a) to receive remuneration not provided for in paragraph (b) for services as a reviewer at a rate and of a kind determined by the Prime Minister in accordance with the fees framework; and

(b) in accordance with the fees framework, to be reimbursed for actual and reasonable travelling and other expenses incurred in carrying out his or her office as a reviewer.

(2) For the purposes of subsection (1), **fees framework** means the framework determined by the Government from time to time for the classification and remuneration of statutory and other bodies in which the Crown has an interest.

Compare: 1996 No 46 s 25

240 Provision of administrative and other support

(1) The Ministry of Justice is responsible for providing to the reviewers the administrative, secretarial, and other support necessary for the reviewers to conduct their review effectively and efficiently.

(2) A person providing administrative, secretarial, or other support under subsection (1) must hold a government-sponsored security clearance of a level determined by the Prime Minister.

Compare: 1996 No 46 s 26

241 Reviewers to determine own procedure

The reviewers may determine their own procedure subject to any matters specified under section 236(3)(b).

Compare: 1996 No 46 s 27

Part 8
Repeals and amendments

Repeals

242 Repeals

(1) Sections 15A to 15F of the Inspector-General of Intelligence and Security Act 1996 are repealed.

(2) The Inspector-General of Intelligence and Security Act 1996 (1996 No 47) is repealed.

(3) The following Acts are repealed:

(a) New Zealand Security Intelligence Service Act 1969 (1969 No 24):

(b) Intelligence and Security Committee Act 1996 (1996 No 46):

(c) Government Communications Security Bureau Act 2003 (2003 No 9).

Amendments to Biosecurity Act 1993

243 Amendments to Biosecurity Act 1993

Section 244 amends the Biosecurity Act 1993.

244 Section 142I amended (Disclosure of personal information in New Zealand)

(1) After section 142I(1), insert:

(1A) The Director-General may disclose the personal information to an intelligence and security agency only if the Director-General believes, on reasonable grounds, that the disclosure of the information is necessary to enable the agency to perform any of its functions under section 10, 11, 13, or 14 of the Intelligence and Security Act 2017.

(2) In section 142I(2), replace "information to agencies" with "personal information to other agencies".

(3) After section 142I(5), insert:

(6) In this section, **intelligence and security agency** means—

(a) the New Zealand Security Intelligence Service:

(b) the Government Communications Security Bureau.

Amendments to Births, Deaths, Marriages, and Relationships Registration Act 1995

245 Amendments to Births, Deaths, Marriages, and Relationships Registration Act 1995

Sections 246 to 249 amend the Births, Deaths, Marriages, and Relationships Registration Act 1995.

246 Section 2 amended (Interpretation)

(1) In section 2, repeal the definition of **Director of Security**.

(2) In section 2, insert in their appropriate alphabetical order:

Director-General of an intelligence and security agency has the meaning given to it by section 4 of the Intelligence and Security Act 2017

intelligence and security agency has the meaning given to it by section 4 of the Intelligence and Security Act 2017

247 Section 65 amended (Request for new identity information for certain witnesses, etc)

(1) Replace section 65(1)(b) with:

(b) the Director-General of an intelligence and security agency, for the purpose of protecting the identity of a person who is, has been, or will be an employee.

(2) Replace section 65(2) with:

(2) The Minister may give a written direction to the Registrar-General to create new identity information for the person if,—

(a) on receiving a request under subsection (1)(a), the Minister is satisfied that it is in the interests of justice that the new identity information be created; or

(b) on receiving a request under subsection (1)(b), the Minister is satisfied, having regard to the matters set out in section 26(3) of the Intelligence and Security Act 2017 (which applies with any necessary modifications), that—

(i) the person will use the new identity information appropriately; and

(ii) it is otherwise appropriate to grant the request.

(3) Replace section 65(4)(b) with:

(b) the Director-General of an intelligence and security agency in relation to new identity information created as the result of a request under subsection (1)(b).

(4) In section 65(5), repeal the definitions of **employee** and **officer**.

(5) In section 65(5), insert in its appropriate alphabetical order:

employee has the meaning given to it by section 22 of the Intelligence and Security Act 2017

248 Section 75F amended (Searches for certain authorised purposes)

Replace section 75F(2)(c) with:

(c) an intelligence and security agency, if it requires the information for the performance of its functions:

249 Section 78 amended (Restrictions on searches relating to new names of certain witnesses, etc)

(1) Replace section 78(5)(b) with:

(b) the Director-General of an intelligence and security agency, if the new identity was created as the result of a request made under section 65(1)(b).

(2) Replace section 78(7)(b)(ii) with:

(ii) the Director-General of an intelligence and security agency, if the new identity was created as the result of a request made under section 65(1)(b).

(3) In section 78(8), replace "Director of Security" with "Director-General of the relevant intelligence and security agency".

Amendments to Corrections Act 2004

250 Amendments to Corrections Act 2004

Sections 251 and 252 amend the Corrections Act 2004.

251 Section 3 amended (Interpretation)

In section 3(1), definition of **official agency**, after paragraph (d), insert:

(da) the Inspector-General of Intelligence and Security; or

252 Section 117 amended (Authorised disclosure of information)

(1) Before section 117(1), insert:

(1AAA) An authorised person may disclose a prisoner call only as provided in this section.

(2) Replace section 117(2)(c) with:

(c) is necessary to prevent or lessen a serious threat (as defined in section 2(1) of the Privacy Act 1993) to—

(i) public health or public safety; or

(ii) the life or health of any person; or

(3) After section 117(2), insert:

(2A) An authorised person may disclose a prisoner call to an intelligence and security agency only if the authorised person believes, on reasonable grounds, that the disclosure is necessary to enable the agency to perform any of its functions under section 10, 11, 13, or 14 of the Intelligence and Security Act 2017.

(4) After section 117(6), insert:

(7) In this section, **intelligence and security agency** means—

(a) the New Zealand Security Intelligence Service:

(b) the Government Communications Security Bureau.

Amendments to Crimes Act 1961

253 Amendments to Crimes Act 1961

Sections 254 and 255 amend the Crimes Act 1961.

254 New section 78AA inserted (Wrongful communication, retention, or copying of classified information)

After section 78, insert:

78AA Wrongful communication, retention, or copying of classified information

(1) Every person specified in subsection (2) is liable to imprisonment for a term not exceeding 5 years if the person, within or outside New Zealand,—

(a) knowingly or recklessly, and with knowledge that he or she is acting without proper authority, communicates any classified information to any other person; or

(b) knowing that he or she is acting without proper authority, retains or copies any classified information; or

(c) knowingly fails to comply with any directions issued by a lawful authority for the return of any classified information that is in his or her possession or under his or her control.

(2) Subsection (1) applies to—

(a) a person who holds, or has held, a government-sponsored national security clearance to access classified information; or

(b) a person to whom classified information has been disclosed in confidence if—

(i) the disclosure is authorised; and

(ii) the person knows that the disclosure is in respect of classified information.

(3) In this section,—

classified information means—

(a) information that—

(i) is, or was, official information; and

(ii) is classified under the New Zealand Government Security Classification System as being accessible only to persons who have a national security clearance:

(b) foreign government information that is—

(i) classified in a foreign country; and

(ii) accessible only to persons having a government-sponsored national security clearance

New Zealand Government Security Classification System means the security classification system applying to official information that is published (and from time to time amended) on an Internet site maintained by or on behalf of the New Zealand Security Intelligence Service

official information has the meaning given to it by section 78A(2).

255 Section 78B amended (Consent of Attorney-General to proceedings in relation to espionage or wrongful communication, retention, or copying of official information)

(1) In the heading to section 78B, after "**copying of**", insert "**classified information or**".

(2) In section 78B(1)(a), (b), and (c), replace "section 78 or section 78A(1)" with "section 78, 78AA(1), or 78A(1)".

Amendments to Customs and Excise Act 1996

256 Amendments to Customs and Excise Act 1996

Sections 257 and 258 amend the Customs and Excise Act 1996.

257 Section 280M replaced (Direct access to database information for counter-terrorism investigation purposes)

Replace section 280M with:

280M Direct access to database information for purposes of counter-terrorism and national security

(1) The purpose of this section is to facilitate an agency's access to information stored in a database for the purpose of assisting the agency to perform its functions related to, or involving, all or any of the following:

(a) the prevention, detection, or investigation of any potential, suspected, or actual—

(i) terrorist act; or

(ii) facilitation of a terrorist act:

(b) national security.

(2) The chief executive of the Customs may, for the purpose of this section, allow the chief executive of an agency to access 1 or more databases to search for information, including personal information.

(3) Before allowing the chief executive of an agency access to any database in accordance with subsection (2), the chief executive of the Customs must enter into a written agreement with the chief executive of the agency.

(4) The written agreement must specify—

(a) the database or databases that may be accessed:

(b) the particular information that may be accessed:

(c) the particular purpose or purposes for which the information is accessed:

(d) how the information accessed is to be used by the agency to achieve those particular purposes:

(e) the positions or designations of the persons in the agency who may access the database or databases:

(f) the records to be kept in relation to each occasion on which a database is accessed:

(g) the safeguards that are to be applied for protecting personal information that is disclosed:

(h) the requirements relating to storage and disposal of information obtained by the agency from the database or databases:

(i) the circumstances (if any) in which the information may be disclosed by the agency to another specified agency, and how that disclosure may be made:

(j) the requirements for reviewing the agreement.

(5) An agreement may be varied by the chief executive of the Customs and the chief executive of the agency.

(6) Before entering into an agreement, or varying an agreement, the chief executive of the Customs must consult the Privacy Commissioner.

(7) In this section,—

access, in relation to a database, includes remote access to the database

agency means—

(a) a department specified in Schedule 1 of the State Sector Act 1988, other than—

(i) the Government Communications Security Bureau; and

(ii) the New Zealand Security Intelligence Service:

(b) a departmental agency that is part of a department referred to in paragraph (a):

(c) the New Zealand Police:

(d) the New Zealand Defence Force

chief executive of an agency—

(a) means the head of that agency; and

(b) includes the Commissioner of Police

database means any information recording system or facility used by the Customs to store information

information—

(a) means—

(i) any information held by the Customs that relates to goods, passengers, crew, or craft and the movements of the goods, passengers, crew, or craft:

(ii) any other border-related information held by the Customs; and

(b) includes, but is not limited to,—

(i) arrival and departure information:

(ii) information specified in section 282(1):

(iii) biometric information:

(iv) border information (as defined in section 282D):

(v) information collected or generated by the Customs in the course of preventing, detecting, or investigating a border-related offence (as defined in section 132B(1))

terrorist act has the same meaning as in section 5(1) of the Terrorism Suppression Act 2002.

