New Zealand Intelligence and Security Bill

Government Bill

Explanatory note

General policy statement

The New Zealand Intelligence and Security Bill implements the Government response to the *Report of the First Independent Review of Intelligence and Security in New Zealand: Intelligence and Security in a Free Society* (G.24a) (the **Review**).

The Review is the first that has been undertaken pursuant to amendments to the Intelligence and Security Committee Act 1996 that were made in 2013, and it has resulted in wide-ranging recommendations. In particular, the Review recommends that the Government Communications Security Bureau (the **GCSB**) and the New Zealand Security Intelligence Service (the **NZSIS**) and their oversight bodies be covered by a single, comprehensive piece of legislation. It emphasises the need to remove barriers to effective co-operation between the GCSB and the NZSIS and the need to improve transparency and oversight arrangements to give the public greater confidence that the agencies are acting lawfully and appropriately.

The Bill adopts the majority of the Review's recommendations. In developing its response to the Review, the Government has sought to ensure that the new legislation—

- is adaptable to changing circumstances and is technology-neutral; and
- reflects New Zealand's long-standing commitment to human rights, democracy, accountability, and the rule of law; and
- is effective, clear, and easy to understand; and
- promotes a joined-up and efficient New Zealand intelligence community that engages effectively with other domestic agencies, including law enforcement agencies; and
- facilitates effective engagement and co-operation with New Zealand's international security partners.

The Bill replaces the 4 Acts that currently apply to the GCSB, the NZSIS, and their oversight bodies (the Inspector-General of Intelligence and Security and the Intelligence and Security Committee). Having 1 piece of legislation will make the law much easier to understand and access.

The Bill continues existing protections around political neutrality, lawful advocacy, protest, and dissent and it requires the Director-General of an intelligence and security agency to regularly consult the Leader of the Opposition. Its purpose is expressly framed as to "protect New Zealand as a free, open, and democratic society", and a variety of provisions are included to increase transparency around the intelligence and security agencies' activities. For example, some activities carried out by the GCSB and the NZSIS as part of their functions will be acknowledged in legislation for the first time (for example, the use of assumed identities and human intelligence activities).

The Bill will bring the GCSB and the NZSIS more fully within the ambit of normal State sector arrangements. Specifically, it establishes the NZSIS as a public service department under the State Sector Act 1988 and makes the GCSB fully subject to that Act. The Director-General of each agency will be appointed by the State Services Commissioner, and their terms and conditions will be determined within the State Sector Act 1988 framework.

To remove artificial and confusing barriers to co-operation and to make clear the consistency of purpose and links within the New Zealand intelligence community, the Bill contains shared objectives, functions, and powers for the GCSB and the NZSIS. It contains a single authorisation regime applying to both agencies that covers their intelligence collection and protective security functions.

Warrants may authorise the intelligence and security agencies to carry out an otherwise unlawful activity where it contributes to 1 of the 3 shared objectives of the agencies. The proposed activity must be necessary and proportionate to the purpose for which it is sought to be carried out in order for a warrant to be issued. The authorisation regime also provides for the possibility of joint warrants being issued that enable the agencies to conduct joint operations using the specialist capabilities of both agencies, where this is judged to be appropriate.

All warrants require the approval of the Attorney-General. Where a warrant is sought to collect intelligence about a New Zealander, both the Attorney-General and a Commissioner of Intelligence Warrants will need to approve the activity that the authorisation is sought for. All warrants are subject to review and audit by the Inspector-General of Intelligence and Security.

To support the GCSB and the NZSIS to carry out their functions and to ensure clarity and transparency around their access to information, the Bill contains a comprehensive information-sharing regime. It also significantly increases the number of Privacy Act 1993 information privacy principles applying to the GCSB and the NZSIS, which will give individuals an avenue for making complaints in respect of certain actions taken by the GCSB and the NZSIS where none has previously existed.

The Bill also makes a number of significant enhancements to the oversight institutions and their roles. These include the removal of the current restriction on the Inspector-General of Intelligence and Security inquiring into operationally sensitive matters, and clarifying that the Inspector-General may review warrants on substantive, as well as procedural, grounds. The Intelligence and Security Committee will be able to request that the Inspector-General of Intelligence and Security inquire into any matter relating to the intelligence and security agencies' compliance with New Zealand law, including human rights law.

The Bill also continues, for an unlimited time, the provisions put in place by the Countering Terrorist Fighters Legislation Bill in 2014, including the amendments to the Passports Act 1992, which enable the refusal of applications for, or cancellation of, New Zealand travel documents of a person if there are reasonable grounds to believe that the person is a danger to national or international security. This Bill includes an additional protection that requires all such decisions regarding New Zealand travel documents to be subject to review by a Commissioner of Intelligence Warrants.

Departmental disclosure statement

The Department of the Prime Minister and Cabinet is required to prepare a disclosure statement to assist with the scrutiny of this Bill. The disclosure statement provides access to information about the policy development of the Bill and identifies any significant or unusual legislative features of the Bill.

A copy of the statement can be found at http://legislation.govt.nz/disclosure.aspx?type=bill&subtype=government&year=2016&no=158

Regulatory impact statement

The Department of the Prime Minister and Cabinet produced a regulatory impact statement on 5 April 2016 to help inform the main policy decisions taken by the Government relating to the contents of this Bill. An addendum to this regulatory impact statement was produced on 11 August 2016.

A copy of this regulatory impact statement and addendum can be found at—

- http://www.dpmc.govt.nz/nziasb16
- http://www.treasury.govt.nz/publications/informationreleases/ris

Clause by clause analysis

Clause 1 is the Title clause. The Bill is, at the end of its Committee of Whole House stage, intended to be divided into the following 2 Bills:

- *Parts 1 to 7 and Schedules 1 to 3* will become the New Zealand Intelligence and Security Act **2016**:
- *Part 8 and Schedule 4* will become the New Zealand Intelligence and Security (Repeals and Amendments) Act **2016**.

Clause 2 is the commencement clause. There are 3 commencement dates—

- on the day after the date of Royal assent the provisions enabling the intelligence and security agencies to have direct access to databases storing the public sector information specified in **Schedule 2** come into force, to ensure the intelligence and security agencies have the benefit of these provisions as soon as possible:
- on **1 April 2017** the amendments to the Passports Act 1992 and the provisions relating to the appointment and functions of the Commissioners of Intelligence Warrants come into force, to ensure the continuity of the temporary provisions in the Passports Act 1992 that expire on 31 March 2017:
- on the day that is 6 months after the date of Royal assent all of the other provisions in the Bill come into force.

Part 1
Preliminary provisions

Clause 3 states the purpose of the Bill.

Clause 4 defines terms used in the Bill. Key terms include intelligence and security agency and ministerial policy statement.

Clause 5 defines national security (as recommended in the Review).

Clause 6 defines sensitive information.

Clause 7 gives effect to the transitional, savings, and related provisions in *Schedule 1*.

Clause 8 states that the Bill binds the Crown.

Part 2
Intelligence and security agencies

Clause 9 continues the New Zealand Security Intelligence Service (the **NZSIS**) and establishes it as a department of State. The NZSIS specialises in human intelligence activities.

Clause 10 continues the Government Communications Security Bureau (the **GCSB**). The GCSB specialises in signals intelligence and information assurance and cybersecurity activities.

Objectives

Clause 11 provides that the principal objectives of the intelligence and security agencies are to contribute to—

- the protection of New Zealand's national security; and
- the international relations and well-being of New Zealand; and
- the economic well-being of New Zealand.

Functions

Clause 12 sets out the following principles that underpin the performance of the functions, of an intelligence security agency. When performing its functions, an intelligence and security agency must act—

- in accordance with New Zealand law and all human rights obligations recognised by New Zealand law; and
- in the performance of its operational functions, independently and impartially; and
- with integrity and professionalism; and
- in a manner that facilitates effective democratic oversight.

Clauses 13 to 18 set out the functions of the intelligence and security agencies. These functions are—

- intelligence collection and analysis:
- protective security services, advice, and assistance:
- co-operation with other entities to facilitate their functions:
- co-operation with other entities to respond to an imminent threat:
- other functions conferred or imposed by or under any other enactment.

Clause 19 provides that it is not a function of an intelligence and security agency to enforce measures for national security except as may be required in connection with information assurance and cybersecurity activities undertaken by the GCSB, or under any other enactment.

Clause 20 provides that activities undertaken by an intelligence and security agency must be relevant to the performance of its functions and that an intelligence and security agency must be kept free from any influence or consideration that is not relevant to its functions.

Clause 21 provides that the activities of an intelligence and security agency must be kept politically neutral.

Clause 22 provides that nothing in the Bill limits the right of persons to engage in lawful advocacy, protest, or dissent, and that the exercise of such rights does not of itself justify the collection of intelligence on any person who is in New Zealand or any class of persons who are in New Zealand.

Clause 23 provides that the Director-General of an intelligence and security agency must keep the Leader of the Opposition informed about matters relating to the agency's functions.

Part 3
Covert activities of intelligence and security agencies

Subpart 1—Assumed identities

Clause 24 states the purpose of this subpart. The purpose is to enable an employee of an intelligence and security agency to acquire, use, and maintain an assumed identity for the purposes of—

- enabling the agency to carry out its activities secretly:
- protecting the identity of the employee.

Clause 25 defines terms used in this subpart. Key terms include assumed identity, authorised person, and employee.

Clause 26 provides that an employee of an intelligence and security agency may acquire, use, and maintain an assumed identity if authorised to do so by the Director-General of the intelligence and security agency. An authorisation may only be given by the Director-General if he or she is satisfied that the acquiring, use, and maintenance of the assumed identity is necessary for a purpose specified in *clause 24*. *Clause 26* also allows an intelligence and security agency to make a false document for use in supporting the use or maintenance of an assumed identity if the Director-General is satisfied that this is necessary for a purpose specified in *clause 24* and the document is of a kind that is not ordinarily issued or given by a Minister or government agency.

Clause 27 provides that an employee may use an assumed identity as if it were his or her own identity.

Clause 28 enables the Director-General of an intelligence and security agency to request any other agency to assist with acquiring, using, and maintaining an assumed identity. A request must provide certain details and confirm that the request is made for either or both the purposes specified in *clause 24*.

Clause 29 provides that an agency may grant a request under *clause 28* for assistance if it is satisfied it is appropriate to do so and that there are reasonable protections in place to ensure the assumed identity will be used appropriately. Assistance may include—

- issuing evidence of an assumed identity (for example, issuing a birth certificate, driver licence, or passport); and
- inserting any information in a register or other record of information (for example, inserting information relating to the assumed identity in the register of births or marriages):
- inserting any operational or administrative information that may be necessary to support evidence of the assumed identity (for example, inserting information supporting the issue of a passport in the name of an assumed identity).

Clause 30 provides that an agency must cancel evidence of an assumed identity if directed to do so by the Director-General of an intelligence and security agency.

Clause 31 provides that evidence of an assumed identity may be issued, given, changed, or cancelled without complying with the requirements of any enactment, policy, or practice specifying any criteria, standards, requirements, or process, or procedure.

Clause 32 imposes restrictions on persons being permitted access to a request for assistance received under *clause 28* or a direction given under *clause 30*.

Clause 33 protects from civil and criminal liability persons who comply with a request made under *clause 28* or a direction given under *clause 30*.

Clause 34 protects from civil and criminal liability authorised persons acquiring, using, and maintaining an assumed identity for any action taken in good faith and with reasonable care and in accordance with any protections referred to in *clause 29(1)*.

Subpart 2—Corporate identities

Clause 35 states the purpose of this subpart. The purpose is to enable an intelligence and security agency to create and maintain a legal entity through which an agency may conduct transactions in order to keep its activities secret.

Clause 36 defines terms used in this subpart. Key terms include agency, entity, and regulatory authority.

Clause 37 enables the Director-General of an intelligence and security agency to request any other agency to take an action that—

- forms or incorporates an entity:
- confers on an entity any legal status or capacity:
- allocates to an entity a unique identifier:
- provides evidence of any legal identity, status, or capacity having been conferred on an entity:
- provides evidence of a unique identifier having been allocated to an entity:
- is ancillary to, or consequential on, any of the above actions.

A request must provide certain details and confirm that the request is made for the purpose specified in *clause 35*.

Clause 38 provides that an agency may comply with a request if it is satisfied it is appropriate to do so and that there are reasonable protections in place to ensure the appropriate use of the legal identity, status, or capacity to be conferred on the entity, or of the unique identifier to be allocated to the entity.

Clause 39 enables the Director-General of an intelligence and security agency to request any other agency to assist with maintaining the legal identity, status, or capacity that has been conferred under *clause 38*.

Clause 40 provides that an agency must take such steps as may subsequently be directed by the Director-General of an intelligence and security agency to negate the effect

of an action earlier taken by that agency in response to a request received under *clause 37*, and to expunge any record of that earlier action.

Clause 41 provides that compliance with a request or direction received from the Director-General of an intelligence and security agency under this subpart may be made without complying with any enactment, policy, or practice that requires compliance with any criteria, standards, requirements, or process or procedure.

Clause 42 imposes restrictions on persons being permitted access to a request for assistance made under *clause 37 or 39* or direction given under *clause 40*.

Clause 43 provides for an entity that has been conferred any legal identity, status, or capacity to 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. In order to maintain the secrecy of an agency's activities, an exemption is neither a legislative instrument nor a disallowable instrument for the purposes of the Legislation Act 2012.

Clause 44 protects from civil and criminal liability persons who comply with a request made under *clause 37 or 39* or a direction given under *clause 40*.

Clause 45 protects from civil and criminal liability entities that have been conferred any legal identity, status, or capacity for any action taken in good faith and with reasonable care in the course of carrying out their activities and in accordance with any protections referred to in *clause 38*.

Part 4
Authorisations

Clause 46 states the purpose of this Part. The purpose is to establish an authorisation regime for intelligence and security agencies that—

- authorises as lawful the carrying out of an activity that would otherwise be unlawful, if certain criteria are satisfied; and
- confers on an intelligence and security agency specified powers for giving effect to an authorisation.

Clause 47 defines terms used in this Part. Key terms include authorised activity, intelligence warrant, and permanent resident of New Zealand.

Clause 48 states that 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.

Clause 49 states that an intelligence and security agency may carry out an otherwise unlawful activity only if that activity is authorised. An authorised activity may lawfully be carried out by an intelligence and security agency despite anything to the contrary in any other Act.

Subpart 1—Intelligence warrants

Types of intelligence warrants

Clause 50 states there are 2 types of intelligence warrants—

- Type 1 intelligence warrants; and
- Type 2 intelligence warrants.

Clause 51 provides that a Type 1 intelligence warrant authorises an intelligence and security agency to carry out an otherwise unlawful activity for any authorised purpose in respect of any person who is—

- a New Zealand citizen; or
- a permanent resident of New Zealand.

Clause 52 provides that a Type 2 intelligence warrant authorises an intelligence and security agency to carry out an otherwise unlawful activity for any authorised purpose other than in respect of—

- a New Zealand citizen; or
- a permanent resident of New Zealand.

Application and issue of intelligence warrants

Clause 53 requires—

- an application for a Type 1 intelligence warrant to be made by the Director-General of an intelligence and security agency to the Attorney-General and the Chief Commissioner of Intelligence Warrants; and
- an application for a Type 2 intelligence warrant to be made by the Director-General of an intelligence and security agency to the Attorney-General.

Clause 54 provides that 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.

Clause 55 provides that a Type 1 intelligence warrant may be issued jointly by the Attorney-General and a Commissioner of Intelligence Warrants if they are satisfied of the matters specified.

Clause 56 provides that a Type 2 intelligence warrant may be issued by the Attorney-General if he or she is satisfied of the matters specified.

Clause 57 sets out the additional criteria for the issue of an intelligence warrant that must be satisfied.

Clause 58 requires the Attorney-General to consult the Minister of Foreign Affairs before issuing an intelligence warrant authorising an activity that is likely to have implications for New Zealand's foreign policy or New Zealand's international relations.

Clause 59 provides for the issue of joint intelligence warrants so that the Director-General of Security and the Director-General of the Government Communications

Security Bureau may jointly or severally carry out the activities authorised by the warrant, and exercise all of the powers under the warrant.

Clause 60 provides that an intelligence warrant may be issued subject to restrictions or conditions that are considered desirable in the public interest by the Attorney-General and a Commissioner of Intelligence Warrants in the case of a Type 1 intelligence warrant, or by the Attorney-General in the case of a Type 2 intelligence warrant.

Clause 61 sets out the matters to be stated in an intelligence warrant. These matters include the type of intelligence warrant issued, the purpose for which the warrant is issued, and the particular activity or activities authorised to be carried out.

Clause 62 requires an intelligence warrant to specify a period not exceeding 12 months for which it is valid.

Authorised activities and powers

Clause 63 sets out the activities that may be carried out under an intelligence warrant that would otherwise be unlawful. These activities include conducting surveillance, intercepting private communications, searching, and seizing.

Clause 64 provides that an intelligence warrant may authorise the carrying out of certain activities for a purpose specified in the warrant and for reasons specified in the warrant. The persons in respect of whom and places in respect of which the activities will be undertaken do not always need to be specified.

Clause 65 sets out the powers of the New Zealand Security Intelligence Service acting under an intelligence warrant. These powers include the power to—

- enter a place, vehicle, or other thing; and
- install, use, maintain, or remove a visual surveillance device, a tracking device, or an interception device; and
- access an information infrastructure, or class of information infrastructures.

Clause 66 sets out the powers of the Government Communications Security Bureau acting under an intelligence warrant. Fewer powers are listed than under *clause 65*; in particular the Government Communications Security Bureau does not have the power to enter a place, vehicle or thing, or to take photographs.

Clause 67 provides that an intelligence warrant does not authorise the carrying out of any activity or the exercise of any power in relation to privileged communications of a New Zealand citizen or permanent resident of New Zealand.

Requests for assistance

Clause 68 enables the Director-General of an intelligence and security agency, when carrying out an activity authorised by an intelligence warrant, to request assistance from the New Zealand Police, any person, or any other organisation. A person who assists is subject to the control of the Director-General and has the same immunities as an employee of an intelligence and security agency.

Urgent intelligence warrants

Clause 69 provides for the issue of a Type 1 intelligence warrant in a situation of urgency. A Type 1 intelligence warrant may urgently be issued by the Attorney-General and a Commissioner of Intelligence Warrants jointly or by the Attorney-General alone. In the latter case, the intelligence warrant is effective as if it had been issued by the Attorney-General and a Commissioner of Intelligence Warrants but the Attorney-General must immediately notify the Chief Commissioner of Intelligence Warrants. The Chief Commissioner of Intelligence Warrants has power to revoke the warrant at any time.

Clause 70 provides for the issue of a Type 2 intelligence warrant by the Attorney-General in a situation of urgency.

Clause 71 requires that the reasons for the urgent issue of an intelligence warrant to be recorded as soon as practicable.

Clause 72 provides that a Type 1 intelligence warrant that has been urgently issued is revoked by operation of law 48 hours after its issue unless, within that time, an application for the issue of a warrant is made in the usual way under *clause 53*.

Clause 73 provides that a Type 2 intelligence warrant that has been urgently issued is revoked by operation of law 48 hours after its issue unless, within that time, an application for the issue of a Type 2 intelligence warrant is made in the usual way under *clause 53*.

Clause 74 provides that information collected under an intelligence warrant issued under *clause 69 or 70* that is subsequently revoked must be destroyed. However, any incidentally obtained intelligence may be retained under *clause 91*.

Clause 75 provides that an intelligence warrant issued urgently under *clause 69 or 70* must be referred as soon as practicable to the Inspector-General of Intelligence and Security for review.

Amendment and revocation of intelligence warrants

Clause 76 provides for the amendment and revocation of intelligence warrants.

Authorisations by Director-General of intelligence and security agency

Clauses 77 to 81 provide for the issue of very urgent authorisations by a Director-General of an intelligence and security agency.

Clause 77 provides that if an application for the urgent issue of a Type 1 or Type 2 intelligence warrant needs to be made but the delay in making that application would defeat the purpose of obtaining the warrant, the Director-General of an intelligence and security agency may authorise the carrying out of the otherwise unlawful activity.

Clause 78 provides that an authorisation given by the Director-General of an intelligence and security agency to carry out an activity for which a Type 1 intelligence warrant is required is effective as if it were a Type 1 intelligence warrant. The Director-General must give notice of the authorisation to both the Attorney-General and the Chief Commissioner of Intelligence Warrants and within 24 hours make an applica-

tion under *clause 53* for the issue of a Type 1 intelligence warrant. The authorisation is revoked if that application is not made, if the Attorney-General or the Chief Commissioner of Intelligence Warrants determines, or if a Type 1 intelligence warrant is not subsequently issued.

Clause 79 similarly provides that an authorisation given by the Director-General of an intelligence and security agency to carry out an activity for which a Type 2 intelligence warrant is required is effective as if it were a Type 2 intelligence warrant. The Director-General must give notice of the authorisation to the Attorney-General and within 24 hours make an application under *clause 53* for the issue of a Type 2 intelligence warrant. The authorisation is revoked if that application is not made, if the Attorney-General determines, or if a Type 2 intelligence warrant is not subsequently issued.

Clause 80 provides that, if an authorisation given by the Director-General of an intelligence and security agency is revoked, all information collected under that authorisation must be immediately destroyed. However, any incidentally-obtained intelligence may be retained under *clause 91*.

Clause 81 provides that an authorisation given by the Director-General of an intelligence and security agency must be referred as soon as practicable to the Inspector-General of Intelligence and Security for review.

Collection of intelligence

Clause 82 states that, in carrying out an authorised activity or in exercising any power, the Director-General of an intelligence and security agency must take all practicable steps that are reasonable in the circumstances to minimise the likelihood of collecting intelligence outside the scope of the authorised activity.

Clause 83 provides that intelligence that is unintentionally collected outside the scope of an authorised activity, or in the course of providing co-operation, advice and assistance under *clause 17*, must be destroyed. However, it need not be destroyed if *clause 91* applies, or if a Type 1 intelligence warrant or Type 2 intelligence warrant is issued authorising its collection.

Offences and immunities

Clause 84 provides that it is an offence to knowingly fail to comply with *clause 74, 80, or 83*. The penalty is a fine not exceeding $10,000.

Clause 85 provides that it is an offence to disclose that an activity is an authorised activity or to use or disclose information obtained from the carrying out of the authorised activity. The penalty is a fine not exceeding $10,000.

Clause 86 provides that it is an offence for a person to knowingly disclose information acquired in carrying out an authorised activity otherwise than in the course of his or her duties. The penalty is a fine not exceeding $10,000.

Clause 87 provides that an employee is immune from criminal liability for any act done in good faith if the person reasonably believed that the act was necessary to ob-

tain an intelligence warrant, and the carrying out of the activity was done in a reasonable manner.

Clause 88 provides that a person is immune from criminal liability for any act done in good faith in carrying out an authorised activity if the person reasonably believed the act was necessary to carry out the activity, and the carrying out of the activity was done in a reasonable manner.

Register of intelligence warrants

Clause 89 requires the Director-General of an intelligence and security agency to keep a register of intelligence warrants issued to him or her. Certain information must be entered in the register in relation to each intelligence warrant, including the type of warrant issued, the particular activity or activities authorised to be carried out, and the conditions that the warrant is subject to. The register must be accessible to the Minister responsible for the intelligence and security agency, the Attorney-General, the Inspector-General of Intelligence and Security, and the Chief Commissioner of Intelligence Warrants (in relation to Type 1 intelligence warrants only).

Subpart 2—Removal warrants

Clause 90 provides that, if any device or equipment that has been installed under an intelligence warrant remains in a place or thing after the warrant has ceased to be in force, the Attorney-General may, on an application, issue a removal warrant. The removal warrant may authorise the removal of the device from the place or thing. For this purpose, a place or thing may be entered and searched and certain powers may be exercised. A removal warrant must specify the period for which it is valid, which may not exceed 12 months.

Subpart 3—Incidentally obtained intelligence

Clause 91 enables the Director-General of an intelligence and security agency to retain any incidentally obtained intelligence for the purpose only of disclosing it to specified persons in specified circumstances (for example, the Director-General may retain the intelligence for the purpose of disclosing it to the Police for the purpose of preventing or detecting a serious crime in New Zealand).

Subpart 4—Commissioners of Intelligence Warrants

Clause 92 provides for the appointment of up to 3 Commissioners of Intelligence Warrants on the recommendation of the Prime Minister. One Commissioner must be appointed Chief Commissioner of Intelligence Warrants.

Clause 93 provides that only a person who has previously held office as a Judge of the High Court may be appointed a Commissioner of Intelligence Warrants.

Clause 94 sets out the functions of a Commissioner of Intelligence Warrants. These functions include advising the Attorney-General on applications for Type 1 intelligence warrants and conducting reviews under *new section 27GF* of the Passports Act 1992.

Clause 95 sets out additional functions of the Chief Commissioner of Intelligence Warrants. The Chief Commissioner is to be the point of contact for all communications with Commissioners.

Clause 96 applies *Part 1 of Schedule 3* (administrative provisions relating to Commissioners).

Part 5
Accessing information held by other agencies

Clause 97 defines terms used in this Part. Key terms include access, agency, and holder agency.

Clause 98 sets out the relationship between Part 5 and other law relating to information disclosure.

Subpart 1—Request and disclosure of information

Clause 99 states the purpose of this subpart. The purpose is to recognise—

- the existing ability of an intelligence and security agency to request information held by other agencies; and
- the existing ability of an agency to disclose information to an intelligence and security agency.

This subpart does not confer on an agency any legal right or obligation.

Clause 100 provides that the Director-General of an intelligence and security agency may request information from another agency if that information is required for the performance or exercise of a function, duty, or power.

Clause 101 provides that an agency may disclose to an intelligence and security agency information that it holds if it is satisfied that the information is required by the intelligence and security agency for the purpose of performing or exercising a function, duty, or power. The disclosure of information may be made whether or not a request for the information has been received. However, this clause is subject to any other enactment that imposes a prohibition or restriction on the disclosure of information, or regulates the manner in which information may be obtained or disclosed. It is also subject to any obligation of confidence.

Subpart 2—Direct access to database information

Clause 102 states the purpose of this subpart. The purpose is to enable an intelligence and security agency to have direct access to the information listed in *Schedule 2*. This information is adoption information, birth information, civil union information, death information, marriage information, name change information, citizenship information, information collected under the Immigration Act 2009, and information collected under the Customs and Excise Act 1996.

Clause 103 provides that an agency holding any of this information (the **holder agency**) must allow the Director-General of an intelligence and security agency access to

any database storing the information if that access is allowed by an agreement entered into between the Minister responsible for the intelligence and security agency and the Minister responsible for the holder agency.

Clause 104 sets out the matters the Ministers must have regard to before entering into an agreement. One of these matters is whether direct access to the information is necessary to enable the intelligence and security agency to perform or exercise a function, duty, or power.

Clause 105 provides that, before entering into an agreement, the Ministers must consult the Privacy Commissioner and the Inspector-General of Intelligence and Security.

Clause 106 specifies the matters that must be included in the content of an agreement.

Clause 107 sets out the requirements for the publication of an agreement.

Clause 108 requires an agreement to be reviewed every 3 years.

Clause 109 provides for the amendment of *Schedule 2* by Order in Council.

Subpart 3—Access to restricted information

Clause 110 states the purpose of this subpart. The purpose is to enable intelligence and security agencies to access restricted information.