258 New section 293A inserted (Saving of agreements made under section 280M before commencement of section 257 of Intelligence and Security Act 2017)

After section 293, insert:

293A Saving of agreements made under section 280M before commencement of section 257 of Intelligence and Security Act 2017

Every agreement made under section 280M between the chief executive and the Commissioner of Police that is in force immediately before the commencement of section 257 of the Intelligence and Security Act 2017 is to be treated as if it were made under section 280M as in force after the commencement of section 257 of that Act.

Amendment to Education Act 1989

259 Amendment to Education Act 1989

Section 260 amends the Education Act 1989.

260 Section 346 amended (Offences)

Replace section 346(1) with:

(1) An authorised user commits an offence, and is liable on conviction to a fine not exceeding $15,000, if the authorised user uses or discloses a person's national student number otherwise than—

(a) in accordance with the authorisations under section 344 that apply to that user; or

(b) as required by section 141 of the Intelligence and Security Act 2017 (to the extent that a permission granted under section 137 or 138 of that Act permits the Director-General of an intelligence and security agency to access information relating to national student numbers).

Amendment to Electronic Identity Verification Act 2012

261 Amendment to Electronic Identity Verification Act 2012

Section 262 amends the Electronic Identity Verification Act 2012.

262 Section 12 amended (Exception to section 11 for certain individuals with new identity information)

(1) Replace section 12(2) with:

(2) An individual referred to in subsection (1) (a **specified individual**) is—

(a) a person who is, has been, or will be, an undercover Police officer; or

(b) an employee of an intelligence and security agency.

(2) Replace section 12(9) with:

(9) In this section,—

employee has the meaning given to it by section 22 of the Intelligence and Security Act 2017

intelligence and security agency has the meaning given to it by section 4 of the Intelligence and Security Act 2017

undercover Police officer has the meaning given to it by section 65(5) of the Births, Deaths, Marriages, and Relationships Registration Act 1995.

Amendment to Employment Relations Act 2000

263 Amendment to Employment Relations Act 2000

Section 264 amends the Employment Relations Act 2000.

264 New section 172A inserted (Reports from Inspector-General of Intelligence and Security)

After section 172, insert:

172A Reports from Inspector-General of Intelligence and Security

(1) This section applies if—

(a) any matter that comes before the Authority relates to or arises from a recommendation made by the New Zealand Security Intelligence Service under section 11 of the Intelligence and Security Act 2017 about whether an individual should be granted a security clearance; and

(b) a report on the recommendation has not previously been prepared by the Inspector-General of Intelligence and Security under section 185 of that Act.

(2) The Authority must request the Inspector-General of Intelligence and Security to prepare a report on the recommendation made by the New Zealand Security Intelligence Service.

(3) As soon as practicable after receiving a request under subsection (2), the Inspector-General of Intelligence and Security must prepare and provide a report to the Authority.

(4) To enable the Inspector-General of Intelligence and Security to prepare a report, the Authority must provide to the Inspector-General all relevant documents within its possession or under its control.

(5) The parties are entitled—

(a) to receive a copy of the report; and

(b) to make submissions on it to the Authority.

(6) The Authority must have regard to the report prepared by the Inspector-General of Intelligence and Security before making a determination on the matter.

(7) In this section,—

Inspector-General of Intelligence and Security means the Inspector-General of Intelligence and Security holding office under section 157 of the Intelligence and Security Act 2017

New Zealand Security Intelligence Service means the New Zealand Security Intelligence Service continued by section 7 of the Intelligence and Security Act 2017.

Amendments to Immigration Act 2009

265 Amendments to Immigration Act 2009

Sections 266 to 279 amend the Immigration Act 2009.

266 Section 3 amended (Purpose)

Replace section 3(2)(c) with:

(c) allows for the management of persons crossing the border by setting requirements that apply to—

(i) persons arriving, or intending to arrive, in New Zealand; and

(ii) persons departing, or intending to depart, from New Zealand; and

267 Section 4 amended (Interpretation)

(1) In section 4, replace the definition of **approved system** with:

approved system means a system, including an electronic system, approved by the chief executive for the purpose of—

(a) providing information to the chief executive under section 96; or

(b) giving notice under section 97(2) of a decision made under section 97(1); or

(c) giving notice under section 97A(3) of a decision made under section 97A(1)

(2) In section 4, insert in its appropriate alphabetical order:

scheduled international service means a series of flights or voyages that are—

(a) performed by a craft for the transport of passengers, cargo, or mail between New Zealand and 1 or more points in any other country or territory, if the flights or voyages are so regular or frequent as to constitute a systematic service, whether or not in accordance with a published timetable; and

(b) operated in such a manner that each flight or voyage is open to use by members of the public

268 Section 9A amended (Meaning of mass arrival group)

In section 9A(2), delete "(within the meaning of section 96(4))".

269 Section 29 amended (Automated decision making in advance passenger processing)

In section 29, after "section 97(1)", insert "or 97A(1)".

270 Section 96 replaced (Responsibilities of carrier, and person in charge, of commercial craft before it departs from another country to travel to New Zealand)

Replace section 96 with:

96 Carrier, and person in charge, of commercial craft to provide advance passenger processing information before departure

(1) This section applies to a carrier, and a person in charge, of a commercial craft if—

(a) one of the following applies:

(i) the craft is scheduled to travel to New Zealand in the course of a scheduled international service:

(ii) it is proposed that the craft travel to New Zealand from another country:

(iii) the craft is scheduled to travel from New Zealand in the course of a scheduled international service:

(iv) it is proposed that the craft travel from New Zealand to another country; and

(b) the chief executive has notified the carrier, or a person in charge, of the craft that the carrier or person in charge of the craft must comply with this section.

(2) A carrier, or a person in charge, of a commercial craft must—

(a) obtain from every person who intends to board the craft for the purpose of travelling to, or from, New Zealand the advance passenger processing information prescribed for the purposes of this subsection; and

(b) provide that information to the chief executive, by means of an approved system, before the departure of the craft to travel to, or from, New Zealand.

(3) The chief executive may, by notice in writing, in any specified circumstances, exempt a carrier, or person in charge, of a commercial craft from complying with some or all of the requirements under subsection (2).

271 Section 97 amended (Chief executive may make decision about person boarding craft for purpose of travelling to New Zealand)

(1) Replace the heading to section 97 with "**Chief executive may make decision about person boarding commercial craft for purpose of travelling to New Zealand**".

(2) Replace section 97(1) with:

(1) The chief executive may decide that a person in relation to whom information has been received under section 96(2) and who intends to board a commercial craft for the purpose of travelling to New Zealand—

(a) may board the craft; or

(b) may not board the craft; or

(c) may board the craft only if he or she complies with conditions specified by the chief executive.

(3) Replace section 97(2)(a) with:

(a) must notify a carrier, or a person in charge, of a commercial craft from whom information has been received under section 96(2) of a decision made under subsection (1); and

(4) Replace section 97(6) with:

(6) Nothing in section 305 applies to the chief executive when he or she is giving a notification under subsection (2).

272 New section 97A inserted (Chief executive may make decision about person boarding commercial craft for purpose of travelling from New Zealand)

After section 97, insert:

97A Chief executive may make decision about person boarding commercial craft for purpose of travelling from New Zealand

(1) The chief executive may decide that a person in relation to whom information has been received under section 96(2) and who intends to board a commercial craft for the purpose of travelling from New Zealand—

(a) may board the craft; or

(b) may not board the craft; or

(c) may board the craft only if he or she complies with conditions specified by the chief executive.

(2) The chief executive may make a decision under subsection (1)(b) or (c) only if the chief executive has reason to believe that the person is attempting to travel on—

(a) a lost, stolen, or invalid passport or certificate of identity; or

(b) a forged, false, fraudulently obtained, or improperly altered passport or certificate of identity; or

(c) a passport or certificate of identity that does not relate to that person.

(3) The chief executive—

(a) must notify a carrier, or a person in charge, of a commercial craft from whom information has been received under section 96(2) of a decision made under subsection (1); and

(b) may do so in any form that he or she thinks appropriate, including, but not limited to, by means of an approved system, which may contain code that represents the outcome of the decision; and

(c) may do so in any manner that he or she thinks appropriate, including, but not limited to, by means of an automated electronic notification.

(4) Nothing in section 305 applies to the chief executive when he or she is giving a notification under subsection (3).

273 Section 101 amended (Obligations in relation to craft en route to or arriving in New Zealand)

Repeal section 101(5).

274 Section 102 amended (Obligations of carriers, and persons in charge, of craft to provide information)

Replace section 102(2) to (4) with:

(2) A carrier, and a person in charge, of a commercial craft who is required under section 96 to provide information to the chief executive must also provide to the chief executive the information prescribed for the purposes of this section about every person who intends or intended to board the craft for the purpose of—

(a) travelling to New Zealand, including persons who did not board the craft for any reason (including because of a decision made by the chief executive under section 97); or

(b) travelling from New Zealand, including persons who did not board the craft for any reason (including because of a decision made by the chief executive under section 97A).

(3) The chief executive may, by notice in writing, in any specified circumstances, exempt a carrier, or a person in charge, of a commercial craft from complying with some or all of the requirements under subsection (2).

(4) Despite being granted an exemption, a carrier, or a person in charge, of a commercial craft must provide to the chief executive—

(a) some or all of the information required under subsection (2)(a) if requested by the chief executive not more than 14 days before or after the arrival of the craft in New Zealand; or

(b) some or all of the information required under subsection (2)(b) if requested by the chief executive not more than 14 days before or after the departure of the craft from New Zealand.

275 Section 303 amended (Disclosure of information to enable specified agencies to check identity and character)

(1) In section 303(4), replace "to which subsection (6) applies" with "entered into in accordance with section 303C".

(2) Repeal section 303(6).

276 New sections 303A to 303C inserted

After section 303, insert:

303A Disclosure of information to specified agencies for purposes of law enforcement, counter-terrorism, and security

(1) The purpose of this section is to enable the disclosure of information by the Department to a specified agency to allow that agency a longer period of time to—

(a) identify any person of interest who is intending to board a craft for the purpose of travelling from New Zealand; and

(b) perform any of its functions, or exercise any of its powers, in relation to an identified person of interest before that person departs from New Zealand.