Clause 111 defines restricted information. Restricted information is—

- information referred to in section 81 of the Tax Administration Act 1994:
- information relating to national student numbers assigned to students under section 343 of the Education Act 1989:
- photograph images used for driver licences that are stored under section 28(5) of the Land Transport Act 1998.

Clause 112 provides that a Director-General of an intelligence and security agency seeking access to restricted information must apply for permission to—

- the Attorney-General and the Chief Commissioner of Intelligence Warrants if the person to whom the information relates is a New Zealand citizen or a permanent resident of New Zealand; or
- the Attorney-General in any other case.

An application must state the particular restricted information in respect of which access is sought.

Clause 113 specifies the matters on which the Attorney-General and Chief Commissioner of Intelligence Warrants need to be satisfied before permitting access to restricted information relating to a New Zealand citizen or permanent resident of New Zealand.

Clause 114 specifies the matters on which the Attorney-General needs to be satisfied before permitting access to restricted information relating to a person who is not a New Zealand citizen or permanent resident of New Zealand.

Clause 115 sets out criteria that need to be satisfied before access to restricted information may be permitted under *clause 113 or 114*.

Clause 116 requires a permission given under *clause 113 or 114* to specify the particular restricted information that may be accessed by an intelligence and security agency.

Clause 117 requires an agency holding or controlling the restricted information specified in a permission to make that information available to the Director-General of an intelligence and security agency to whom the permission was granted.

Clause 118 provides that restricted information accessed by an intelligence and security agency may only be used, retained, and disclosed by an intelligence and security agency in the performance of its functions.

Part 6
Oversight of intelligence and security agencies

Clause 119 states the purpose of this Part. That purpose is to provide for the independent oversight of the intelligence and security agencies. To this end, both the office of the Inspector-General of Intelligence and Security and the Intelligence and Security Committee are continued with oversight roles.

Subpart 1—Inspector-General of Intelligence and Security

Appointment, functions, duties, and powers of Inspector-General

Clause 120 continues the office of the Inspector-General of Intelligence and Security. The Inspector-General is appointed by the Governor-General on the recommendation of the House of Representatives. Before a person may be recommended for appointment, the Prime Minister must consult the Intelligence and Security Committee about the proposed appointment and advise the House of Representatives that this consultation has been undertaken.

Clause 121 sets out the functions of the Inspector-General. These functions are substantially the same as the Inspector-General's current functions under section 11 of the Inspector-General of Intelligence and Security Act 1996 (the **IGISA**). However, an inquiry undertaken by the Inspector-General into any matter relating to an intelligence and security agency's compliance with the law, or into the propriety of an intelligence and security agency's actions, will be able to be requested by the Intelligence and Security Committee.

Clause 122 requires the Inspector-General to submit to the Ministers each year for comment a draft work programme. The Inspector-General may amend the draft proposed programme to take account of the Ministers' comments. A copy of the final programme must be given to the Ministers and published on the Internet.

Clause 123 re-enacts section 18 of the IGISA and affords protection to employees of intelligence and security agencies who, in good faith, bring any matter to the attention of the Inspector-General. Such employees may not suffer penalty or discrimination

from their employer as a consequence of bringing matters to the attention of the Inspector-General.

Clause 124 re-enacts section 12 of the IGISA, which enables the Inspector-General to liaise with the Auditor-General to avoid inquiries being conducted by both the Inspector-General and the Auditor-General in relation to the same matter. The Inspector-General may also consult specified public office holders about any matter relating to his or her functions and disclose information necessary for the purposes of that consultation.

Clause 125 re-enacts section 15(1) and (2) of the IGISA, which provides that the exercise by the Inspector-General of his or her functions does not limit the jurisdiction of any court, or affect the lawful exercise by a Police employee of any powers in relation to an intelligence and security agency.

Clause 126 provides that if, in conducting a review of an authorisation issued or given under *Part 4*, the Inspector-General identifies any irregularity, that finding does not invalidate the authorisation or any action taken by an intelligence and security agency in reliance on it. The irregularity may also be reported to the Attorney-General and, in the case of an authorisation that is a Type 1 intelligence warrant, to the Chief Commissioner of Intelligence Warrants.

Appointment, functions, duties, and powers of Deputy Inspector-General

Clause 127 continues the office of the Deputy Inspector-General of Intelligence and Security. The Deputy Inspector-General is appointed by the Governor-General on the recommendation of the House of Representatives. Before a person may be recommended for appointment, the Prime Minister must consult the Intelligence and Security Committee about the proposed appointment and advise the House of Representatives that this consultation has been undertaken.

Clause 128 sets out the functions, duties, and powers of the Deputy Inspector-General.

Administrative provisions

Clause 129 provides that the provisions in *Part 2 of Schedule 3* apply in relation to the Inspector-General and Deputy Inspector-General. These provisions deal with administrative matters such as term of office, vacancies, and remuneration.

Advisory panel

Clause 130 continues the advisory panel established under section 15A of IGISA.

Clause 131 re-enacts section 15B of the IGISA, which sets out the functions of the advisory panel. The functions of the advisory panel are to provide advice to the Inspector-General and to report to the Prime Minister on any matter relating to intelligence and security that it considers should be drawn to the attention of the Prime Minister.

Clause 132 substantially re-enacts section 15C of the IGISA and sets out the membership of the advisory panel. The Inspector-General is no longer to be a member of the panel. The panel is to consist of 2 members only, appointed by the Governor-General on the recommendation of the Prime Minister after consultation with the Intelligence and Security Committee. There is no longer the requirement that one of the members be a lawyer.

Clause 133 provides that the provisions in *Part 3 of Schedule 3* apply in relation to the advisory panel. Those provisions deal with administrative matters such as term of office, remuneration, and the procedure of the advisory panel.

Clause 134 provides that a complaint may be made to the Inspector-General by—

- a New Zealand person alleging 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; or
- an employee or former employee of an intelligence agency alleging that he or she has or may have been adversely affected by any act, omission, practice, policy, or procedure of an intelligence agency in any case where all established internal remedies have been exhausted or the chief executive of the agency otherwise agrees; or
- the Speaker of the House of Representatives on behalf of 1 or more members of Parliament alleging that the House has or may have been adversely affected by any act, omission, practice, policy, or procedure of an intelligence and security agency.

The provision re-enacts section 11(1)(b), (ba), and (5) of the IGISA.

Clause 135 provides that complaints may be made orally or in writing, but if made orally must be subsequently confirmed in writing.

Clause 136 provides that as soon as practicable after receiving a complaint, the Inspector-General must decide whether to conduct an inquiry in respect of the complaint and advise the complainant of his or her decision.

Clause 137 sets out the circumstances in which the Inspector-General may decide not to conduct, or continue to conduct, an inquiry in respect of a complaint. The circumstances in which the Inspector-General may decide not to inquire into a complaint include where the complaint is trivial, frivolous, vexatious, or not made in good faith. In any case where the Inspector-General decides not to continue to conduct an inquiry in respect of a complaint, the Inspector-General must inform the complainant of that decision.

Procedure for inquiries

Clause 138 provides that on commencing an inquiry the Inspector-General must give the chief executive of the relevant intelligence and security agency notice of the inquiry and, if relevant, a copy of the complaint to which the inquiry relates. If the inquiry was commenced not by a complaint but on the Inspector-General's own initia-

tive, the Inspector-General must also inform the Minister responsible for the relevant intelligence and security agency.

Clauses 139 to 146 re-enact existing sections 19 to 24, 25(3), and 26 of the IGISA and relate to the procedures and powers of the Inspector-General when conducting inquiries. These clauses—

- provide for the obtaining of information by the Inspector-General:
- confer powers of entry to places occupied or used by an intelligence and security agency:
- provide for the protection and privileges of witnesses appearing before the Inspector-General.

Clause 147 re-enacts sections 11(6) and 25(1), (2), and (8) of the IGISA and provides that the Inspector-General must, after completing an inquiry, report his or her conclusions to the complainant and, together with any recommendations, to the Minister and Director-General of the intelligence and security agency to which the inquiry related. This clause also provides that the Inspector-General must also forward his or her report to the Intelligence and Security Committee if the inquiry was conducted at the request of the Committee, or on the Inspector-General's own initiative, or if the Minister or Prime Minister agrees.

Clause 148 re-enacts section 25(5) of the IGISA and provides that the Inspector-General may report to the Minister on the compliance by an intelligence and security agency with the recommendations in the Inspector-General's report, and on the adequacy of any remedial or preventative measures taken by the agency following an inquiry.

Clause 149 re-enacts section 25(6) and (7) of the IGISA and requires the Minister, after receiving a report from the Inspector-General, to provide a response to the Minister and the chief executive of the intelligence and security agency to which the inquiry related. This clause also provides that the Minister may forward his or her response to the Intelligence and Security Committee.

Clause 150 re-enacts section 25A of the IGISA which provides for the publication of an Inspector-General's report.

Clause 151 re-enacts section 25(4) of the IGISA and requires that when the Inspector-General has completed an inquiry he or she must return all documents and materials belonging to an intelligence and security agency. All other documents and things relating to an inquiry must either be kept in safe custody or disposed of in accordance with the requirements applying to intelligence and security agencies.

Clause 152 re-enacts section 19(9) of the IGISA and provides that a proceeding, report, or finding of the Inspector-General may not be challenged, reviewed, quashed or questioned in any court, except on the ground of lack of jurisdiction.

Clause 153 re-enacts section 29 of the IGISA and prohibits the publication or broadcast of certain matters relating to an inquiry.

Subpart 2—Intelligence and Security Committee

Continuation of Intelligence and Security Committee

Clause 154 continues the Intelligence and Security Committee.

Clause 155 sets out the functions of the Committee, which replicate the Committee's existing functions in section 6 of the Intelligence and Security Committee Act 1996 (the **ISCA**) and add one further function. The Committee may request the Inspector-General to inquire into an intelligence and security agency's compliance with New Zealand law or into the propriety of particular activities of an agency.

Clause 156 sets out the membership of the Committee. The Committee must comprise at least 5, but no more than 7 members. The members comprise the Prime Minister, the Leader of the Opposition, members nominated by the Prime Minister, and members nominated by the Leader of the Opposition.

Clause 157 specifies how a vacancy in the membership of the Committee is to be filled.

Clause 158 requires the House of Representatives to endorse nominated members.

Clause 159 provides that the Committee may not transact business until the nominated members have been endorsed.

Clause 160 re-enacts section 7(3) and 7A(1)–(3) of the ISCA and provides that it is generally the Prime Minister who chairs the Committee.

Clause 161 provides that the provisions in *Part 4 of Schedule 3* apply in relation to the Committee. Those provisions deal with the membership and procedure of the Committee.

Evidence

Clause 162 re-enacts section 14 of the ISCA and provides that the Committee may require persons to attend before it.

Clause 163 re-enacts section 17 of the ISCA and deals with the provision of information to the Committee and the safe keeping of that information by the Committee.

Clause 164 re-enacts section 19 of the ISCA and prohibits persons appointed to assist the Committee from disclosing certain information, including sensitive information.

Part 7
Miscellaneous provisions

Ministerial policy statements

Clause 165 requires the Minister responsible for an intelligence and security agency to issue ministerial policy statements for covert activities under *Part 3* in relation to—

- authorising the acquiring, use, and maintenance of an assumed identity:
- acquiring, using, and maintaining an assumed identity:

- creating and maintaining a legal entity.

Clause 166 requires the Minister responsible for an intelligence and security agency to issue ministerial policy statements providing guidance to the intelligence and security agency in relation to—

- co-operating with an overseas public authority:
- providing advice and assistance to an overseas public authority:
- sharing intelligence with an overseas public authority.

Clause 167 enables the Minister responsible for an intelligence and security agency to issue other ministerial policy statements providing guidance to an intelligence and security agency in relation to any other matter.

Clause 168 states the matters that a ministerial policy statement must contain.

Clause 169 requires a Minister to undertake consultation with certain persons, including the Inspector-General, before issuing a ministerial policy statement.

Clause 170 provides for ministerial policy statements to be amended, revoked, or replaced by the Minister in consultation with certain other persons.

Clause 171 enables a ministerial policy statement to be issued applying to both intelligence and security agencies.

Clause 172 provides that a ministerial policy statement takes effect when it is signed by the issuing Minister and continues in effect for up to 3 years.

Clause 173 provides for the publication of ministerial policy statements. The Director-General of the intelligence and security agency to which a ministerial policy statement applies must make it publicly available on an Internet site.

Clause 174 confirms that a ministerial policy statement is not, for the purposes of the Legislation Act 2012, a legislative instrument or a disallowable instrument. MPSs are neither legislative nor disallowable instruments because they do not have legislative effect, but rather are intended to provide guidance as to how lawful activities may be carried out. Failure to comply with a MPS does not make the activity unlawful.

Security records

Clause 175 re-enacts section 20 of the IGISA and provides for the Inspector-General to have access to security records.

Clause 176 re-enacts section 26 of the IGISA and provides that the Inspector-General, the Deputy Inspector-General, an employee of the Inspector-General, and a member of the advisory panel, must not disclose to any other person security records or other official information relating to the activities of an intelligence and security agency. Disclosure of information relating to the activities of an intelligence and security agency may, however, be made to the Minister responsible for that agency.

Confidentiality

Clause 177 re-enacts existing provisions that require office holders, employees and contractors to keep confidential all information that comes to their knowledge in the

performance or exercise of their functions, duties, and powers, and not to record, use, or disclose that information except for the purpose of carrying out their functions or duties.

Security clearance information

Clause 178 provides that information that the New Zealand Security Intelligence Service has for the purposes of a security clearance assessment may only be used for the purposes of that assessment, any other security clearance assessment, or counter-intelligence. This provision overrides information privacy principle 10 in section 6 of the Privacy Act 1993.

Annual reports

Clause 179 re-enacts section 4J of the New Zealand Security Intelligence Service Act 1969 and section 12 of the Government Communications Security Bureau Act 2003 and provides for the preparation and publication of the annual reports of the intelligence and security agencies. In addition to the information required by section 45 of the Public Finance Act 1989 to be included in an annual report, *subclause (2)* sets out other information that agencies will now need to include. For example, agencies will now need to include in their reports a statement as to the number of applications made for a Type 1 intelligence warrant, and the number of those applications approved or declined.

Clause 180 re-enacts section 27 of the IGISA and provides for the preparation and publication of the Inspector-General's annual report.

Clause 181 requires the Intelligence and Security Committee to present an annual report to the House of Representatives on the activities of the Committee, and to make all annual reports publicly available.

Clause 182 re-enacts section 18 of the ISCA and restricts what the Committee may disclose in its annual report.

Offences

Clause 183 re-enacts section 23(8) of the IGISA and provides that it is an offence to obstruct, hinder, or resist the Inspector-General in the exercise of his or her powers, or to refuse or wilfully fail to comply with any lawful requirement of the Inspector-General. The penalty on conviction is a fine not exceeding $5,000.

Clause 184 makes it an offence to do any of the following without reasonable excuse—

- pretend to be an employee of an intelligence and security agency:
- assume the name, designation, or description of an employee of an intelligence and security agency.

The penalty on conviction is a term of imprisonment of 12 months or a fine not exceeding $15,000, or both.

Clause 185 re-enacts section 13A of the New Zealand Security Intelligence Service Act 1969 and makes it an offence for a person, without the written consent of the Minister responsible for the intelligence and security agency, to publish, broadcast, or otherwise distribute and disclose the fact that a person is an employee of an intelligence and security agency (other than the Director-General of an intelligence and security agency). The penalty on conviction is a fine not exceeding $5,000 in the case of an individual, or a fine not exceeding $20,000 in the case of a body corporate.

False or misleading representations about employment

Clause 186 allows an employee of an intelligence and security agency to make a false or misleading representation about his or her employment if the representation is made for the purpose of keeping secret the fact that he or she is an employee of the agency. The representation may only be made in accordance with any requirements of the Director-General of the agency.

Clause 187 provides an immunity and other protections to the employee in relation to the false or misleading representation.

Exceptions and immunities

Clause 188 provides an exception from criminal liability for an employee in respect of the offence of receiving under the Crimes Act in certain cases where the employee receives unsolicited information. *Clause 188* also restricts an intelligence and security agency disclosing unsolicited information that it obtains.

Clause 189 provides an exception from criminal liability for an employee of the New Zealand Security Intelligence Service for breaches of Parts 3, 5, and 6 of the Land Transport(Road User) Rule 2004 where the employee reasonably needs to take that action to continue visual surveillance from a vehicle in a public road. The employee is required to take all reasonable steps to ensure that his or her actions do not cause injury or damage or interfere with any other person.

Clause 190 provides that where a question about whether an immunity under the Bill applies in a particular situation, the employee or entity concerned must establish, on the balance of probabilities, that the immunity applies. *Clause 90* also provides that, in the event of an inconsistency between the immunities provided by the Bill and immunities under any other enactments, the provision of the Bill prevail.

Intelligence functions of Chief Executive of Department of the Prime Minister and Cabinet

Clause 191 sets out the functions of the Chief Executive of the Department of the Prime Minister and Cabinet in relation to intelligence assessments.

Clause 192 provides that in performing the functions in *clause 191* the Chief Executive must act independently.

Periodic reviews

Clause 193 provides for periodic reviews of this legislation. The first review must be commenced 5 years after the legislation comes into force, and subsequent reviews must be held at intervals not shorter than 5 years and not longer than 7 years.

Clause 194 provides for the appointment of 2 reviewers by the Prime Minister and for the Prime Minister to specify the terms of reference.

Clause 195 provides for the provision of information to the reviewers.

Clause 196 requires the reviewers to prepare a report at the conclusion of their review and for this report to be provided to the Intelligence and Security Committee and subsequently presented to the House of Representatives.

Clause 197 provides for the reviewers to receive remuneration at a rate and of a kind determined by the Prime Minister in accordance with the Government fees framework.

Clause 198 provides that the Ministry of Justice is responsible for providing the reviewers with administrative, secretarial, and other necessary support.

Clause 199 provides that the reviewers may determine their own procedure.

Part 8
Repeals and amendments

Clause 200 repeals the following Acts, which are replaced by the Bill:

- New Zealand Security Intelligence Service Act 1969:
- Intelligence and Security Committee Act 1996:
- Inspector-General of Intelligence and Security Act 1996:
- Government Communications Security Bureau Act 2003.

Amendments to Births, Deaths, Marriages, and Relationships Registration Act 1995

Clause 201 to 205 relate to the Births, Deaths, Marriages, and Relationships Registration Act 1995 (the **Act**). The substantive amendment is to section 65 of the Act. Currently, under section 65 the Minister in charge of the New Zealand Security Intelligence Service can request the Minister responsible for the administration of the Act to create new identity information. This provision is amended to enable the Director-General of either of the intelligence and security agencies to request the creation of new identity information. If, on receiving a request, the Minister responsible for the administration of the Act is satisfied of the matters in *clause 29(1)* of this Bill, the Minister may direct the Registrar-General to create the new identity information requested. Consequential amendments are made to sections 2, 75F, and 78 of the Act.

Amendments to Crimes Act 1961

Clauses 206 to 208 relate to the Crimes Act 1961 (the **Act**). A *new section 78AA* is inserted in the Act similar to existing section 78A of the Act. Existing section 78A of the Act is an offence provision relating to the wrongful communication, retention, or copying of official information. *New section 78AA* mirrors this provision in respect of classified information and applies to persons who hold, or have held, a New Zealand Government-sponsored national security clearance to access classified information and to persons to whom classified information has been disclosed in confidence. The consent of the Attorney-General will be required to prosecute this new offence.

Amendments to Education Act 1989

Clauses 209 and 210 relate to the Education Act 1989 (the **Act**). Section 346 of the Act is amended so that it is not an offence to use or disclose a person's national student number if required to do so by *clause 117* of the Bill (access to restricted information must be provided if permitted).

Amendments to Electronic Identity Verification Act 2012

Clauses 211 and 212 relate to the Electronic Identity Verification Act 2012 (the **Act**). Section 12 of the Act, which enables certain individuals to have more than 1 electronic identity credential, is amended to apply also to employees of the Government Communications Security Bureau. This amendment is necessary because of the amendment to section 65 of the Births, Deaths, Marriages, and Relationships Registration Act 1995 (*see clauses 201 to 205*).

Amendment to Employment Relations Act 2000

Clauses 213 and 214 relate to the Employment Relations Act 2000 (the **Act**). A *new section 172A* is inserted in the Act to provide that when any matter coming before the Employment Relations Authority relates to or arises from a recommendation of the New Zealand Security Intelligence Service about whether an individual should be granted a security clearance, the Inspector-General must be requested to prepare a report on the recommendation (if the Inspector-General has not done so already). The parties are entitled to receive a copy of the Inspector-General's report and to make submissions on it. The Employment Authority must have regard to the report before making a determination.

Amendments to Immigration Act 2009

Clauses 215 to 229 relate to the Immigration Act 2009 (the **Act**). There are 4 substantive changes to the Act as follows:

- section 96 is replaced so that the chief executive of the Ministry of Business, Innovation, and Employment may request a carrier or person in charge of a commercial craft to collect advance passenger processing information from persons travelling to, or from, New Zealand. Currently, advance passenger processing information is collected only from persons travelling to New Zealand:

- a *new section 97A* is inserted in the Act that enables the chief executive to decide that a person intending to travel from New Zealand may not board a craft, or may board a craft subject to conditions, and to notify the carrier or the person in charge of the craft accordingly. This provision corresponds to section 97 of the Act, which empowers the chief executive to make decisions about persons intending to board a craft for the purpose of travelling to New Zealand:
- section 102 of the Act is amended to require a carrier, or a person in charge of a commercial craft, to provide to the chief executive other prescribed information about persons intending to travel from New Zealand (including persons who did not board the craft):
- *new sections 303A to 303C* are inserted in the Act to enable the Ministry of Business, Innovation, and Employment to provide information to a specified agency (the New Zealand Police, the Department of Corrections, the New Zealand Customs Service, and the Civil Aviation Authority of New Zealand) so that the agency has a longer period of time to identify any person of interest who is intending to board a craft to travel from New Zealand and to exercise any functions or powers in relation to that person before he or she departs from New Zealand.

Amendments to Land Transport Act 1998

Clauses 230 to 232 amend the Land Transport Act 1998 (the **Act**). Section 24A of the Act is amended to enable the Director-General of either intelligence and security agency to request the New Zealand Transport Agency to create and issue a driver licence for an assumed identity (currently only the Director of Security can make such request). As with the amendments to the Births, Deaths, Marriages, and Relationships Registration Act 1995 (*see clauses 201 to 205*), and to the Electronic Identity Verification Act 2012 (*see clauses 211 and 212*), this amendment is necessary because of the provisions in *subpart 1 of Part 3* of the Bill.

Section 200 of the Act is also amended. This section restricts who may have access to photograph images used for driver licences, and is amended to reflect that the Director-General of an intelligence and security agency may be permitted access to these images under *subpart 3 of Part 5* of the Bill.

Amendments to Passports Act 1992

Clauses 233 to 261 relate to the Passports Act 1992 (the **Act**). The temporary provisions inserted in the Act by the Passports Amendment Act 2014 (sections 45 and 46 and Schedule 2 of the Act) expire on 31 March 2017. The purpose of the amendments in *clauses 234 to 261* is to continue those provisions beyond this date. The continuation of the provisions is without interruption as the transitional provision in section 46 of the Act (inserted by the Passports Amendment Act 2014) is repealed.

The effect of the amendments is to extend the Minister's powers, on the grounds of national security, to—

- refuse to issue a passport:

- cancel a passport:
- cancel a certificate of identity:
- cancel an emergency travel document:
- refuse to issue a refugee travel document:
- cancel a refugee travel document.

The amendments also provide for the temporary suspension of these New Zealand travel documents, clarify the application of sections 29AA to 29AC in respect of these provisions, and limit Crown liability for certain decisions taken under the provisions. There is 1 substantive policy change implemented in the amendments. If the Minister of Internal Affairs decides to cancel or refuse to issue a New Zealand travel document, the Minister must notify the Chief Commissioner of Intelligence Warrants. After receipt of all relevant documents, the Chief Commissioner must review the Minister's decision and prepare a report if he or she considers that the decision is not supported by the documentation. That report must recommend the Minister reconsider his or her decision and state the reasons for that recommendation. The Minister must then reconsider his or her decision and confirm, vary, or revoke it. In any case where the Minister reviews his or her decision, the person affected by that decision must be notified of the Chief Commissioner's recommendation and the outcome of the Minister's reconsideration.

Amendments to Privacy Act 1993

Clauses 262 to 264 relate to the Privacy Act 1993 (the **Act**). Three amendments are made to the Act as follows:

- information privacy principle 10 in section 6 of the Act is amended to include a further exception. This further exception will allow an agency holding personal information to use that information for a different purpose from the purpose for which it was obtained if the agency believes on reasonable grounds that the different purpose is necessary to enable an intelligence and security agency to perform a statutory function:
- information privacy principle 11 in section 6 of the Act is amended to include a further exception. This further exception will allow an agency holding personal information to disclose the information if the agency believes on reasonable grounds that the disclosure is necessary to enable an intelligence and security agency to perform a statutory function:
- section 57, which provides that only information privacy principles 6 and 7 apply to intelligence and security agencies, is replaced. All of the information privacy principles will now apply to intelligence and security agencies, except information privacy principles 2, 3, and 4(b). This will mean, for example, that intelligence and security agencies must not collect personal information by any unlawful means, and may only use and disclose personal information in accordance with information privacy principles 10 and 11.

Amendments to Protected Disclosures Act 2000

Clauses 265 to 267 relate to the Protected Disclosures Act 2000 (the **Act**). Section 12 of the Act requires the internal procedures of an intelligence and security agency to contain certain rules about whom disclosures may be made to. A *new section 12* extends the application of this provision to any other organisation in the public sector that holds or has access to classified information, or information relating to the activities of an intelligence and security agency. Section 13 is also replaced with a new provision that does not include reference to intelligence and security (as this is now covered by *new section 12*).

Amendments to Public Finance Act 1989

Clauses 268 to 271 relate to the Public Finance act 1989 (the **Act**). The definition of department in section 2 of the Act is amended to recognise that the New Zealand Security Intelligence Service is now a department so no longer needs to be separately identified. Section 15A of the Act is amended so that intelligence and security agencies will no longer be exempt from the requirement to provide a concise explanation of what an appropriation is intended to achieve. Section 45E of the Act is amended to remove some of the exemptions currently applying to intelligence and security agencies.

Amendments to Search and Surveillance Act 2012

Clauses 272 to 274 relate to the Search and Surveillance Act 2012 (the **Act**). The effect of the amendments is to extend the application of section 25 of the Act so that a constable may, without a warrant, carry out a search if there are reasonable grounds to suspect that an offence against *new section 78AA* of the Crimes Act 1961 (inserted by *clause 207*) has been, is being, or will be committed and that there is great urgency requiring immediate action.

Amendments to State Sector Act 1988

Clauses 275 to 277 relates to the State Sector Act 1988 (the **Act**). Schedule 1 of the Act is amended to list the New Zealand Security Intelligence Service as a department. A consequential amendment is made to section 44 of the Act.

Amendment to Tax Administration Act 1994

Clauses 278 and 279 relate to the Tax Administration Act 1994 (the **Act**). Section 81 of the Act is amended so that an Inland Revenue officer may communicate information to the Director-General of an intelligence and security agency if required to do so under *clause 117* of the Bill (access to restricted information must be provided if permitted).