(2) For the purpose of this section, the chief executive of a specified agency may supply to the chief executive of the Department personal information about a person of interest.

(3) The chief executive of the Department may compare the information received under subsection (2) about a person of interest with APP information that he or she holds.

(4) If the chief executive of the Department holds APP information about the person of interest, he or she may, under an agreement entered into in accordance with section 303C,—

(a) notify the chief executive of the specified agency that the person of interest intends to board a craft for the purpose of travelling from New Zealand; and

(b) disclose to that chief executive—

(i) the APP information held by the chief executive of the Department about the person of interest; and

(ii) any other information held by the chief executive of the Department about the person's intended travel (for example, when and where the person checked in).

(5) In this section,—

APP information means advance passenger processing information that the chief executive of the Department has received under section 96(2) about persons intending to board a craft for the purpose of travelling from New Zealand

chief executive of a specified agency means the head of that specified agency

person of interest means a person of interest to the chief executive of a specified agency because the chief executive believes on reasonable grounds that the person may attempt to leave New Zealand and that the person—

(a) poses a threat or risk to the security of New Zealand or another country because the person intends to engage in, or facilitate,—

(i) a terrorist act within the meaning of section 5 of the Terrorism Suppression Act 2002; or

(ii) the proliferation of weapons of mass destruction; or

(iii) any other unlawful activity designed or likely to cause serious economic damage to New Zealand, carried out for the purpose of commercial or economic gain; or

(b) is—

(i) a person under control or supervision (as defined in section 3(1) of the Corrections Act 2004); or

(ii) on bail with an electronic monitoring condition granted under section 30B of the Bail Act 2000; or

(iii) liable to be arrested (with or without a warrant) by an employee or agent of a specified agency; or

(iv) suspected of escaping from lawful custody; or

(v) suspected of being a perpetrator or victim of an offence under section 98D of the Crimes Act 1961 (trafficking in persons); or

(vi) suspected of being involved in the unlawful movement of illegal goods; or

(vii) a person who poses a risk, for any reason, to the safety of other passengers, the crew, or craft

personal information, in relation to a person of interest, includes the following information:

(a) the person's—

(i) full name; and

(ii) date of birth; and

(iii) place of birth; and

(iv) nationality; and

(v) gender; and

(b) the details specified in the person's passport or certificate of identity, if known, including—

(i) the passport or certificate of identity number; and

(ii) the expiry date; and

(iii) the issuer of the person's certificate of identity (if any), if it is not the person's country of nationality

specified agency means—

(a) the New Zealand Police:

(b) the department of State responsible for the administration of the Corrections Act 2004:

(c) the department of State responsible for the administration of the Customs and Excise Act 1996:

(d) the Civil Aviation Authority of New Zealand established under section 72A(1) of the Civil Aviation Act 1990.

303B Direct access to information for purposes of law enforcement, counter-terrorism, and security

(1) For the purpose of section 303A, the chief executive of the Department may allow the chief executive of a specified agency to access the APP information database or databases to search for information relating to a person of interest.

(2) Before allowing the chief executive of a specified agency access to the APP information, the chief executive of the Department must enter into an agreement with the specified agency in accordance with section 303C.

(3) The agreement must specify, in addition to the matters set out in section 303C(2)(d) to (h),—

(a) the particular information that may be accessed:

(b) the particular purpose or purposes for which the information may be accessed:

(c) the positions or designations of the persons in the specified agency who may access the database or databases:

(d) the records to be kept in relation to each occasion on which a database is accessed:

(e) the safeguards that are to be applied for protecting personal information that is accessed:

(f) the requirements relating to storage and disposal of information obtained by the specified agency from the database:

(g) the requirements for reviewing the agreement.

(4) In this section,—

access, in relation to a database, includes remote access to the database

APP information, **chief executive of a specified agency**, **specified agency**, and **person of interest** have the meanings given to them by section 303A(5)

APP information database means the database of APP information

database means any information recording system or facility used by the Department to store or process information.

303C Requirements for agreements entered into under section 303, 303A, or 303B

(1) This section applies to an agreement entered into under section 303, 303A, or 303B.

(2) An agreement—

Making

(a) must not be made until the chief executive of the Department has consulted the Privacy Commissioner:

(b) must be made between the chief executive of the Department and the chief executive of the specified agency:

(c) must be in writing:

Contents

(d) must state the criteria for the disclosure under it of information by the Department to the specified agency:

(e) must state the use that the specified agency may make of the information disclosed to it:

(f) must—

(i) state that the specified agency must not disclose the information disclosed to it to any other agencies, bodies, or persons; or

(ii) state the other agencies, bodies, or persons to which the specified agency may disclose information disclosed to it, the extent to which the specified agency may disclose the information, and the conditions subject to which the specified agency may disclose the information:

(g) may state the form in which the information may be disclosed:

(h) may state the method by which the information may be disclosed:

Varying

(i) may be varied:

(j) must not be varied until the chief executive of the Department has consulted the Privacy Commissioner:

Reviews and reports

(k) must, if the Privacy Commissioner requires, provide that the agreement, and the arrangements for disclosure under it, be the subject of reviews and reports to the Privacy Commissioner by the chief executive of the specified agency at intervals of no less than 12 months.

277 Section 349 amended (Offences relating to carriers, and persons in charge, of craft)

(1) Replace section 349(1)(b) with:

(b) allows a person to travel to, or from, New Zealand before a decision has been made by the chief executive under section 97(1) or 97A(1); or

(2) After section 349(1)(c), insert:

(ca) having been notified under section 97A(3) of a decision made by the chief executive under section 97A(1)(b) or (c), fails without reasonable excuse to ensure that the person to whom the decision relates complies with it; or

278 Section 366 amended (Evidence in proceedings: certificates in relation to persons)

(1) After section 366(2)(22), insert:

(22A) the person did or did not travel from New Zealand before a decision was made by the chief executive under section 97A(1); or

(2) After section 366(2)(23), insert:

(23A) the person travelled from New Zealand contrary to a decision made by the chief executive under section 97A(1)(b) or (c); or

279 Section 402 amended (Regulations relating to procedures and requirements in relation to arrivals in and departures from New Zealand)

In section 402(a), after "travelling to", insert "or from".

Amendments to Land Transport Act 1998

280 Amendments to Land Transport Act 1998

Sections 281 and 282 amend the Land Transport Act 1998.

281 Section 24A amended (Authorised persons may request driver licences for certain persons)

(1) Replace section 24A(1)(b) with:

(b) the Director-General of an intelligence and security agency, for the purpose of protecting the identity of a person who is, has been, or will be an employee:

(2) Replace section 24A(4)(b) with:

(b) the Director-General of an intelligence and security agency, in relation to new identity information created as the result of a request under subsection (1)(b); or

(3) In section 24A(5), repeal the definitions of **Director of Security**, **employee**, and **officer**.

(4) In section 24A(5), insert in their appropriate alphabetical order:

Director-General of an intelligence and security agency has the meaning given to it by section 4 of the Intelligence and Security Act 2017

employee, in relation to an intelligence and security agency, has the meaning given to it by section 22 of the Intelligence and Security Act 2017

intelligence and security agency has the meaning given to it by section 4 of the Intelligence and Security Act 2017

282 Section 200 amended (Restrictions on access to photographic images of driver licence holders)

Replace section 200(1) with:

(1) No person other than a person acting in the course of the person's official duties as an employee of the Agency may access or use any photographic image stored under section 28(5).

(1A) Subsection (1) is subject to—

(a) subsections (2) and (2A):

(b) section 141 of the Intelligence and Security Act 2017.

Amendments to Passports Act 1992

283 Amendments to Passports Act 1992

Sections 284 to 310 amend the Passports Act 1992.

284 Section 2 amended (Interpretation)

In section 2, insert in their appropriate alphabetical order:

Chief Commissioner of Intelligence Warrants means the Chief Commissioner of Intelligence Warrants appointed under section 112 of the Intelligence and Security Act 2017

Commissioner of Intelligence Warrants means a Commissioner of Intelligence Warrants appointed under section 112 of the Intelligence and Security Act 2017

285 Section 4 amended (Issue of passport)

In section 4(1), replace "4A" with "27GA".

286 Section 4A repealed (Refusal to issue passport on grounds of national security)

Repeal section 4A.

287 Section 8A repealed (Cancellation of passport on grounds of national security)

Repeal section 8A.

288 Section 9 amended (Cancellation of passport on other grounds)

(1) After section 9(1), insert:

(1AA) The Minister may, under section 27GA, recall a New Zealand passport, and cancel it or retain possession of it.

(2) In section 9(2), replace "this section" with "subsection (1) or (1A)".

289 Section 11 amended (Delivery of recalled passport)

In section 11(1), after "sections 8 to 10", insert "or section 27GA".

290 Section 11A amended (Warnings on New Zealand travel document database)

In section 11A(a), replace "and 27F" with "27F, and 27GA".

291 Section 20 amended (Cancellation of certificate of identity)

After section 20(1), insert:

(1AA) The Minister may, under section 27GA, recall any certificate of identity issued to any person by or on behalf of the Government of New Zealand, and cancel it or retain possession of it.

292 Section 20A repealed (Cancellation of certificate of identity on grounds of national security)

Repeal section 20A.

293 Section 22 amended (Delivery of recalled certificate of identity)

In section 22(1), replace "section 20 or section 20A or section 21" with "section 20, 21, or 27GA".

294 Section 23 amended (Issue of emergency travel document)

Replace section 23(3)(a) with:

(a) the person has under section 27GA been refused a passport, or under that section has had his or her passport or emergency travel document cancelled; and

295 Section 25 amended (Cancellation of emergency travel document)

After section 25(1), insert:

(1AA) The Minister may, under section 27GA, recall an emergency travel document, and cancel it or retain possession of it.

296 Section 25A repealed (Cancellation of emergency travel document on grounds of national security)

Repeal section 25A.

297 Section 27 amended (Delivery of recalled emergency travel document)

In section 27(1), replace "section 25 or section 25A or section 26" with "section 25, 26, or 27GA".

298 Section 27A amended (Issue of refugee travel document)

In section 27A(1), replace "section 27B" with "section 27GA".

299 Section 27B repealed (Refusal to issue refugee travel document on grounds of national security)

Repeal section 27B.

300 Section 27D amended (Cancellation of refugee travel document)

After section 27D(1), insert:

(1AA) The Minister may, under section 27GA, recall a New Zealand refugee travel document, and cancel it or retain possession of it.

301 Section 27E repealed (Cancellation of refugee travel document on grounds of national security)

Repeal section 27E.