Consequential amendments

Clause 280 gives effect to *Schedule 4*, which makes consequential amendments to other enactments.

Schedules

Schedule 1 sets out transitional, savings, and related provisions.

Schedule 2 sets out the databases accessible to intelligence and security agencies under *subpart 2 of Part 5*.

Schedule 3 sets out administrative provisions applying to Commissioners of Intelligence Warrants, the Inspector-General and Deputy Inspector-General, the advisory panel, and the Intelligence and Security Committee.

Schedule 4 sets out consequential amendments to other enactments.

Rt Hon John Key

New Zealand Intelligence and Security Bill

Government Bill

Contents

Part 5
Accessing information held by other agencies

Part 6
Oversight of intelligence and security agencies

The Parliament of New Zealand enacts as follows:

1 Title

This Act is the New Zealand Intelligence and Security Act **2016**.

2 Commencement

(1) The following provisions come into force on the day after the date of Royal assent:

(a) **subpart 2 of Part 5**:

(b) **Schedule 2**:

(c) the amendments in **Schedule 4** relating to the Customs and Excise Act 1996.

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

(a) **subpart 4 of Part 4**:

(b) **clauses 233 to 261**:

(c) **Part 1 of Schedule 3**.

(3) 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 130**

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 92(2)**

Commissioner of Intelligence Warrants means a Commissioner of Intelligence Warrants appointed under **section 92(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

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

Deputy Inspector-General means the Deputy Inspector-General of Intelligence and Security appointed under **section 127**

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

entity has the meaning given to it by **section 36**

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

Government Communications Security Bureau means the Government Communications Security Bureau continued by **section 10**

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 taken 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 120**

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 154**

intelligence warrant has the meaning given to it by **section 47**

ministerial policy statement means a ministerial policy statement issued under **section 165, 166, or 167**, and includes any amendments made to a statement under **section 170**

national security has the meaning given to it by **section 5**

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 **subparagraph (i)** or **(ii)**; 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 9**

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

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)**

sensitive information has the meaning given to it by **section 6**

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 Meaning of national security

In this Act, **national security** means the protection against—

(a) threats, or potential threats, to New Zealand's status as a free and democratic society from unlawful acts or foreign interference:

(b) imminent threats to the life and safety of New Zealanders overseas:

(c) threats, or potential threats, that may cause serious harm to the safety or quality of life of the New Zealand population:

(d) unlawful acts, or acts of foreign interference, that may cause serious damage to New Zealand's economic security or international relations:

(e) threats, or potential threats, to the integrity of information or infrastructure of critical importance to New Zealand:

(f) threats, or potential threats, that may cause serious harm to the safety of a population of another country as a result of unlawful acts by a New Zealander that are ideologically, religiously, or politically motivated:

(g) threats, or potential threats, to international security.

6 Meaning of sensitive information

(1) In this Act, unless the context otherwise requires, **sensitive information** means information of a kind specified in **subsection (2)** that, if disclosed, would be likely to—

(a) prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand; or

(b) 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) prejudice the maintenance of the law, including the prevention, investigation, and detection of offences and the right to a fair trial; or

(d) endanger the safety of any person.

(2) The kinds of information are as follows:

(a) information that might lead to the identification of, or provide 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 carrying out of 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 by which that information has been provided; 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 intelli-

gence and security agency without the consent of the Government or agency by which that information has been provided.

7 Transitional, savings, and related provisions

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

8 Act binds the Crown

This Act binds the Crown.

Part 2
Intelligence and security agencies

9 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

10 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

11 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

12 Principles underpinning performance of functions

(1) 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.

(2) **Subsection (1)** does not impose particular duties on, or give particular powers to,—

(a) an intelligence and security agency; or

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

(c) an employee of an intelligence and security agency.

(3) Despite **subsection (2)(b)**, the Director-General of an intelligence and security agency must take all reasonable steps to ensure that any co-operation with foreign jurisdictions and international organisations in the performance of any function is consistent with **subsection (1)(a)**.

Compare: 1969 No 24 s 4AAA(1)(c), (2); 2003 No 9 s 8D(1), (2)

13 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 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 in accordance with **subsection (3)** to receive the 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 entity authorised by the Minister for the purposes of this subsection.

(3) Before authorising, under **subsection (1)(b)(iii)**, the provision of intelligence to any overseas person or class of persons, the Minister must be satisfied that the intelligence and security agency will be acting in accordance with **section 12(1)(a)** when providing that intelligence.

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

Compare: 2003 No 9 s 8B

14 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) public authorities (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) 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)

15 Information assurance and cybersecurity activities

(1) The information assurance and cybersecurity activities referred to in **section 14(2)(a)(ii)**, in relation to the Government Communications Security Bureau, are—

(a) providing information assurance and cybersecurity activities to—

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

(ii) any person or class of persons (whether in New Zealand or overseas) authorised by the Minister for the purpose of this subsection; 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) Any activity carried out by the Government Communications Security Bureau under **subsection (1)(a)** does not require an authorisation under **Part 4** if that activity is—

(a) a lawful activity; or

(b) undertaken with the consent of the public authority or entity.

(4) Any information obtained by the Government Communications Security Bureau in performing the activities under this section may be used only in the performance or exercise of a function, duty, or power under **section 14** unless otherwise authorised under **Part 4**.

Compare: 2003 No 9 s 8A

16 Co-operation with other entities 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 following entities for the purpose of facilitating the performance or exercise of their functions, duties, or powers:

(i) the New Zealand Police; and

(ii) the New Zealand Defence Force.

(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 entities may lawfully undertake; and

(b) subject to and in accordance with any limitations, restrictions, and protections under which those entities 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 an entity under **subsection (1)(b)**, is subject to—

(a) the jurisdiction of any other body or authority to the same extent as the entity'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) An employee is immune from criminal liability for any act done under this section in good faith in providing assistance to the New Zealand Police or the New Zealand Defence Force if—

(a) the employee reasonably believed that the act was necessary to provide the 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

17 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, any entity that is responding to an imminent threat to the life and 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 13 or 14**; 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 83(3)**; 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) Any co-operation, advice, and assistance provided under this section is subject to the oversight of the Inspector-General.

18 Additional functions

In addition to the functions specified in **sections 13 to 17**, 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)

19 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) under any other enactment.

Compare: 1969 No 24 s 4(2)

20 Activities of agencies must be relevant to functions

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

(a) the activities of the intelligence and security agency are limited to those that are relevant to the performance of its functions; and

(b) the intelligence and security agency is kept free from any influence or consideration that is not relevant to the agency's functions.

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

21 Activities of intelligence and security agencies must be politically neutral

The Director-General of an intelligence and security agency must take all reasonable steps to ensure that the agency does not take any action for the purpose of furthering or harming the interests of any political party.

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

22 Limitation on collecting intelligence within New Zealand

(1) Nothing in this Act limits the right of persons to engage in lawful advocacy, protest, or dissent in respect of any matter.

(2) The exercise of the right in **subsection (1)** does not, of itself, justify an intelligence and security agency collecting intelligence on any person who is in New Zealand or any class of persons who are in New Zealand.

Compare: 1969 No 24 ss 2(2)

23 Director-General of 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

24 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 that assumed identity, and maintain that 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.

25 Interpretation

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 any information

acquire an assumed identity means 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 26** to acquire an assumed identity, to use that assumed identity, and to maintain that assumed identity

employee means—

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

(b) any person who is approved by the Director-General of an intelligence and security agency to undertake 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.

26 Assumed identity may be acquired, used, and maintained

(1) An employee of an intelligence and security agency may acquire an assumed identity, use that identity, and maintain that identity if the acquiring, use, and maintenance of the assumed identity is authorised by the Director-General of the intelligence and security agency.

(2) The Director-General may authorise the acquiring, use, and maintenance of an assumed identity only if he or she is satisfied that the acquiring, use, and main-

tenance of the assumed identity is necessary for a purpose specified in **section 24**.

(3) An intelligence and security agency 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 is necessary for a purpose specified in **section 24**; and

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

(4) Regard must be had to every relevant ministerial policy statement that has been issued in the following cases:

(a) when authorising the acquiring, use, and maintenance of an assumed identity:

(b) when acquiring, using, and maintaining that identity:

(c) when considering whether the making and use of a false document is necessary for a purpose specified in **section 24**.

27 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 29**):

(b) to establish, maintain, and operate a legal entity (with or without assistance under **section 38 or 39**).

(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 26(3)**.

28 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 that assumed identity:

(c) maintain that assumed identity.

(2) A request must—

(a) provide details of—

(i) the authorised person; 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 24**.

29 Assistance to acquire, use, and maintain assumed identity

(1) An agency that receives a request under **section 28** may grant the request if it is satisfied that—

(a) it is appropriate to do so having regard to—

(i) the purposes of this subpart; and

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

(b) reasonable protections are or will be in place for the purpose of ensuring that, as far as practicable, the authorised person will use the assumed identity appropriately.

(2) 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 record of information (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)**.

30 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 28**.

(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 record of information:

(b) preventing or restricting access to any information in a register or other record of information:

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

31 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.

32 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 28** or compliance with a direction under **section 30** where the access may compromise the secrecy relating to the acquisition, use, and maintenance of an assumed identity.

(2) An agency must not permit any person (**person A**) to access a request made under **section 28**, a direction given under **section 30**, 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 the 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) the 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)**.

33 Immunity of persons assisting and 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 28**; or

(b) a direction given under **section 30**.

(2) An intelligence and security agency is protected from civil and criminal liability, however it may arise, in relation to any act that it does, or omits to do, in good faith and with reasonable care in the course of making a false document under **section 26(3)**.

34 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 26**; and

(b) in accordance with any protections referred to in **section 29(1)**.

(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

35 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.

36 Interpretation

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 any information

agency means—

(a) the chief executive of a department:

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

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

(d) a regulatory authority

entity means—

(a) an unincorporated body:

(b) a body corporate:

(c) a corporation sole:

(d) a trust

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.

37 Request for corporate identity, status, etc

(1) The Director-General of an intelligence and security agency may, for the purpose specified in **section 35**, request any other agency to do any of the following:

(a) form or incorporate 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; 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 35**.

38 Conferring corporate identity, status, etc

(1) An agency that receives a request under **section 37** may comply with that request if it is satisfied that—

(a) it is appropriate to do so having regard to—

(i) the purpose of this subpart; and

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

(b) reasonable protections are or will be in place for the purpose of ensuring that, as far as practicable, the intelligence and security agency uses 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.

(2) In granting the request, the agency may do anything to take an action referred to in **section 37**, including—

(a) omitting, amending, replacing, or inserting any information in any register or other record of information (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)**.

39 Maintaining corporate identity and status

(1) The Director-General of an intelligence and security agency may, for the purpose specified in **section 35**, request an agency to assist with maintaining the legal identity, status, or capacity that has been conferred under **section 38**.

(2) An agency that receives a request under **subsection (1)** may comply with that request if it is satisfied that it is appropriate to do so having regard to—

(a) the purposes 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.

(3) 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 record of information (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)**.

40 Dissolution or deregistration, etc, of entity

(1) A Director-General of an intelligence and security agency who made a request under **section 37** may, at any time, direct an agency that took any action of the kind specified in **section 37(1)** 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 made 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 record of information:

(b) preventing or restricting access to any information in a register or any other record of information:

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

41 Non-compliance with enactments, policies, and practices

Compliance with a request made under **section 37, 39, or 43** or a direction given under **section 40** 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.

42 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 37 or 39**, an exemption under **section 43**, or compliance with a direction under **section 40** where the access may compromise the secrecy relating to the creation and maintenance of the legal entity.

(2) An agency must not permit any person (**person A**) to access a request made under **section 37, 39, or 43**, a direction given under **section 40**, 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)**.

43 Entity exempt from complying with legal requirements, etc

(1) An entity that has been conferred with any legal identity, status, or capacity under **section 38** 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.

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

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

(a) the exemption is necessary to enable the entity to maintain its legal identity, status, or capacity for the purposes of this subpart; and

(b) granting the exemption will not have a significant negative impact on any members of the public.

(4) The agency must, in considering the matters under **subsection (3)**, have regard to the purposes of the enactment referred to in **subsection (1)**.

(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.

44 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 37, 39, or 43**; or

(b) a direction given under **section 40**.

45 Immunity of entity

(1) An entity that has been conferred any legal identity, status, or capacity under **section 38** 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 38(1)**.

(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.

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)

authorised activity means an activity that is authorised by—

(a) an intelligence warrant; or

(b) an authorisation given under **section 77**; or

(c) a removal warrant

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 intelligence means intelligence that—

(a) is collected in the course of performing or exercising a function under **section 13 or 14**; 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

private activity means activity that, in the circumstances, any 1 or more of the participants in it ought reasonably to expect is 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 under 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 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 90**

search includes a remote access search

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

serious crime means,—

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

(b) in relation to any other country, any 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 55**

Type 2 intelligence warrant means an intelligence warrant issued under **section 56**

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 unlawful activity

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

(a) an intelligence warrant; or

(b) an authorisation given under **section 77**; or

(c) a removal warrant.

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

Subpart 1—Intelligence warrants

Types of intelligence warrants

50 Types of intelligence warrant

There are 2 types of intelligence warrants as follows:

(a) Type 1 intelligence warrants:

(b) Type 2 intelligence warrants.

51 Type 1 intelligence warrant

A Type 1 intelligence warrant authorises an intelligence and security agency to carry out an otherwise unlawful activity for any authorised purpose in respect of any person who is—

(a) a New Zealand citizen; or

(b) a permanent resident of New Zealand.

52 Type 2 intelligence warrant

A Type 2 intelligence warrant authorises an intelligence and security agency to carry out an otherwise unlawful activity for any authorised purpose other than in respect of a person described in **section 51**.

Application and issue of intelligence warrants

53 Application for intelligence warrant

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

(2) An application for a Type 1 intelligence warrant must be made to the Attorney-General and the Chief Commissioner of Intelligence Warrants.

(3) An application for a Type 2 intelligence warrant must be made to the Attorney-General.

54 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.

55 Issue of Type 1 intelligence warrant

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

- (a) the Attorney-General; and
- (b) a Commissioner of Intelligence Warrants.

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

- (a) that,—
  - (i) in carrying out the otherwise unlawful activity, the intelligence and security agency will contribute to the objective specified in **section 11(a)**; and
  - (ii) the additional criteria in **section 57** are met; or
- (b) that,—
  - (i) in carrying out the otherwise unlawful activity, the intelligence and security agency will contribute to the objective specified in **section 11(b) or (c)**; and
  - (ii) there is a reasonable suspicion that a person referred to in **section 51(a)** in respect of whom the otherwise unlawful 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; and

(iii) the additional criteria in **section 57** are met; or

(c) that,—

(i) in carrying out the otherwise unlawful activity, the intelligence and security agency will contribute to the objective specified in **section 11(b) or (c)**; and

(ii) there is a reasonable suspicion that a class of persons referred to in **section 51(a)** in respect of whom the otherwise unlawful 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

(iii) the additional criteria in **section 57** are met.

56 Issue of Type 2 intelligence warrant

(1) A Type 2 intelligence warrant is issued by the Attorney-General.

(2) A Type 2 intelligence warrant may be issued to the Director-General of an intelligence and security agency only if the Attorney-General is satisfied that,—

(a) in carrying out the otherwise unlawful activity, the intelligence and security agency will contribute to 1 or more of the objectives specified in **section 11**; and

(b) the additional criteria in **section 57** are met.

57 Additional criteria for issue of intelligence warrant

The additional criteria for the issue of an intelligence warrant referred to in **sections 55(2)** and **56(2)(b)** are that—

(a) the carrying out of the otherwise unlawful activity is necessary for one of the following purposes:

(i) to perform any function of the intelligence and security agency; or

(ii) to test, maintain, or develop the capabilities of the intelligence and security agency; or

(iii) to train employees to perform any function of the intelligence and security agency; 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 nothing will be done in reliance on the warrant beyond what is necessary and reasonable for the proper performance of a function of the intelligence and security agency; and

(e) there are satisfactory arrangements in place to ensure that any information collected in reliance on the 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)

58 Minister of Foreign Affairs to be consulted in certain cases

(1) The Attorney-General must consult the Minister of Foreign Affairs before a 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.

(2) For the purposes of **subsection (1)**, **warrant** means—

(a) a Type 1 intelligence warrant issued under **section 55 or 69**; and

(b) a Type 2 intelligence warrant issued under **section 56 or 70**; and

(c) a removal warrant issued under **section 90**.

59 Issue of joint intelligence warrant

(1) A joint Type 1 intelligence warrant may be issued under **section 55** if the Attorney-General 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 56** if the Attorney-General 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 the 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).

60 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 Attorney-General and a Commissioner of Intelligence Warrants, in the case of a Type 1 intelligence warrant:

(b) the Attorney-General, 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)

61 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 54**, 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 11** 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 conditions or restrictions imposed under **section 61**:

(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

62 Term of intelligence warrant

(1) An intelligence warrant must specify a period not exceeding 12 months for 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

Authorised activities and powers

63 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 another jurisdiction to undertake an activity that, if undertaken 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 undertaken 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 New Zealand Government (including identifying and responding to threats or potential threats to those communications or infrastructures) without the consent of any person.

64 Authorised activities under purpose-based warrant

(1) An intelligence warrant may authorise the carrying out of 1 or more of the following activities for a purpose specified in the warrant and for reasons specified in the warrant:

(a) conducting surveillance:

(b) intercepting any 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) undertaking the activities specified in **section 63(1)(e) to (g)**.

(2) An intelligence warrant may authorise the carrying out of activities for a specified purpose and for reasons specified in the warrant without describing the persons in respect of whom, or the places at which, the activities will be undertaken only,—

(a) in the case of a Type 1 intelligence warrant, if the Attorney-General and the Commissioner of Intelligence Warrants are satisfied that the objectives of the warrant cannot be accomplished by the provisions of **section 63** (whether because of difficulties in identifying the persons or places concerned or otherwise):

(b) in the case of a Type 2 intelligence warrant, if the Attorney-General is satisfied that the objectives of the warrant cannot be accomplished by the provisions of **section 63** (whether because of difficulties in identifying the persons or places concerned or otherwise).

(3) However, if an intelligence warrant is to be, or may be, used in respect of 1 or more persons specified in **subsection (4)** and it is proposed to install a surveillance device (including a visual surveillance device) or access an information infrastructure, the warrant must specify the kinds of persons or places or information infrastructure in respect of which those activities may be carried out.

(4) The persons referred to in **subsection (3)** are—

(a) New Zealand citizens:

(b) permanent residents of New Zealand.

65 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, or is likely to be, 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 and use in or on a place, vehicle, or other thing searched any equipment:

(g) use any equipment found 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 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 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 imposed on the warrant under **section 60**.

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

66 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 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 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 imposed on the warrant under **section 60**.

(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.

67 Privileged communications

(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 of—

(a) a New Zealand citizen; or

(b) a permanent resident of New Zealand.

(2) In **subsection (1)**, **privileged communications** means communications that are protected by legal professional privilege or privileged in proceedings under section 54, 56, 58, or 59 of the Evidence Act 2006.

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

Requests for assistance

68 Request for assistance to give effect to intelligence warrant

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

(a) the New Zealand Police; or

(b) any person; or

(c) any other organisation.

(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 88**).

(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

Urgent intelligence warrants

69 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 Attorney-General 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 a Type 1 intelligence warrant; or

(b) the Attorney-General 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 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 Attorney-General and a Commissioner of Intelligence Warrants, but—

(a) the Attorney-General 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 72** is determined, revoke the warrant.

70 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 Attorney-General 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 a Type 2 intelligence warrant.

71 Reasons for urgent issue of intelligence warrant to be recorded

The reasons for the urgent issue of an intelligence warrant under **section 69 or 70** must be recorded as soon as practicable by—

(a) the Attorney-General; or

(b) the Attorney-General and the Commissioner of Intelligence Warrants, in the case of a warrant issued under **section 69(2)(a)(ii)**.

72 Intelligence warrant issued under section 69 revoked unless confirmed

(1) An intelligence warrant issued under **section 69** 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 53** for the issue of a Type 1 intelligence warrant.

(2) On an application made under **section 53**, the Attorney-General 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 that section on the date the urgent intelligence warrant was issued; or

(b) revoke the intelligence warrant issued under **section 69**.

73 An intelligence warrant issued under section 70 revoked unless confirmed

(1) An intelligence warrant issued under **section 70** 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 53** for the issue of a Type 2 intelligence warrant.

(2) On an application made under **section 53**, the Attorney-General may—

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

(b) revoke the intelligence warrant issued under **section 70**.

74 Information to be destroyed if intelligence warrant issued under section 69 or 70 revoked

(1) If an intelligence warrant issued under **section 69** is revoked under **section 72(1)**, all information collected under that warrant must be destroyed as soon as practicable.

(2) If an intelligence warrant issued under **section 70** is revoked under **section 73(1)**, all information collected under that warrant must be destroyed as soon as practicable .

(3) **Subsections (1) and (2)** do not apply to any incidentally-obtained intelligence that may be retained under **section 91**.

75 Intelligence warrants issued under section 69 or 70 to be referred to Inspector-General

An intelligence warrant issued under **section 69 or 70** must be referred as soon as practicable after issue to the Inspector-General for review.

Amendment and revocation of intelligence warrants

76 Amendment and revocation of intelligence warrants

(1) The Attorney-General and a Commissioner of Intelligence Warrants may at any time amend or revoke a Type 1 intelligence warrant.

(2) The Attorney-General may at any time amend or revoke a Type 2 intelligence warrant.

Authorisations by Director-General of intelligence and security agency

77 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.

78 Authorisation given under section 77(2)(a) effective as Type 1 intelligence warrant

(1) An authorisation given under **section 77(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 Attorney-General; and

(ii) the Chief Commissioner of Intelligence Warrants; and

(b) within 24 hours after giving the authorisation, make an application under **section 53** for the issue of a Type 1 intelligence warrant.

(2) An authorisation given under **section 77(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 53** is made.

(3) The Attorney-General or the Chief Commissioner of Intelligence Warrants may, at any time before an application made under **section 53** is determined, revoke an authorisation given under **section 77(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.

79 Authorisation given under section 77(2)(b) effective as Type 2 intelligence warrant

(1) An authorisation given under **section 77(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 Attorney-General; and

(b) within 24 hours after giving the authorisation, make an application under **section 53** for the issue of a Type 2 intelligence warrant.

(2) An authorisation given under **section 77(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 53** is made.

(3) The Attorney-General may, at any time before an application made under **section 53** is determined, revoke an authorisation given under **section 77(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.

80 Information to be destroyed if authorisation given under section 77 revoked

(1) If an authorisation given under **section 77(2)(a) or (b)** is revoked, all information collected under that authorisation must be destroyed as soon as practicable.

(2) **Subsection (1)** does not apply to any incidentally-obtained intelligence that may be retained under **section 91**.

81 Authorisations given under section 77 to be referred to Inspector-General

An authorisation given under **section 77** must be referred as soon as practicable after it is given to the Inspector-General for review.

Collection of intelligence

82 Duty to collect intelligence only within scope of authorised activity

In carrying out an authorised activity, and in exercising any power for the purpose of carrying out that activity, a Director-General of an intelligence and security agency must take all practicable steps that are reasonable in the circumstances to minimise the likelihood of collecting intelligence outside the scope of the authorised activity.

83 Collection of unauthorised intelligence

(1) If, in carrying out an authorised activity, intelligence is unintentionally collected outside the scope of the authorised activity (**unauthorised intelligence**), that intelligence must be destroyed.

(2) **Subsection (1)** is subject to—

- (a) **subsection (3)**:
- (b) **section 91**.

(3) If the unauthorised intelligence —

- (a) is collected in the carrying out of an activity authorised under a Type 2 intelligence warrant, or during the provision of cooperation, advice, and assistance under **section 17**, and the collection of that intelligence is of a kind that could be authorised under a Type 1 intelligence warrant,—
  - (i) an application for a Type 1 intelligence warrant under **section 53** authorising the collection of the unauthorised intelligence may be made as soon as practicable; and
  - (ii) the unauthorised intelligence need not be destroyed if a Type 1 intelligence warrant is issued authorising its collection; or
- (b) is collected during the provision of cooperation, advice, and assistance under **section 17**, and the collection of that intelligence is of a kind that could be authorised under a Type 2 intelligence warrant,—
  - (i) an application for a Type 2 intelligence warrant under **section 53** authorising the collection of the unauthorised intelligence may be made as soon as practicable; and
  - (ii) the unauthorised intelligence need not be destroyed if a Type 2 intelligence warrant is issued authorising its collection.

Offences and immunities

84 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 74**:

(b) **section 80**:

(c) **section 83**.

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

85 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 that the activity is an authorised activity; or

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

(c) disclose 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)

86 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 course of his or her duties.

(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)

87 Immunities from criminal liability in relation to obtaining intelligence warrant

(1) An employee is immune from criminal liability for any act done in good faith to obtain an intelligence warrant if—

(a) the person 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.

88 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 carrying out of the activity was done 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.

Register of intelligence warrants

89 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:

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

(c) any conditions the intelligence warrant is subject to:

(d) the term for which the intelligence warrant is valid:

(e) the date 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 for an intelligence warrant made by him or her; 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 58**; and

(c) the original of every intelligence warrant issued to him or her.

(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 Attorney-General:

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

(d) the Inspector-General.

Compare: 2003 No 9 s 19

Subpart 2—Removal warrants

90 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 (the **original intelligence warrant**) remains in a place or thing after the original intelligence warrant has ceased to be in force.

(2) The Attorney-General may, on the written application of the Director-General of the intelligence and security agency to whom the original intelligence warrant was issued, issue a removal warrant authorising the removal of the device or equipment from the place or thing.

(3) A person acting under a removal warrant may enter the place or thing concerned or take possession of the thing concerned for the purpose of removing the device or equipment and may—

(a) search the place or thing entered; and

(b) exercise any of the powers specified in **section 65(1)(d), (f) to (h), (j), and (k)**.

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

Compare: 1969 No 24 s 4I

Subpart 3—Incidentally-obtained intelligence

91 Retention of incidentally-obtained intelligence

(1) The Director-General of an intelligence and security agency may retain any incidentally-obtained intelligence 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 employee of the other intelligence and security agency:

(d) 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 intelligence 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 or avoiding loss of life of any person who is outside the territorial jurisdiction of any country.

Compare: 2003 No 9 s 25

Subpart 4—Commissioners of Intelligence Warrants

92 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)

93 Eligibility for appointment

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

Compare: 1969 No 24 s 5A(3)

94 Functions of Commissioners

The functions of a Commissioner of Intelligence Warrants are—

(a) to advise the Attorney-General on applications under **section 53** for Type 1 intelligence warrants:

(b) to consider with the Attorney-General applications under **section 53** for Type 1 intelligence warrants:

(c) to deliberate with the Attorney-General on applications under **section 53** for Type 1 intelligence warrants:

(d) to issue Type 1 intelligence warrants under **section 55** jointly with the Attorney-General:

(e) to consider with the Attorney-General applications under **section 112** seeking permission to access restricted information:

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

(g) 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:

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

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

95 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 69(3)(a)** of the issue of a Type 1 intelligence warrant by the Attorney-General and consider whether to revoke it:

(e) to receive notice under **section 78(1)(a)** of an authorisation given under **section 77(2)(a)** and consider whether to revoke it:

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

96 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

97 Interpretation

In this Part, unless the context otherwise requires,—

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)

agency—

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

(b) includes a department

citizenship information means information that relates to the acquisition or loss of citizenship by, or to the citizenship status of, any person

database means the information recording system or facility used by a holder agency to store information

holder agency means an agency specified in the first 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.