302 Section 27G amended (Delivery of recalled refugee travel document)

In section 27G(1), replace "section 27D or section 27E or section 27F" with "section 27D, 27F, or 27GA".

303 New sections 27GA to 27GF and cross-heading inserted

After section 27G, insert:

National and international security

27GA Refusal to issue, or cancellation or retention of, New Zealand travel document on grounds of national or international security

(1) The Minister may decide to take any action specified in subsection (3) in relation to a person if the Minister has reasonable cause to believe—

(a) the person is a danger to the security of New Zealand because the person intends to engage in, or facilitate,—

(i) a terrorist act within the meaning of section 5 of the Terrorism Suppression Act 2002; or

(ii) the proliferation of weapons of mass destruction; or

(iii) any other unlawful activity designed or likely to cause serious economic damage to New Zealand, carried out for the purpose of commercial or economic gain; and

(b) the taking of that action will prevent or effectively impede the ability of the person to do any of the activities specified in paragraph (a); and

(c) the danger to the security of New Zealand cannot be effectively averted other than by taking an action specified in subsection (3).

(2) The Minister may also decide to take any action specified in subsection (3) in relation to a person if the Minister has reasonable cause to believe—

(a) the person is a danger to the security of a country other than New Zealand because the person intends to engage in, or facilitate,—

(i) a terrorist act within the meaning of section 5 of the Terrorism Suppression Act 2002; or

(ii) the proliferation of weapons of mass destruction; and

(b) the taking of that action will prevent or effectively impede the ability of the person to do either of the activities specified in paragraph (a); and

(c) the danger to the security of that country cannot be effectively averted other than by taking an action specified in subsection (3).

(3) In any case to which subsection (1) or (2) applies, the Minister may—

(a) refuse to issue a New Zealand passport to the person:

(b) recall the person's New Zealand passport, and—

(i) cancel it; or

(ii) retain possession of it:

(c) recall the person's certificate of identity issued by or on behalf of the New Zealand Government, and—

(i) cancel it; or

(ii) retain possession of it:

(d) recall the person's emergency travel document (not being a journey-specific emergency travel document issued under section 23(3)), and—

(i) cancel it; or

(ii) retain possession of it:

(e) refuse to issue a New Zealand refugee travel document to the person:

(f) recall the person's New Zealand refugee travel document, and—

(i) cancel it; or

(ii) retain possession of it.

(4) The Minister may take any of the actions specified in subsection (3)(a) to (e) whether or not the person is in New Zealand.

(5) The Minister may take the action specified in subsection (3)(f) only if the person is in New Zealand.

Compare: 1992 No 92 Schedule 2 cls 1(1)–(3), 2(1)–(3), 3(1)–(3), 4(1)–(3), 5(1)–(3), 6(1), (2), (9) (pre-1 April 2017)

27GB Chief Commissioner of Intelligence Warrants to be notified of action taken under section 27GA

(1) If the Minister takes an action specified in section 27GA(3) in relation to a person, the Minister must notify the Chief Commissioner of Intelligence Warrants of—

(a) the action that has been taken; and

(b) the reasons for the taking of that action.

(2) The Minister must arrange for all documents that he or she considered when deciding to take the action to be referred to the Chief Commissioner of Intelligence Warrants.

27GC Person to be notified of action taken under section 27GA

(1) If the Minister takes an action specified in section 27GA(3) in relation to a person, the Minister must, as soon as practicable, notify the person of—

(a) the action that has been taken; and

(b) the date on which the decision to take that action was made; and

(c) the reasons for making that decision; and

(d) the period during which the person is not entitled to obtain a New Zealand travel document.

(2) However, the Minister may defer notifying the person of the matters specified in subsection (1) for a period not exceeding 30 days after taking the action if the Minister is satisfied that giving notice sooner may prejudice an ongoing investigation or put the security or safety of any person at risk.

(3) Notice under this section is to be treated as given if the Minister has taken all practicable steps to provide it.

Compare: 1992 No 92 Schedule 2 cls 1(4)(a), (5), 2(4)(a), (5), 3(4)(a), (5), 4(4)(a), (5), 5(4)(a), (5), 6(4)(a), (5) (pre-1 April 2017)

27GD Person not entitled to obtain New Zealand travel document if action taken under section 27GA

(1) If the Minister takes an action specified in section 27GA(3) in relation to a person, the person is not entitled to obtain a New Zealand travel document during the 12-month period (the **disqualification period**) starting with the date on which the decision to take the action was made, unless that decision is—

(a) revoked by the Minister; or

(b) set aside by a court.

(2) Despite subsection (1), the Minister may decide to specify a longer disqualification period in the notice given under section 27GC(1), not exceeding 36 months, if the Minister is satisfied that the person would continue to pose a danger to the security of New Zealand or any other country for longer than 12 months.

(3) If the disqualification period exceeds 12 months,—

(a) the person may, within 30 days after the date on which the notice was given under section 27GC(1), make a written submission to the Minister about the length of the disqualification period and, if a submission is made, the Minister must review the length of the disqualification period, having regard to the person's submission; and

(b) the Minister must, every 12 months after the date on which the notice was given under section 27GC(1) (unless the disqualification period has sooner expired), review the decision made under subsection (2) by—

(i) inviting the person to make a written submission to the Minister about the decision; and

(ii) determining whether the decision should be revoked or amended having regard to the person's submission (if any).

(4) The Minister may, at any time before the expiry of the disqualification period, apply to the High Court for an order to extend the disqualification period for a further period not exceeding 12 months.

(5) The High Court must make the order applied for under subsection (4) if satisfied that—

(a) the information presented in support of the application is credible, having regard to its source or sources; and

(b) the information reasonably supports a finding that there continue to be grounds for the Minister to make a decision under section 27GA(1) or (2) in relation to the person who is subject to the disqualification period.

Compare: 1992 No 92 Schedule 2 cls 1(4)(b), (6)–(9), 2(4)(b), (6)–(9), 3(4)(b), (6)–(9), 4(4)(b), (6)–(9), 5(4)(b), (6)–(9), 6(3)(b), (5)–(8) (pre-1 April 2017)

27GE Temporary suspension of New Zealand travel documents pending decision under section 27GA

(1) The Minister may suspend a person's New Zealand travel document for a period not exceeding 10 working days if the Minister—

(a) is investigating or considering whether to take an action under section 27GA; and

(b) is satisfied that the person is likely to travel overseas before a decision under that section is made.

(2) The Minister may mark the electronic record of a New Zealand travel document on a New Zealand travel document database with a warning to indicate that the New Zealand travel document has been suspended.

(3) If it subsequently becomes apparent that the grounds for taking an action under section 27GA cannot be established,—

(a) the suspension lapses; and

(b) the Minister must remove the warning (if any) marked on the electronic record of the New Zealand travel document under subsection (2).

Compare: 1992 No 92 Schedule 2 cl 7 (pre-1 April 2017)

27GF Review of Minister's decision under section 27GA

(1) If the Chief Commissioner of Intelligence Warrants receives notice under section 27GB that the Minister has taken an action under section 27GA, the Chief Commissioner of Intelligence Warrants must arrange for a Commissioner of Intelligence Warrants to conduct a review of the Minister's decision to take that action.

(2) A Commissioner of Intelligence Warrants must review the Minister's decision by—

(a) assessing the documents referred by the Minister under section 27GB(2); and

(b) considering whether the documents reasonably support the decision.

(3) If the Commissioner of Intelligence Warrants considers that the documents do not reasonably support the Minister's decision, the Commissioner of Intelligence Warrants must prepare a report of the review—

(a) recommending that the Minister reconsider his or her decision; and

(b) stating the reasons for that recommendation.

(4) The Minister must, after receiving a report under subsection (3),—

(a) reconsider his or her decision and either confirm, vary, or revoke it; and

(b) notify the person in respect of whom the action under section 27GA was taken of—

(i) the recommendation of the Commissioner of Intelligence Warrants and the reasons for it; and

(ii) the outcome of the Minister's reconsideration of his or her decision.

304 Section 27I amended (Electronic cancellation of New Zealand travel documents)

Replace section 27I(1) and (2) with:

(1) The Minister may cancel a New Zealand travel document under any of sections 8, 9, 9A, 20, 25, 27D, 27GA, and 27H by electronically recording the cancellation of that travel document on a New Zealand travel document database.

(2) Despite any provision in any of sections 8, 9, 9A, 20, 25, 27D, and 27GA, the Minister need not recall a New Zealand travel document, under the relevant section, nor have possession of the document, before cancelling it in accordance with subsection (1).

305 Section 28 amended (Appeal to High Court)

In section 28(5A), replace "on grounds of national security" with "under section 27GA".

306 Section 29 amended (Appeal to Court of Appeal in certain cases)

(1) Replace section 29(1A) with:

(1A) Any party who is dissatisfied with a decision of the High Court under section 27GD(5) to extend the period for which a person is not entitled to obtain a New Zealand travel document may, with the leave of the court, or, if the court refuses leave, with the leave of the Court of Appeal, appeal to the Court of Appeal.

(2) Replace section 29(3A) with:

(3A) This section is subject to sections 29AA to 29AC in the case of an appeal relating to—

(a) a decision of the Minister under section 27GA to refuse to issue a New Zealand travel document, or to cancel or retain a New Zealand travel document; or

(b) a decision of the High Court under section 27GD(5) to extend the period during which a person is not entitled to obtain a New Zealand travel document.

307 Cross-heading above section 29AA replaced

Replace the cross-heading above section 29AA with:

Special provision for proceedings where national or international security involved

308 Section 29AA amended (Proceedings where national security involved)

(1) Replace the heading to section 29AA with "**Proceedings where national or international security involved**".

(2) Replace section 29AA(1) and (2) with:

(1) This section applies to the following proceedings:

(a) an application to the High Court by the Minister under section 27GD(4) for an order extending the period during which a person is not entitled to obtain a New Zealand travel document, and any appeal under section 29(1A) against such an order:

(b) an appeal under section 28 or 29 relating to a decision of the Minister under section 27GA to refuse to issue a New Zealand passport or refugee travel document, or to cancel or retain a New Zealand travel document:

(c) an appeal under section 28 or 29 relating to a decision of the Minister to refuse to issue a certificate of identity under section 16 or an emergency travel document under section 23, where the Minister certifies that he or she had reasonable cause to believe—

(i) the person concerned was a danger to the security of New Zealand or another country because the person intended to engage in, or facilitate, an activity of a kind described in section 27GA(1)(a) or (2)(a); and

(ii) the refusal to issue the certificate of identity or emergency travel document concerned would prevent or effectively impede the ability of the person to carry out that intended activity; and

(iii) the danger to the security of New Zealand or the other country could not be effectively averted by other means:

(d) an application for judicial review of a decision made by the Minister under section 27GA or 27GD.