98 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

99 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.

100 Requests for information

(1) The Director-General of an intelligence and security agency may request information from any other agency if the Director-General considers that access to the information is required to enable the intelligence and security agency to perform or exercise a function, duty, or power.

(2) A request must—

(a) provide details of the information requested; and

(b) confirm that access to the information is required to enable the intelligence and security agency to perform or exercise a function, duty, or power.

101 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 is satisfied that the information is required by the intelligence and security agency to perform or exercise a function, duty, or power.

(2) An agency may disclose the information either—

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

(b) on its own initiative.

(3) This section is subject to—

(a) a provision contained in any other Act that—

(i) imposes a prohibition or restriction in relation to the disclosure of the information (for example, in relation to personal information, information privacy principle 11 in section 6 of the Privacy Act 1993); or

(ii) regulates the manner in which the information may be obtained or made available (for example, section 236 of the Land Transport Act 1998); 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.

Subpart 2—Direct access to database information

102 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.

103 Direct access to certain information

(1) A holder agency must allow the Director-General of an intelligence and security agency access to any database storing the information held by the holder agency specified in the second column of the table in **Schedule 2** opposite the name of that holder agency.

(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.

104 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 103(2)** must be satisfied that—

(a) direct access to the information is necessary to enable the intelligence and security agency to perform or exercise a function, duty, or power; and

(b) there are adequate safeguards to protect the privacy of individuals, including whether the proposed compliance and audit requirements for the access, use, disclosure, and retention of the information are sufficient; and

(c) the agreement will include appropriate procedures for access, use, disclosure, and retention of the information.

105 Consultation on direct access agreement

Before entering into a direct access agreement, or varying an agreement, the Ministers referred to in **section 103(2)** 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.

106 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 function, duty, or power being, or to be, performed or exercised by the intelligence and security agency for which the information is required:

(d) the mechanism by which the information is to be accessed:

(e) the position held by the person or persons in the intelligence and security agency who may access the information:

(f) the records to be kept in relation to each occasion a database is accessed:

(g) the safeguards that are to be applied for protecting particular information (for example, personal information or commercially sensitive information):

(h) the requirements relating to storage, retention, and disposal of information obtained from the database or databases:

(i) 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:

(j) the appointment of the costs incurred by the holder agency and the intelligence and security agency under the agreement.

107 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 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 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 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 intelligence and security agency.

108 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.

109 Amendment of Schedule 2

(1) The Governor-General may, by Order in Council made on the recommendation of the relevant Minister given after consultation with the Intelligence and Security Committee,—

(a) add, remove, amend, or replace any item in **Schedule 2**; or

(b) repeal **Schedule 2** and substitute a new schedule.

(2) In this section, **relevant Minister** means,—

(a) if only 1 intelligence and security agency is affected, or likely to be affected, by the proposed Order in Council, the Minister responsible for that agency:

(b) if both intelligence and security agencies are affected, or likely to be affected, by the proposed Order in Council, the Minister or Ministers responsible for those agencies.

Subpart 3—Access to restricted information

110 Purpose of subpart

The purpose of this subpart is to enable an intelligence and security agency to access restricted information.

111 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 to students by the Secretary of Education under section 343 of the Education Act 1989:

(c) photographic images used for driver licences that are stored under section 28(5) of the Land Transport Act 1998.

112 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 Attorney-General and 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 Attorney-General, 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.

113 Permission to access restricted information granted on application made under section 112(2)(a)

The Attorney-General and a Commissioner of Intelligence Warrants may grant an application made under **section 112(2)(a)** and permit access to specified restricted information if they are satisfied—

(a) that—

(i) access to the restricted information will contribute to the objective in **section 11(a)**; and

(ii) the further criteria in **section 115** are met; or

(b) that—

(i) access to the restricted information will contribute to the objective in **section 11(b) or (c)**; and

(ii) there is a reasonable suspicion that the person referred to in **section 112(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 115** are met.

114 Permission to access restricted information granted on application made under section 112(2)(b)

The Attorney-General may grant an application made under **section 112(2)(b)** and permit access to specified restricted information if the Attorney-General is satisfied—

(a) that access to the restricted information will contribute to 1 or more of the objectives specified in **section 11**; and

(b) the further criteria in **section 115** are met.

115 Further criteria for permitting access to restricted information

The further criteria for permitting access to restricted information referred to in **sections 113 and 114** are that—

(a) access to the restricted information is necessary for the purpose of enabling the intelligence and security agency to perform any of its functions; 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.

116 Permission must specify restricted information that may be accessed

A permission given under **section 113 or 114** must specify the particular restricted information that the intelligence and security agency may access.

117 Access to restricted information must be provided if permitted

An agency must provide 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 within the control of that agency.

118 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.

Part 6
Oversight of intelligence and security agencies

119 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 are operating 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, and powers to—

(i) ensure that the intelligence and security agencies conduct their activities lawfully and with propriety:

(ii) receive certain types of complaints about the agencies:

(iii) conduct inquiries relating to the agencies:

(iv) advise the 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

120 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 that the Intelligence and Security Committee has been consulted.

(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)

121 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 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 134**:

(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 warrants; and

(ii) compliance systems of each intelligence and security agency for operational activity, 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 unscheduled audits of the procedures and compliance systems described in **paragraph (f)**:

(h) to conduct a review in relation to—

(i) the issue of an authorisation; and

(ii) the carrying out of an activity under an authorisation:

(i) to undertake all work programmes published under **section 122**:

(j) 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** means—

(a) an intelligence warrant issued under **section 55, 56, 69, or 70**:

(b) an authorisation given under **section 77**:

(c) a removal warrant issued under **section 90**.

Compare: 1996 No 47 s 11(1)(a), (c), (ca), (d), (da), (f), (3)

122 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 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)

123 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

124 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 176(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 powers, duties, and responsibilities 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)

125 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)

126 Reviews relating to authorisations

(1) If a review conducted under **section 121(1)(h)** identifies any irregularity in the issue of an authorisation or the carrying out of an activity authorised by the authorisation, that finding does not—

(a) invalidate the authorisation; or

(b) invalidate any action taken by an intelligence and security agency, or any other person, in reliance on the authorisation or any intelligence collected under it; or

(c) require the intelligence collected under the authorisation to be destroyed.

(2) The Inspector-General may report the irregularity to—

(a) the Attorney-General and the Chief Commissioner of Intelligence Warrants, in the case of—

(i) a Type 1 intelligence warrant; or

(ii) an authorisation given under **section 77(2)(a)**; or

(b) the Attorney-General, in the case of—

(i) a Type 2 intelligence warrant; or

(ii) an authorisation given under **section 77(2)(b)**; or

(iii) a removal warrant.

Appointment, functions, duties, and powers of Deputy Inspector-General

127 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 that the Intelligence and Security Committee has been consulted.

(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)

128 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

129 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

130 Advisory panel

There continues to be an advisory panel.

Compare: 1996 No 47 s 15A

131 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 37 s 15B

132 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)

133 Administrative provisions relating to advisory panel

Part 3 of Schedule 3 applies in relation to the membership and procedure of the advisory panel.

Complaints

134 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 that the House has, or may have, been adversely affected by any act, omission, practice, policy, or procedure of an intelligence and security agency.

Compare: 1996 No 47 s 11(1)(b), (ba), (5)

135 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)

136 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 137**, 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

137 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.

(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) having regard to all the circumstances of the case, further inquiries are unnecessary; or

(b) 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

138 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 121(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)

139 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)

140 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)

141 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)

142 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)

143 Disclosure of information may be required despite obligation of secrecy

(1) A person who is bound by the provisions of an enactment 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 the enactment by which that obligation is imposed.

(3) This section is subject to **section 144**.

Compare: 1996 No 47 s 23(5)

144 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)

145 Information disclosed to Inspector-General privileged

(1) 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.

(2) 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.

(3) Nothing in **subsection (2)** applies in respect of proceedings for—

(a) an offence against **section 177**; 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)

146 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

147 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; 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)

148 Advice on compliance with Inspector-General's recommendations

The Inspector-General may advise the Minister who received a report under **section 147(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)

149 Minister to respond to Inspector-General's report

(1) As soon as practicable after receiving a report from the Inspector-General under **section 147(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 security clearance issue.

Compare: 1996 No 47 s 25(6), (7)

150 Publication of Inspector-General's report

(1) As soon as practicable after sending a report in accordance with **section 147(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

151 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)

152 Proceedings not to be questioned or reviewed

No proceeding, report, or finding of the Inspector-General may be challenged, reviewed, quashed, or called in question in any court except on the ground of lack of jurisdiction.

Compare: 1996 No 47 s 19(9)

153 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 147(5)**; or

(b) a report made publicly available by the Inspector-General under **section 150(1)** or **180(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 the broadcasting or reporting of proceedings in Parliament.

(6) In this section, **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

154 Intelligence and Security Committee

There continues to be an Intelligence and Security Committee.

Compare: 1996 No 46 s 5

155 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, a financial 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

156 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 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 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.

(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)

157 Filling vacancy in membership of Committee

(1) If the office of a member nominated under **section 156(2)(c)** becomes vacant, the Leader of the Opposition must nominate, in accordance with **section 156(2)(c)**, another member of the House of Representatives to fill that vacancy.

(2) If the office of a member nominated under **section 156(2)(d)** becomes vacant, the Prime Minister—

(a) must nominate, in accordance with **section 156(2)(d)**, another member of the House of Representatives to fill that vacancy, if the vacancy leaves the Committee with fewer than 6 members; or

(b) may nominate, in accordance with **section 156(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

158 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 156(2)(c) and (d)**; and

(b) **section 157** (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 156(2)(c)**, or the Prime Minister under **section 156(2)(d)**, as the case requires.

Compare: 1996 No 46 s 8(1), (2)

159 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 156(2)(c) and (d)** has been endorsed.

Compare: 1996 No 46 s 8(3)

160 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 156(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)

161 Administrative provisions relating to Committee

Part 4 of Schedule 3 applies in relation to the Committee.

Evidence

162 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

163 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) Information that has not been disclosed to the Committee on the ground specified in **subsection (1)(b)** must be disclosed to the Committee if—

(a) the information is not sensitive information under **section 6(1) and (2)(d)**; and

(b) the Prime Minister considers that disclosure of the information is desirable in the public interest.

(4) If any document or other information having 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

164 Information disclosed to Committee privileged

(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 163(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 182(2)(a) to (c)**; or

(ii) **section 182(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 the exercise of the person's powers under this Act; or

(c) 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 180**); or

(ii) the conduct of the business of the Committee; or

(b) the disclosure is authorised in writing by the Committee or its chairperson.

(4) A person who contravenes this section 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.

(5) The leave of the Attorney-General must be obtained before an offence against this section is prosecuted.

Compare: 1996 No 46 s 19

Part 7
Miscellaneous provisions

Ministerial policy statements

165 Issue of ministerial policy statements relating to covert activities

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) authorising the acquiring, use, and maintenance of an assumed identity under **subpart 1 of Part 3** (for example, the circumstances in which authorising the acquiring and use of an assumed identity is appropriate):

(b) acquiring, using, and maintaining an assumed identity under **subpart 1 of Part 3** (for example, the responsibilities and obligations of persons acting under an assumed identity):

(c) creating and maintaining a legal entity under **subpart 2 of Part 3** (for example, the circumstances in which it is appropriate to create and maintain a legal entity).

166 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)**.

167 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 a ministerial policy statements that provide guidance to the intelligence and security agency in relation to any other matter.

168 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).

169 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)**.

170 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—

(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)**.

171 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 169 and 170** apply with all necessary modifications.

172 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.

173 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.

174 Status of ministerial policy statements

A ministerial policy statement 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.

Security records

175 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

176 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

177 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 194(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

178 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 14** 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

179 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 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 69**; and

(iv) the urgent issue of a Type 2 intelligence warrant under **section 70**; and

(v) a joint Type 1 intelligence warrant under **section 54**; and

(vi) a joint Type 2 intelligence warrant under **section 54**; and

(b) a statement as to the number of applications referred to in each of **subparagraphs (i) to (vi) of paragraph (a)** that were—

(i) approved; and

(ii) declined; and

(c) a statement as to the number of authorisations given by the Director-General under **section 77**; and

(d) a statement as to the number of occasions that the agency has provided assistance under **section 16(1)(b)** to—

(i) the New Zealand Police:

(ii) the New Zealand Defence Force; and

(e) a statement as to the number of occasions that the agency has provided assistance under **section 17**; and

(f) 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 deleted from the report if the Minister considers that the information is likely to—

(a) prejudice the security or defence of New Zealand or international relations of the Government of New Zealand; or

(b) 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) prejudice the entrusting of information to the Government of New Zealand on a basis of confidence by any international organisation; or

(d) endanger the safety of any person; or

(e) 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

180 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 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 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

181 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 182**.

(3) The Intelligence and Security Committee must make all annual reports presented to the House of Representatives publicly available on the Internet site of the New Zealand Parliament.

Compare: 1996 No 46 s 6(1)(e)

182 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 163(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-Gen-

eral, 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

183 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

(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.

(2) In this section, **Inspector-General** includes the Deputy Inspector-General.

Compare: 1996 No 47 s 23(8)

184 Personation

(1) A person commits an offence if the person, without reasonable excuse and in circumstances likely to lead a 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

185 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 or broadcasts, or causes to be published or broadcast, or otherwise distributes or discloses, 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 the broadcasting or 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, **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

186 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) In imposing requirements under **subsection (1)(b)**, the Director-General must have regard to any relevant ministerial policy statement.

(4) 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.

187 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 186**.