(2) In hearing an appeal to which this section applies, the court must determine whether—

(a) the information that led to the decision is credible, having regard to its source or sources; and

(b) the information reasonably supports a finding that—

(i) the person concerned is a danger to the security of New Zealand or another country because the person intends to engage in, or facilitate, an activity of a kind described in section 27GA(1)(a) or (2)(a); and

(ii) the refusal to issue the New Zealand travel document concerned, or to cancel or retain the New Zealand travel document, will prevent or effectively impede the ability of the person to carry out that intended activity; and

(iii) the danger to the security of New Zealand or the other country cannot be effectively averted by other means.

(3) Replace section 29AA(5)(a) with:

(a) relevant to whether there are or may be grounds for believing that—

(i) the person concerned is a danger to the security of New Zealand or another country because the person intends to engage in, or facilitate, an activity of a kind described in section 27GA(1)(a) or (2)(a); or

(ii) the refusal to issue the New Zealand travel document concerned, or to cancel or retain the New Zealand travel document, will prevent or effectively impede the ability of the person to carry out the intended activity; or

(iii) the danger to the security of New Zealand or the other country cannot be effectively averted by other means; and

309 Section 29AB amended (Proceedings involving classified security information)

After section 29AB(4), insert:

(4A) If at any time a decision is made to withdraw any classified security information,—

(a) the classified security information—

(i) must be kept confidential and must not be disclosed by the court; and

(ii) must be returned to the relevant agency; and

(b) the court must continue to make the decision or determine the proceedings—

(i) without regard to that classified security information; and

(ii) in the case of an appeal or a review of proceedings, as if that information had not been available in making the decision subject to the appeal or review.

Compare: 1992 No 92 Schedule 2 cl 8(2) (pre-1 April 2017)

310 New section 37B inserted (Crown liability)

After section 37A, insert:

37B Crown liability

(1) This section applies to any decision made under section 27GA, 27GD, or 27GE.

(2) The Crown is not liable to any person for any loss or damage as a result of, or in connection with, a decision referred to in subsection (1) unless the person or persons taking those actions, or any employee of the Crown performing any function directly or indirectly connected with those actions, has not acted in good faith or has been grossly negligent.

Compare: 1992 No 92 Schedule 2 cl 9 (pre-1 April 2017)

311 Section 46 repealed (Transitional provision)

Repeal section 46.

Amendments to Privacy Act 1993

312 Amendments to Privacy Act 1993

Sections 313 to 317 amend the Privacy Act 1993.

313 Section 2 amended (Interpretation)

(1) In section 2(1), replace the definition of **intelligence organisation** with:

intelligence and security agency means—

(a) the New Zealand Security Intelligence Service:

(b) the Government Communications Security Bureau

(2) In section 2(1), definition of **organisation**, replace paragraph (b)(ii) with:

(ii) an intelligence and security agency

314 Section 6 amended (Information privacy principles)

(1) In section 6, principle 10, insert as subclause (2):

(2) In addition to subclause (1), an intelligence and security agency that holds personal information that was obtained in connection with one purpose may use the information for any other purpose (a **secondary purpose**) if the agency be-

lieves on reasonable grounds that the use of the information for the secondary purpose is necessary to enable the agency to perform any of its functions.

(2) In section 6, principle 11, after paragraph (f), insert:

(fa) that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions; or

315 Section 57 replaced (Intelligence organisations)

Replace section 57 with:

57 Exemption for intelligence and security agencies

Information privacy principles 2, 3, and 4(b) do not apply to information collected by an intelligence and security agency.

316 Cross-heading above section 81 amended

In the cross-heading above section 81, replace "*intelligence organisations*" with "*intelligence and security agencies*".

317 Section 81 replaced (Special procedure relating to intelligence organisations)

Replace section 81 with:

81 Special procedure relating to intelligence and security agencies

(1) Nothing in sections 76, 77, and 82 to 89 applies to—

(a) any complaint made under this Part in relation to an action of an intelligence and security agency; or

(b) any investigation conducted under this Part in relation to an action of an intelligence and security agency.

(2) If, after completing an investigation, the Commissioner is of the opinion that an action of an intelligence and security agency is an interference with the privacy of an individual, the Commissioner must provide to the intelligence and security agency a report setting out—

(a) his or her opinion; and

(b) the reasons for that opinion.

(3) A report provided under subsection (2) may include any recommendations the Commissioner considers appropriate.

(4) When making a report under subsection (2), the Commissioner may request the intelligence and security agency to notify him or her within a specified time of any steps the agency proposes to take in response to the report and to any recommendations included in the report.

(5) If, within a reasonable time after any report is made, no steps are taken by the intelligence and security agency in response to the report that seem to be ad-

equate and appropriate, the Commissioner may send a copy of the report to the Prime Minister.

(6) As soon as practicable after receiving a report under subsection (5), the Prime Minister may present the report, or any part of the report, to the House of Representatives.

Amendments to Protected Disclosures Act 2000

318 Amendments to Protected Disclosures Act 2000

Sections 319 and 320 amend the Protected Disclosures Act 2000.

319 Section 3 amended (Interpretation)

In section 3(1), insert in its appropriate alphabetical order:

classified information has the meaning given to it by section 78AA of the Crimes Act 1961

320 Sections 12 and 13 replaced

Replace sections 12 and 13 with:

12 Special rules on procedures of organisations relating to intelligence and security matters

(1) This section applies to—

(a) an intelligence and security agency; and

(b) any other organisation in the public sector that holds or has access to—

(i) classified information; or

(ii) information relating to the activities of an intelligence and security agency.

(2) An organisation to which this section applies must have internal procedures that—

(a) provide that the persons to whom a disclosure of information described in subsection (1)(b) may be made must be persons holding an appropriate security clearance and be authorised to have access to the information; and

(b) state that the only appropriate authority to whom information described in subsection (1)(b) may be disclosed is the Inspector-General of Intelligence and Security; and

(c) invite any employee who has disclosed, or is considering the disclosure of, information described in subsection (1)(b) under this Act to seek information and guidance from the Inspector-General of Intelligence and Security, and not from an Ombudsman; and

(d) state that no disclosure of information described in subsection (1)(b) may be made to an Ombudsman or to a Minister of the Crown other than—

(i) the Minister responsible for an intelligence and security agency; or

(ii) the Prime Minister.

13 Special rules on procedures of certain organisations relating to international relations

(1) This section applies to the internal procedures of the following agencies to the extent that those procedures relate to the disclosure of information (other than classified information) concerning the international relations of the Government of New Zealand:

(a) the Department of the Prime Minister and Cabinet; and

(b) the Ministry of Foreign Affairs and Trade; and

(c) the Ministry of Defence; and

(d) the New Zealand Defence Force.

(2) The internal procedures must—

(a) state that the only appropriate authority to whom information may be disclosed is an Ombudsman; and

(b) invite any employee who has disclosed, or is considering the disclosure of, information under this Act to seek information and guidance from an Ombudsman; and

(c) state that no disclosure may be made to a Minister of the Crown other than—

(i) the Prime Minister; or

(ii) the Minister responsible for foreign affairs and trade.

Amendments to Public Finance Act 1989

321 Amendments to Public Finance Act 1989

Sections 322 to 324 amend the Public Finance Act 1989.

322 Section 2 amended (Interpretation)

In section 2(1), definition of **department**, repeal paragraph (a)(iv).

323 Section 15A amended (Main Appropriation Bill: supporting information relating to appropriations)

In section 15A(4)(a), replace "subsection (2)(a) and (c) do" with "subsection (2)(c) does".

324 Section 45E amended (Application of this Part to intelligence and security departments)

(1) Replace section 45E(1)(a) with:

> (a) section 40 must be read as if the discretion conferred on the Minister by section 40(2)(d)(ii) were only able to be exercised with the agreement of the responsible Minister; and

(2) Repeal section 45E(1)(b).

(3) Replace section 45E(1)(c) with:

> (c) section 221 of the Intelligence and Security Act 2017 is substituted for sections 43 and 44.

Amendment to Remuneration Authority Act 1977

325 Amendment to Remuneration Authority Act 1977

Section 326 amends the Remuneration Authority Act 1977.

326 Schedule 4 amended

In Schedule 4, insert in their appropriate alphabetical order:

> The Commissioners of Intelligence Warrants
>
> The Inspector-General of Intelligence and Security and the Deputy Inspector-General of Intelligence and Security

Amendments to Search and Surveillance Act 2012

327 Amendments to Search and Surveillance Act 2012

Sections 328 and 329 amend the Search and Surveillance Act 2012.

328 Subpart 8 heading in Part 2 amended

In Part 2, in the subpart 8 heading, after "78", insert "or 78AA".

329 Section 25 amended (Warrantless searches if offence against section 78 of Crimes Act 1961 suspected)

(1) In the heading to section 25, after "**78**", insert "**or 78AA**".

(2) In section 25(2)(a), after "section 78", insert "or 78AA".

Amendments to State Sector Act 1988

330 Amendments to State Sector Act 1988

Sections 331 and 332 amend the State Sector Act 1988.

331 Section 44 amended (Special provisions in relation to certain chief executives)

(1) Replace section 44(1) with:

(1) Nothing in sections 35, 36, 38, 39, and 43 applies in respect of the State Services Commissioner.

(2) Replace section 44(2) with:

(2) For the purposes of this Act,—

(a) the Solicitor-General is the chief executive of the Crown Law Office:

(b) the State Services Commissioner is the chief executive of the State Services Commission.

332 Schedule 1 amended

In Schedule 1, insert in its appropriate alphabetical order:

New Zealand Security Intelligence Service

Amendment to Tax Administration Act 1994

333 Amendment to Tax Administration Act 1994

Section 334 amends the Tax Administration Act 1994.

334 Section 81 amended (Officers to maintain secrecy)

After section 81(4)(s), insert:

(sa) allowing the Director-General of an intelligence and security agency (as defined in section 4 of the Intelligence and Security Act 2017), or an employee of that intelligence and security agency authorised by the Director-General for that purpose, access to information specified in a permission given under section 137 or 138 of the Intelligence and Security Act 2017:

Consequential amendments

335 Consequential amendments

The enactments specified in Schedule 4 are amended in the manner indicated in that schedule.

Schedule 1
Transitional, savings, and related provisions

s 5

Part 1
Provisions relating to this Act as enacted

1 Interpretation

In this Part, **commencement date** means the date on which this Part comes into force.

2 Appointment of Director-General of Government Communications Security Bureau

(1) The person who immediately before the commencement date held office as the Director of the Government Communications Security Bureau under the Government Communications Security Bureau Act 2003 continues in that office on and after the commencement date in accordance with subclause (2).

(2) Unless the person resigns or is removed from office or dies, he or she continues to hold office during the period while his or her term of office is unexpired until—

(a) the end of the day that is 6 months after the commencement date; or

(b) the earlier date on which he or she accepts an offer of appointment from, and agrees to employment arrangements with, the State Services Commissioner.

(3) For the purposes of carrying out the functions of the State Services Commissioner under subclause (2)(b), sections 35, 37, and 40(1A) of the State Sector Act 1988 do not apply.

(4) If the person ceases to hold office under subclause (2)(a), no compensation is payable for loss of office.

3 Appointment of Director-General of New Zealand Security Intelligence Service

(1) The person who immediately before the commencement date held office as the Director of Security under the New Zealand Security Intelligence Service Act 1969 continues in that office on and after the commencement in accordance with subclause (2).

(2) Unless the person resigns or is removed from office or dies, he or she continues to hold office during the period while his or her term of office is unexpired until—

(a) the end of the day that is 6 months after the commencement date; or

(b) the earlier date on which he or she accepts an offer of appointment from, and agrees to employment arrangements with, the State Services Commissioner.

(3) For the purposes of carrying out the functions of the State Services Commissioner under subclause (2)(b), sections 35, 37, and 40(1A) of the State Sector Act 1988 do not apply.

(4) If the person ceases to hold office under subclause (2)(a), no compensation is payable for loss of office.

4 Other appointments continued

(1) The person who, immediately before the commencement date, was appointed under section 5(1)(a) of the Inspector-General of Intelligence and Security Act 1996 as Inspector-General of Intelligence and Security continues to hold that office for the unexpired term of his or her appointment as if he or she had been appointed under section 157 of the Intelligence and Security Act 2017.

(2) The person who, immediately before the commencement date, was appointed under section 5(1)(b) of the Inspector-General of Intelligence and Security Act 1996 as Deputy Inspector-General of Intelligence and Security continues to hold that office for the unexpired term of his or her appointment as if he or she had been appointed under section 164 of the Intelligence and Security Act 2017.

(3) A person who, immediately before the commencement date, was appointed under section 15C of the Inspector-General of Intelligence and Security Act 1996 as a member of the advisory panel continues to hold that office for the unexpired term of his or her appointment as if he or she had been appointed under section 169 of the Intelligence and Security Act 2017.

(4) A person continues to hold office under any of subclauses (1) to (3) on the same terms and conditions that applied to that office immediately before the commencement date, unless or until new terms and conditions are set by the Remuneration Authority.

5 Warrants and authorisations

(1) If an application for a warrant or an authorisation has been made under a former Act before the commencement date and the application is not finally determined before that date, the provisions of the former Act continue to apply to the application and to any matter or obligation relating to the application in all respects as if the former Act had not been repealed.

(2) The provisions of a former Act apply to a continuing warrant or authorisation and to any matter relating to the warrant or authorisation in all respects as if the former Act had not been repealed.

(3) In this clause,—

authorisation means—

(a) an authorisation issued under section 4ID of the New Zealand Security Intelligence Service Act 1969:

(b) an access authorisation issued under section 15A of the Government Communications Security Bureau Act 2003

continuing warrant or authorisation means a warrant or an authorisation issued under a former Act—

(a) before the commencement date; or

(b) on or after the commencement date on an application made before that date

former Act means—

(a) the New Zealand Security Intelligence Service Act 1969:

(b) the Government Communications Security Bureau Act 2003

warrant means a warrant of any kind issued under a former Act.

6 Reports of inquiries commenced under Inspector-General of Intelligence and Security Act 1996

Section 185(4) of this Act applies to a report in respect of an inquiry that was commenced under the provisions of the Inspector-General of Intelligence and Security Act 1996 if the report is completed after that section comes into force.

Schedule 2
Databases accessible to intelligence and security agencies

s 125

Accessing intelligence and security agency	Information	Holder agency
GCSB and NZSIS	Birth information Civil union information Death information Marriage information Name change information	Registrar-General
GCSB and NZSIS	Citizenship information	Secretary for Internal Affairs
GCSB and NZSIS	Information collected in connection with the performance or exercise of a function, duty, or power under the Immigration Act 2009	Ministry of Business, Innovation, and Employment
GCSB and NZSIS	Information about border-crossing persons, goods, and craft that has been collected in connection with the performance or exercise of a function, duty, or power under the Customs and Excise Act 1996	New Zealand Customs Service
GCSB and NZSIS	Financial intelligence information	New Zealand Police
NZSIS	Information about people and locations identified as posing a possible physical threat to GCSB or NZSIS employees	New Zealand Police

Note

In this schedule,—

birth information, **civil union information**, **death information**, **marriage information**, **name change information**, and **Registrar-General** have the meanings given to them by section 2 of the Births, Deaths, Marriages, and Relationships Registration Act 1995

citizenship information means information that relates to the acquisition or loss of citizenship by, or to the citizenship status of, any person

financial intelligence information means information held by the Commissioner of Police in the performance of his or her financial intelligence functions specified in sections 142 and 143 of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009

GCSB means the Government Communications Security Bureau

NZSIS means the New Zealand Security Intelligence Service.

Schedule 3
Administrative provisions

ss 117, 166, 170, 200

Contents

Part 1
Provisions relating to Commissioners of Intelligence Warrants

1 Term of office of Commissioners

(1) A person holds office as a Commissioner for a term of 3 years.

(2) A person who holds office as a Commissioner may be reappointed for 1 or more further terms.

(3) A person who holds office as a Commissioner, unless he or she earlier vacates office by reason of death, resignation, or removal, continues to hold office, even if the term for which he or she was appointed has expired, until one of the following occurs:

(a) the person is reappointed:

(b) the person's successor is appointed.

(4) A person who holds office as a Commissioner may at any time resign by written notice to the Governor-General.

(5) A notice of resignation under subclause (4) must state the date on which the resignation takes effect.

Compare: 1969 No 24 s 5B

2 Removal from office

A Commissioner may be removed from office by the Governor-General, on address from the House of Representatives, for—

(a) incapacity; or

(b) bankruptcy; or

(c) neglect of duty; or

(d) misconduct.

Compare: 1969 No 24 s 5C

3 Remuneration and expenses

(1) A Commissioner must be paid, out of public money and without further appropriation than this clause,—

(a) a salary at the rate determined by the Remuneration Authority; and

(b) allowances (if any) determined by the Remuneration Authority.

(2) The rate of salary and the allowances (if any) determined by the Remuneration Authority must be those applicable to an Acting High Court Judge.

(3) A Commissioner is entitled to receive, in respect of time spent travelling in the performance of his or her functions, travelling allowances and expenses in accordance with the Fees and Travelling Allowances Act 1951, and the provisions of that Act apply accordingly as if a Commissioner were a member of a statutory board and the travelling were in the service of a statutory board.

Compare: 1969 No 24 s 5E

4 Protection of Commissioners

A Commissioner has all the immunities of a Judge of the High Court.

Compare: 1969 No 24 s 5D

5 Disclosure of interests

A Commissioner must give written notice to the Prime Minister of all interests, pecuniary or otherwise, that the Commissioner has or acquires and that could conflict with the proper performance of his or her functions.

Compare: 1969 No 24 s 5F

Part 2
Provisions relating to Inspector-General and Deputy Inspector-General

6 Term of office of Inspector-General and Deputy Inspector-General

(1) A person holds office as the Inspector-General or Deputy Inspector-General for a term (which must not be more than 5 years) that the Governor-General, on the recommendation of the House of Representatives, specifies in the person's appointment.

(2) A person holding office as the Inspector-General may be reappointed for 1 further term of not more than 3 years.

(3) A person holds office as the Deputy Inspector-General for a term (which must be not more than 3 years) that the Governor-General, on the recommendation of the House of Representatives, specifies in the person's appointment.

(4) A person holding office as the Deputy Inspector-General may be reappointed for 1 or more further terms.

(5) The person holding office as the Inspector-General or the Deputy Inspector-General, unless he or she earlier vacates office by reason of death, resignation, or removal, continues to hold office, even if the term for which he or she was appointed has expired, until one of the following occurs:

(a) the person is reappointed:

(b) the person's successor is appointed.

(6) The Inspector-General and Deputy Inspector-General may at any time resign by written notice to the Governor-General.

(7) A notice of resignation under subclause (6) must state the date on which the resignation takes effect.

Compare: 1996 No 47 s 6

7 Filling of vacancy

(1) If a vacancy occurs in the office of Inspector-General, the vacancy must be filled by the appointment of a successor in accordance with section 157(2) and (3).

(2) If a vacancy occurs in the office of the Deputy Inspector-General, the vacancy must be filled by the appointment of a successor in accordance with section 164(2) and (3).

(3) Subclause (4) applies if—

(a) a vacancy specified in subclause (1) or (2) occurs while Parliament is not in session, or exists at the close of a session; and

(b) the House of Representatives has not recommended an appointment to fill the vacancy.

(4) When this subclause applies, the vacancy may, at any time before the commencement of the next session of Parliament, be filled by the appointment of a successor by the Governor-General in Council.

(5) An appointment made under subclause (4) lapses and the office again becomes vacant unless, before the end of the 24th sitting day of the House of Representatives following the date of the appointment, the House confirms the appointment.

Compare: 2004 No 38 Schedule 2 cl 2

8 Removal or suspension from office

(1) The Inspector-General or Deputy Inspector-General may be removed or suspended from office by the Governor-General, on an address from the House of Representatives, for—

(a) incapacity; or

(b) bankruptcy; or

(c) neglect of duty; or

(d) misconduct; or

(e) failure to hold the appropriate security clearance.

(2) If the Inspector-General or Deputy Inspector-General is suspended from office at any time when Parliament is not in session, the suspension does not continue

in force beyond 2 months after the beginning of the next ensuing session of Parliament.

Compare: 1996 No 47 s 7

9 Remuneration and expenses

(1) The Inspector-General and Deputy Inspector-General must be paid, out of public money and without further appropriation than this clause,—

(a) salaries at the rates determined by the Remuneration Authority; and

(b) allowances (if any) determined by the Remuneration Authority.

(2) The Inspector-General and Deputy Inspector-General are entitled to receive from the funds of the Inspector-General's office the actual and reasonable costs for travelling and other expenses that relate to the performance of their functions and duties.

Compare: 1996 No 47 s 8

10 Disclosure of interests

The Inspector-General and Deputy Inspector-General must each give written notice to the Prime Minister of all interests, pecuniary or otherwise, that they have or acquire and that could conflict with the proper performance of their functions and duties.

Compare: 1996 No 47 s 9

11 Staff

(1) The Inspector-General may appoint any employees that the Inspector-General considers necessary for the efficient performance and exercise of his or her functions, duties, and powers.

(2) The power conferred by subclause (1) includes the power to appoint employees on a part-time or temporary basis, or for any period that the Inspector-General and an employee agree.

(3) An employee is employed on the terms and conditions, and paid the salary and allowances, that the Inspector-General determines in consultation with the Secretary for Justice.

(4) An employee may not have access to any information in the possession of an intelligence and security agency except in accordance with the rules governing access to such information applying within the agency.

(5) Only a person who holds an appropriate security clearance may be appointed as an employee.

Compare: 1996 No 47 s 10

12 Inspector-General and others protected

(1) The Inspector-General, the Deputy Inspector-General, and any employee of the Inspector-General are not personally liable for any act done or omitted to be

done in good faith in the performance or intended performance of the Inspector-General's functions or duties.

(2) A member of the advisory panel is not personally liable for any act done or omitted to be done in good faith in the performance or intended performance of his or her functions or duties.

(3) Nothing in subclauses (1) and (2) applies in respect of proceedings for—

(a) an offence against section 219; or

(b) an offence against section 78, 78AA(1), 78A(1), 105, 105A, or 105B of the Crimes Act 1961; or

(c) an offence of conspiring to commit an offence against any of those sections of the Crimes Act 1961; or

(d) an offence of attempting to commit an offence against any of those sections of the Crimes Act 1961.

Compare: 1996 No 47 s 24(1)(a), (2)

Part 3
Provisions relating to advisory panel

13 Term of office of members

(1) A person holds office as a member of the advisory panel for a term (which must not be more than 5 years) that the Governor-General, on the recommendation of the Prime Minister, specifies in the person's appointment.

(2) A member may be reappointed for 1 or more further terms.

(3) A member may at any time resign by written notice to the Prime Minister.

Compare: 1996 No 47 s 15C(5)(a)–(c)

14 Removal from office

A member of the advisory panel may be removed from office by the Prime Minister for—

(a) incapacity; or

(b) bankruptcy; or

(c) neglect of duty; or

(d) misconduct; or

(e) failure to hold the appropriate security clearance.

Compare: 1996 No 47 s 15C(5)(d)

15 Remuneration and expenses

(1) A member of the advisory panel is entitled—

(a) to receive remuneration not provided for within paragraph (b) for services as a member at a rate and of a kind determined by the Minister in accordance with the fees framework; and

(b) in accordance with the fees framework, to be reimbursed for actual and reasonable travelling and other expenses incurred in carrying out his or her office as a member.

(2) For the purposes of subclause (1), **fees framework** means the framework determined from time to time by the Government for the classification and remuneration of statutory and other bodies in which the Crown has an interest.

Compare: 1996 No 47 s 15D

16 Procedure of advisory panel

The advisory panel may determine its own procedure.

Compare: 1996 No 47 s 15F

Part 4
Provisions relating to Intelligence and Security Committee

Membership of Committee

17 Revocation of member's nomination

(1) The Leader of the Opposition may at any time revoke his or her nomination of a person as a member of the Committee under section 194(2)(c).

(2) The Prime Minister may at any time revoke his or her nomination of a person as a member of the Committee under section 194(2)(d).

Compare: 1996 No 46 s 9

18 Suspension and cessation of membership

(1) A person's membership of the Committee is suspended if that member is suspended from the service of the House of Representatives.

(2) A person's membership of the Committee ceases when one of the following occurs:

(a) the person's nomination is revoked under clause 17:

(b) the person ceases to be a member of the House of Representatives:

(c) Parliament is dissolved or expires.

(3) A nominated member may at any time resign from the Committee by written notice signed by the member and addressed to the Prime Minister or Leader of the Opposition, as the case may require.

(4) The office of a member of the Committee becomes vacant if—

(a) the member's membership ceases under subclause (2)(a) or (b); or

(b) the member resigns under subclause (3).

Compare: 1996 No 46 s 10

Procedure for meetings of Committee

19 Convener

Meetings of the Committee must be convened by the chairperson of the Committee.

Compare: 1996 No 46 s 13(1)

20 Chairperson presides

The chairperson of the Committee must preside at all meetings of the Committee.

Compare: 1996 No 46 s 13(2)

21 Quorum

The chairperson and 3 other members must be present at a meeting of the Committee.

Compare: 1996 No 46 s 13(3)

22 Conduct of proceedings

(1) The proceedings of the Committee must, subject to this Act, be conducted in accordance with the rules and practice of the House of Representatives.

(2) The Committee must meet in private, unless—

(a) the Committee is performing its function under section 193(1)(c); or

(b) the Committee by unanimous resolution resolves otherwise.

(3) The Committee may give directions as to who may be present when the Committee meets in private.

Compare: 1996 No 46 s 12

23 Decisions

(1) Every question arising at any meeting of the Committee is determined by a majority of votes of the members who are present and voting on it.

(2) The chairperson has a deliberative vote and, in the case of an equality of votes, also has a casting vote.

Compare: 1996 No 46 s 13(4), (5)

24 Representation

(1) The Leader of the Opposition may appoint the person who acts as his or her deputy in the House of Representatives to attend a meeting of the Committee in his or her place.

(2) No other member of the Committee may be represented at any meeting by any other person.

(3) Subclause (2) is subject to section 198(3).

Compare: 1996 No 46 ss 7A(4), 13(6), (6A)

25 Officers to assist

(1) The Chief Executive of the Department of the Prime Minister and Cabinet must, with the concurrence of the Committee, appoint any officers that are required to assist the Committee in the conduct of its business.

(2) Only a person who has appropriate security clearance may be appointed to assist the Committee.

Compare: 1996 No 46 s 13(7), (8)

Administrative provisions

26 Committee members and others protected

(1) This clause applies to every member of the Committee and to any person appointed under clause 25(1) to assist the Committee.

(2) A person to whom this clause applies is not personally liable for any act done or omitted to be done in good faith in the performance or intended performance of the Committee's functions.

(3) A person to whom this clause applies is not required to give evidence in any court, or in any proceedings of a judicial nature, in respect of anything coming to his or her knowledge in the performance of the Committee's functions.

(4) Nothing in this clause applies in respect of proceedings for an offence against section 219.

Compare: 1996 No 46 s 15

Schedule 4
Consequential amendments

s 335

Part 1
Amendments to Acts

Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (2009 No 35)

In section 5, definition of **government agency**, replace paragraph (c) with:

> (c) the Reserve Bank, the Parliamentary Counsel Office, and the New Zealand Police; or

In section 5, definition of **law enforcement purposes**, replace paragraph (g) with:

> (g) the performance by the New Zealand Security Intelligence Service or the Government Communications Security Bureau of its function under section 10 or 11 of the Intelligence and Security Act 2017:

In section 5, repeal the definition of **security**.

Repeal section 18(2)(e).

Replace section 140(2)(h) with:

> (h) Parts 1 to 7 of the Intelligence and Security Act 2017:

Children's Commissioner Act 2003 (2003 No 121)

In section 27(4)(a), (b), and (c), replace "section 78 or section 78A(1) or section 105 or section 105A or section 105B" with "section 78, 78AA(1), 78A(1), 105, 105A, or 105B".

Civil Aviation Act 1990 (1990 No 98)

In section 77F(4)(a), replace "section 4(1)(bb) of the New Zealand Security Intelligence Service Act 1969" with "section 11 of the Intelligence and Security Act 2017".

In section 77G(1), delete "under section 4(1)(bb) of the New Zealand Security Intelligence Service Act 1969".

In section 77G(1), replace "sections 11 and 16 of the Inspector-General of Intelligence and Security Act 1996" with "sections 158(1)(e) and 171 of the Intelligence and Security Act 2017".

Replace section 77G(5) with:

> (5) In this section,—
>
> **Inspector-General of Intelligence and Security** means the person holding office under section 157 of the Intelligence and Security Act 2017
>
> **New Zealand person** means any person who is—

Civil Aviation Act 1990 (1990 No 98)—*continued*

(a) a New Zealand citizen; or

(b) a person ordinarily resident in New Zealand.

Companies Act 1993 (1993 No 105)

In section 366(1B), definition of **law enforcement purposes**, replace paragraph (g) with:

(g) the performance by the New Zealand Security Intelligence Service or the Government Communications Security Bureau of its function under section 10 or 11 of the Intelligence and Security Act 2017:

Crimes Act 1961 (1961 No 43)

Replace section 216B(2)(b) with:

(b) does so pursuant to, and in accordance with the terms of, any authority conferred on him or her by or under—

(i) the Search and Surveillance Act 2012; or

(ii) Part 4 of the Intelligence and Security Act 2017; or

(iii) the International Terrorism (Emergency Powers) Act 1987.

In section 216D(2)(a) and (b)(ii), replace "officer" with "employee".

In section 216N(1)(c), delete "officer or".

After section 216N(1)(c), insert:

(ca) any employee of the Government Communications Security Bureau; and

Criminal Records (Clean Slate) Act 2004 (2004 No 36)

Replace section 19(3)(a)(iii) with:

(iii) the exercise of the protective security advice and assistance function of the New Zealand Security Intelligence Service under section 11 of the Intelligence and Security Act 2017; or

Environment Act 1986 (1986 No 127)

In section 22A(3)(a), (b), and (c), replace "section 78 or section 78A(1) or section 105 or section 105A or section 105B" with "section 78, 78AA(1), 78A(1), 105, 105A, or 105B".

Financial Markets Authority Act 2011 (2011 No 5)

In section 22(3)(a), after "section 78,", insert "78AA(1),".

Health and Disability Commissioner Act 1994 (1994 No 88)

In section 65(3)(a) and (b), replace "section 78 or section 78A(1) or section 105 or section 105A or section 105B" with "section 78, 78AA(1), 78A(1), 105, 105A, or 105B".

Health and Safety at Work Act 2015 (2015 No 70)

In section 8(2)(a), replace "Director" with "Director-General".

In section 8(2)(b), replace "Director" with "Director-General".

In section 8(6), replace "Director of Security or Director of the Bureau" with "Director-General of Security or the Director-General of the Government Communications Security Bureau".

Replace section 8(7) with:

(7) A worker who is an employee of the Security Intelligence Service or the Government Communications Security Bureau may ask the Inspector-General to review a declaration made under subsection (2) to determine whether, in making the declaration, the Director-General of Security or the Director-General of the Government Communications Security Bureau (as the case requires) met the criteria in subsection (6).

In section 8(9), replace the definition of **Government Communications Security Bureau** or **Bureau** with:

> **Government Communications Security Bureau** or **Bureau** means the Government Communications Security Bureau continued by section 8 of the Intelligence and Security Act 2017

In section 8(9), definition of **Inspector-General**, paragraph (a), replace "section 5 of the Inspector-General of Intelligence and Security Act 1996" with "section 157 of the Intelligence and Security Act 2017".

In section 8(9), definition of **Inspector-General**, paragraph (b), replace "section 5 of the Act" with "section 157 of the Intelligence and Security Act 2017".

In section 8(9), replace the definition of **Minister** with:

> **Minister**,—
>
> (a) in relation to the New Zealand Security Intelligence Service, means the Minister responsible for the New Zealand Security Intelligence Service:
>
> (b) in relation to the Government Communications Security Bureau, means the Minister responsible for the Government Communications Security Bureau

In section 8(9), replace the definition of **Security Intelligence Service** with:

> **Security Intelligence Service** means the New Zealand Security Intelligence Service continued by section 7 of the Intelligence and Security Act 2017.

In Schedule 4, clause 2, definition of **security, intelligence, or law enforcement agency**, paragraph (d), delete ":".

In Schedule 4, clause 2, definition of **security, intelligence, or law enforcement agency**, repeal paragraph (e).

In Schedule 4, clause 2, definition of **specified agency**, repeal paragraph (c).

Human Rights Act 1993 (1993 No 82)

In section 130(3)(a) and (b), replace "section 78 or section 78A(1) or section 105 or section 105A or section 105B" with "section 78, 78AA(1), 78A(1), 105, 105A, or 105B".

Immigration Act 2009 (2009 No 51)

In section 4, definition of **chief executive**, replace paragraph (b) with:

(b) when used in relation to a relevant agency, the chief executive of that agency (including, where appropriate, the Commissioner of Police, the Chief of Defence Force, and the General Manager of the Aviation Security Service)

In section 4, definition of **government agency**, replace paragraph (b) with:

(b) includes the New Zealand Police

Independent Police Conduct Authority Act 1988 (1988 No 2)

In section 33(2)(a), (b), and (c), replace "section 78 or section 78A(1) or section 105 or section 105A" with "section 78, 78AA(1), 78A(1), 105, or 105A".

Judicial Conduct Commissioner and Judicial Conduct Panel Act 2004 (2004 No 38)

In Schedule 2, clause 4(4)(a) and (b), replace "section 78 or section 78A(1) or section 105 or section 105A or section 105B" with "section 78, 78AA(1), 78A(1), 105, 105A, or 105B".

Limited Partnerships Act 2008 (2008 No 1)

In section 79(1B), definition of **law enforcement purposes**, replace paragraph (g) with:

(g) the performance by the New Zealand Security Intelligence Service or the Government Communications Security Bureau of its function under section 10 or 11 of the Intelligence and Security Act 2017:

Mental Health (Compulsory Assessment and Treatment) Act 1992 (1992 No 46)

After section 123(3)(b), insert:

(ba) the Inspector-General of Intelligence and Security:

New Zealand Business Number Act 2016 (2016 No 16)

In section 5, definition of **government agency**, repeal paragraph (e).

Ombudsmen Act 1975 (1975 No 9)

In section 17C(1), replace "section 5 of the Inspector-General of Intelligence and Security Act 1996" with "section 157 of the Intelligence and Security Act 2017".

Ombudsmen Act 1975 (1975 No 9)—*continued*

In section 17C(3), replace "the Inspector-General of Intelligence and Security Act 1996" with "subpart 1 of Part 6 of the Intelligence and Security Act 2017".

In section 21C, replace "section 5 of the Inspector-General of Intelligence and Security Act 1996" with "section 157 of the Intelligence and Security Act 2017".

In section 26(2)(a), (b), and (c), replace "section 78 or section 78A(1) or section 105 or section 105A or section 105B" with "section 78, 78AA(1), 78A(1), 105, 105A, or 105B".

Privacy Act 1993 (1993 No 28)

In section 72B(1) and (3), replace "the Inspector-General of Intelligence and Security Act 1996" with "subpart 1 of Part 6 of the Intelligence and Security Act 2017".

In section 96(3)(a) and (b), replace "section 78 or section 78A(1) or section 105 or section 105A or section 105B" with "section 78, 78AA(1), 78A(1), 105, 105A, or 105B".

In section 117B, delete "under the Inspector-General of the Intelligence and Security Act 1996".

Protected Disclosures Act 2000 (2000 No 7)

In section 3(1), replace the definition of **intelligence and security agency** with:

> **intelligence and security agency** has the meaning given to it by section 4 of the Intelligence and Security Act 2017

In section 14, replace "the Inspector-General of Intelligence and Security Act 1996" with "subpart 1 of Part 6 of the Intelligence and Security Act 2017".

Public Finance Act 1989 (1989 No 44)

In section 39(3), replace "established under the Intelligence and Security Committee Act 1996" with "continued under section 192 of the Intelligence and Security Act 2017".

In section 65T(2), delete "for that department".

In section 65W(5), delete "for that department".

Public Records Act 2005 (2005 No 40)

In section 4, definition of **public office**, repeal paragraph (c)(x).

Radiocommunications Act 1989 (1989 No 148)

Replace section 133A(2)(c) with:

> (c) by an employee of an intelligence and security agency for the purpose of performing the function under section 10 of the Intelligence and Security Act 2017; or

Replace section 133A(2)(e)(ii) and (iia) with:

Radiocommunications Act 1989 (1989 No 148)—*continued*

(ii) Part 4 of the Intelligence and Security Act 2017; or

Replace section 133A(3) with:

(3) In this section, **intelligence and security agency** means—

(a) the New Zealand Security Intelligence Service:

(b) the Government Communications Security Bureau.

Remuneration Authority Act 1977 (1977 No 110)

In Schedule 4, repeal the item relating to the Director of the Government Communications Security Bureau.

In Schedule 4, repeal the item relating to the Director of the New Zealand Security Intelligence Service.

In Schedule 4, insert in its appropriate alphabetical order:

The Inspector-General of Intelligence and Security and the Deputy Inspector-General of Intelligence and Security

Search and Surveillance Act 2012 (2012 No 24)

Replace section 47(1)(c) with:

(c) activities carried out under an authorisation issued under Part 4 of the Intelligence and Security Act 2017:

Takeovers Act 1993 (1993 No 107)

In section 33D(2)(c)(i), (ii), and (iii), replace "section 78 or section 78A(1) or section 105 or section 105A or section 105B" with "section 78, 78AA(1), 78A(1), 105, 105A, or 105B".

Telecommunications (Interception Capability and Security) Act 2013 (2013 No 91)

In section 3(1), replace the definition of **Director** with:

Director means the Director-General of the Government Communications Security Bureau

In section 3(1), replace the definition of **interception warrant** with:

interception warrant means—

(a) a warrant issued under section 53 of the Search and Surveillance Act 2012:

(b) an intelligence warrant issued under Part 4 of the Intelligence and Security Act 2017

In section 3(1), definition of **Minister responsible for the Government Communications Security Bureau**, replace "for the department of State established under the

Telecommunications (Interception Capability and Security) Act 2013 (2013 No 91)—*continued*

Government Communications Security Bureau Act 2003" with "of the Government Communications Security Bureau".

In section 3(1), replace the definition of **other lawful interception authority** with:

> **other lawful interception authority—**
>
> (a) means an authorisation issued under Part 4 of the Intelligence and Security Act 2017 (within the meaning of section 47 of that Act); and
>
> (b) includes an authority to intercept a private communication (whether in an urgent or emergency situation or otherwise) that is granted or issued to any member of a surveillance agency under any other enactment

In the heading to section 56, replace "**Security**" with "**Intelligence**".

In section 56(1)(a), replace "Commissioner" with "Chief Commissioner of Intelligence Warrants".

Replace section 56(1)(b) with:

> (b) on receipt of the notice, the Chief Commissioner of Intelligence Warrants must arrange for a review to be conducted in accordance with this section by a Commissioner as soon as practicable.

Replace section 56(8) with:

(8) In this section and section 57,—

> **Chief Commissioner of Intelligence Warrants** has the meaning given to it by section 4 of the Intelligence and Security Act 2017
>
> **Commissioner** means a Commissioner of Intelligence Warrants within the meaning of section 4 of the Intelligence and Security Act 2017.

Terrorism Suppression Act 2002 (2002 No 34)

In section 4(1), definition of **intelligence and security agency**, repeal paragraph (c).

Part 2
Amendments to legislative instruments

Citizenship Regulations 2002 (SR 2002/73)

Replace regulation 15(2)(b) with:

> (b) for an intelligence and security agency to perform its functions under section 10 or 11 of the Intelligence and Security Act 2017:

After regulation 15(2), insert:

(3) In this regulation, **intelligence and security agency** has the meaning given to it by section 4 of the Intelligence and Security Act 2017.

Hazardous Substances and New Organisms (Personnel Qualifications) Regulations 2001 (SR 2001/122)

Replace regulation 6D(1)(d) with:

(d) the licence holder is the subject of, or is referred to in, advice and information given to the Authority by the Director-General of the New Zealand Security Intelligence Service under section 11 or 104 of the Intelligence and Security Act 2017; or

Legislative history

15 August 2016	Introduction (Bill 158–1)
18 August 2016	First reading and referral to Foreign Affairs, Defence and Trade Committee
24 February 2017	Reported from Foreign Affairs, Defence and Trade Committee (Bill 158–2)
9 March 2017	Second reading
16 March 2017	Committee of the whole House (Bill 158–3)
21 March 2017	Third reading
28 March 2017	Royal assent

This Act is administered by the Department of the Prime Minister and Cabinet.

Wellington, New Zealand:
Published under the authority of the New Zealand Government—2017