(2) Nothing done (or omitted to be done) under **section 186**—

(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

188 Exception from criminal liability under section 246 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 of a certain kind (whether or not on a continuing basis) and that activity could have been authorised by an intelligence warrant.

(3) An intelligence and security agency that obtains information in circumstances where this section 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 13 or 14**, may disseminate that report to another agency.

189 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.

190 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 33, 34, 44, 45, 68(4), 87, 88, and 187** 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

191 Functions of Chief Executive of DPMC in relation to intelligence and assessments

(1) The Chief Executive of DPMC has the following functions:

(a) to provide 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 DPMC considers appropriate; and

(b) to advise Ministers on the setting of priorities for intelligence collection and analysis; and

(c) to advise departments on best practice in relation to the assessment of intelligence.

(2) In this section and in **section 192**, **DPMC** means the Department of the Prime Minister and Cabinet.

192 Duty to act independently

In matters relating to functions specified in **section 191**, the Chief Executive of DPMC must act independently.

Periodic reviews

193 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 194(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

194 Appointment of reviewers and related matters

(1) A review under **section 193** must be conducted by 2 persons (**reviewers**) appointed by the Prime Minister.

(2) The reviewers appointed under **subsection (1)** must have an appropriate security clearance.

(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 that 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

195 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

196 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 182** applies, with all necessary modifications, as if the report had been prepared by the Intelligence and Security Committee.

Compare: 1996 No 46 s 24

197 Remuneration of reviewers

(1) A reviewer is entitled—

(a) to receive remuneration not provided for within **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

198 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 have an appropriate security clearance.

Compare: 1996 No 46 s 26

199 Reviewers to determine own procedure

The reviewers may determine their own procedure subject to any matters specified under **section 194(3)(b)**.

Compare: 1996 No 46 s 27

Part 8
Repeals and amendments

Repeals

200 Repeals

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) Inspector-General of Intelligence and Security Act 1996 (1996 No 47):

(d) Government Communications Security Bureau Act 2003 (2003 No 9).

Amendments to Births, Deaths, Marriages, and Relationships Registration Act 1995

201 Amendments to Births, Deaths, Marriages, and Relationships Registration Act 1995

Sections 202 to 205 amend the Births, Deaths, Marriages, and Relationships Registration Act 1995.

202 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 New Zealand Intelligence and Security Act 2016**

intelligence and security agency has the meaning given to it by **section 4 of the New Zealand Intelligence and Security Act 2016**

203 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 of the matters set out in **section 29(1) of the New Zealand Intelligence and Security Act 2016** (which applies with any necessary modifications).

(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 25 of the New Zealand Intelligence and Security Act 2016**

204 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 exercise of its functions:

205 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 Crimes Act 1961

206 Amendments to Crimes Act 1961

Sections 207 and 208 amend the Crimes Act 1961.

207 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 New Zealand 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 New Zealand 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.

208 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)".

Amendment to Education Act 1989

209 Amendment to Education Act 1989

Section 210 amends the Education Act 1989.

210 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 117 of the New Zealand Intelligence and Security Act 2016** (to the extent that a permission granted under **section 113 or 114** 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

211 Amendment to Electronic Identity Verification Act 2012

Sections 212 amends the Electronic Identity Verification Act 2012.

212 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 25 of the New Zealand Intelligence and Security Act 2016**

intelligence and security agency has the meaning given to it by **section 4 of the New Zealand Intelligence and Security Act 2016**

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

213 Amendment to Employment Relations Act 2000

Section 214 amends the Employment Relations Act 2000.

214 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 14 of the New Zealand Intelligence and Security Act 2016** 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 147** 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 4 of the New Zealand Intelligence and Security Act 2016**

New Zealand Security Intelligence Service means the New Zealand Security Intelligence Service continued by **section 9 of the New Zealand Intelligence and Security Act 2016**.

Amendments to Immigration Act 2009

215 Amendments to Immigration Act 2009

Sections 216 to 229 amend the Immigration Act 2009.

216 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

217 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 a manner where each flight or voyage is open to use by members of the public.

218 Section 9A amended (Meaning of mass arrival group)

In section 9A(2), delete "(within the meaning of section 96(4))".

219 Section 29 amended (Automated decision making in advance passenger processing)

In section 29, after "section 97(1)", insert "or **97A(1)**".

220 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)**.

221 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)**.

222 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)**.

223 Section 101 amended (Obligations in relation to craft en route to or arriving in New Zealand)

Repeal section 101(5).

224 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.

225 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).

226 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 a crime against 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 those 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 when 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 in **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 it, 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.

227 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

228 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

229 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

230 Amendments to Land Transport Act 1998

Sections 231 and 232 amend the Land Transport Act 1998.

231 Section 24A replaced (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 New Zealand Intelligence and Security Act 2016**

employee, in relation to an intelligence and security agency, has the meaning given to it by **section 25 of the New Zealand Intelligence and Security Act 2016**

intelligence and security agency has the meaning given to it by **section 4 of the New Zealand Intelligence and Security Act 2016**

232 Section 200 amended (Restrictions on access to photographic images of driver licence holders)

Replace subsection (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 117 of the New Zealand Intelligence and Security Act 2016**.

Amendments to Passports Act 1992

233 Amendments to Passports Act 1992

Sections 234 to 260 amend the Passports Act 1992.

234 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 92 of the New Zealand Intelligence and Security Act 2016**

Commissioner of Intelligence Warrants means a Commissioner of Intelligence Warrants appointed under **section 92 of the New Zealand Intelligence and Security Act 2016**

235 Section 4 amended (Issue of passport)

In section 4(1), replace "4A" with "**27GA**".

236 Section 4A repealed (Refusal to issue passport on grounds of national security)

Repeal section 4A.

237 Section 8A repealed (Cancellation of passport on grounds of national security)

Repeal section 8A.

238 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)".

239 Section 11 amended (Delivery of recalled passport)

In section 11(1), after "sections 8 to 10", insert "or **section 27GA**".

240 Section 11A amended (Warnings on New Zealand travel document database)

In section 11A(a), replace "and 27F" with "27F, and **27GA**".

241 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.

242 Section 20A repealed (Cancellation of certificate of identity on grounds of national security)

Repeal section 20A.

243 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**".

244 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

245 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.

246 Section 25A repealed (Cancellation of emergency travel document on grounds of national security)

Repeal section 25A.

247 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**".

248 Section 27A amended (Issue of refugee travel document)

In section 27A(1), replace "section 27B" with "**section 27GA**".

249 Section 27B repealed (Refusal to issue refugee travel document on grounds of national security)

Repeal section 27B.

250 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.

251 Section 27E repealed (Cancellation of refugee travel document on grounds of national security)

Repeal section 27E.

252 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**".

253 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.

254 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)**.

255 Section 28 amended (Appeal to High Court)

In section 28(5A), replace "on grounds of national security" with "under **section 27GA**".

256 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 for which a person is not entitled to obtain a New Zealand travel document.

257 Cross-heading above section 29AA replaced

Replace the cross-heading above section 29AA with:

Special provision for proceedings where national or international security involved

258 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.

259 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)

260 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)

261 Section 46 repealed (Transitional provision)

Repeal section 46.

Amendments to Privacy Act 1993

262 Amendments to Privacy Act 1993

Sections 263 and 264 amend the Privacy Act 1993.

263 Section 6 amended (Information privacy principles)

(1) In section 6, principle 10, after paragraph (d), insert:

(da) that the use of the information for that other purpose is necessary to enable an intelligence organisation to perform any of its statutory functions; or

(2) In section 6, principle 11, after paragraph (f), insert:

(fa) that the disclosure of the information is necessary to enable an intelligence organisation to perform any of its statutory functions; or

264 Section 57 replaced (Intelligence organisations)

Replace section 57 with:

57 Exemption for intelligence organisations

Information privacy principles 2, 3, and 4(b) do not apply to information collected by an intelligence organisation.

Amendments to Protected Disclosures Act 2000

265 Amendments to Protected Disclosures Act 2000

Sections 266 and 267 amend the Protected Disclosures Act 2000.

266 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

267 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

268 Amendments to Public Finance Act 1989

Sections 269 to 271 amend the Public Finance Act 1989.

269 Section 2 amended (Interpretation)

In section 2(1), definition of **department**, repeal paragraph (a)(iv).

270 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".

271 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 179 of the New Zealand Intelligence and Security Act 2016** is substituted for sections 43 and 44.

Amendments to Search and Surveillance Act 2012

272 Amendments to Search and Surveillance Act 2012

Sections 273 and 274 amend the Search and Surveillance Act 2012.

273 Subpart 8 heading in Part 2 amended

In Part 2, in the subpart 8 heading, after "78" insert "or **78AA**".

274 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

275 Amendments to State Sector Act 1988

Sections 276 and 277 amend the State Sector Act 1988.

276 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.

277 Schedule 1 amended

In Schedule 1, insert in its appropriate alphabetical order:

New Zealand Security Intelligence Service

Amendment to Tax Administration Act 1994

278 Amendment to Tax Administration Act 1994

Section 279 amends the Tax Administration Act 1994.

279 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 New Zealand Intelligence and Security Act 2016**), 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 113 or 114 of the New Zealand Intelligence and Security Act 2016**:

Consequential amendments

280 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 7

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 **subsection (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 **subsection (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 **subsection (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 **subsection (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 **subsection (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 **subsection (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 120 of the New Zealand Intelligence and Security Act 2016**.

(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 127 of the New Zealand Intelligence and Security Act 2016**.

(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 132 of the New Zealand Intelligence and Security Act 2016**.

(4) A person continues to hold office under any of **subsections (1) to (3)** on the same terms and conditions that applied to that office immediately before the commencement date.

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 section,—

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 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 147(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 came into force.

Schedule 2
Databases accessible to intelligence and security agencies

s 103, 109

Holder agency	Information
Registrar-General	Adoption information Birth information Civil union information Death information Marriage information Name change information
Secretary for Internal Affairs	Citizenship information
Ministry of Business, Innovation, and Employment	Information collected under the Immigration Act 2009
New Zealand Customs Service	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

Note

In this schedule, **adoption information**, **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.

Schedule 3
Administrative provisions

ss 96, 129, 133, 161

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 Acting Chief Commissioner of Intelligence Warrants

If at any time the Chief Commissioner of Intelligence Warrants is unable for any reason (including illness) to perform the duties of that office, he or she may, by notice in writing, appoint another Commissioner of Intelligence Warrants to act in his or her place.

4 Remuneration and expenses

(1) A Commissioner is entitled—

(a) to receive remuneration not provided for within **paragraph (b)** for services as a Commissioner 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 Commissioner.

(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: 1969 No 24 s 5E

5 Protection of Commissioners

A Commissioner has all the immunities of a Judge of the High Court.

Compare: 1969 No 24 s 5D

6 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

7 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:

(c) the Prime Minister informs the person by written notice that the person is not to be reappointed and not to continue to hold office until a 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 (5)** must state the date on which the resignation takes effect.

Compare: 1996 No 47 s 6

8 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 120(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 127(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

9 Removal from office

The Inspector-General or Deputy Inspector-General may be removed 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.

Compare: 1996 No 47 s 7

10 Remuneration and expenses

(1) The Inspector-General and Deputy Inspector-General must be paid, out of public money and without further authority 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

11 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: 1997 No 47 s 9

12 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

13 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 177**; 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

14 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)

15 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)

16 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

17 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

18 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 156(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 156(2)(d)**.

Compare: 1996 No 46 s 9

19 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 18**:

(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

20 Convenor

Meetings of the Committee must be convened by the Prime Minister.

Compare: 1996 No 46 s 13(1)

21 Chairperson presides

The chairperson of the Committee must preside at all meetings of the Committee.

Compare: 1996 No 46 s 13(2)

22 Quorum

The chairperson and 3 other members must be present at a meeting of the Committee.

Compare: 1996 No 46 s 13(3)

23 Conduct of proceedings

(1) The proceedings of the Committee must, subject to this Act, be conducted in accordance with the Standing Orders of the House of Representatives.

(2) The Committee must meet in private, unless—

(a) the Committee is performing its function under **section 155(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

24 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) If the only members present at a meeting are the chairperson and 3 other members, 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)

25 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 160(3)**.

Compare: 1996 No 46 ss 7A(4), 13(6), (6A)

26 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 13(7), (8)

Administrative provisions

27 Privilege

(1) The proceedings of the Committee are to be treated as proceedings in Parliament for the purposes of Article 9 of the Bill of Rights 1688 and the Parliamentary Privilege Act 2014.

(2) Anything said or 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 in the same manner as if the inquiry or proceedings were proceedings in Parliament (as defined in section 10 of the Parliamentary Privilege Act 2014).

Compare: 1996 No 46 s 16

28 Committee members and others protected

(1) This clause applies to every member of the Committee and to any person appointed under **clause 26(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 177**.

Compare: 1996 No 46 s 15

Schedule 4
Consequential amendments

s 280

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 investigation of matters relating to New Zealand's national security under **Parts 1 to 7 of the New Zealand Intelligence and Security Act 2016**:

In section 5, insert in its appropriate alphabetical order:

national security has the meaning given to it by **section 5 of the New Zealand Intelligence and Security Act 2016**

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 New Zealand Intelligence and Security Act 2016**:

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 14 of the New Zealand Intelligence and Security Act 2016**".

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 121(1)(e) and 134 of the New Zealand Intelligence and Security Act 2016**".

Replace section 77G(5) with:

Civil Aviation Act 1990 (1990 No 98)—*continued*

(5) In this section,—

Inspector-General of Intelligence and Security means the person holding office under **section 120 of the New Zealand Intelligence and Security Act 2016**

New Zealand person means any person, who is—

(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 investigation of matters relating to New Zealand's national security under **Parts 1 to 7 of the New Zealand Intelligence and Security Act 2016**:

In section 366(1B), insert in its appropriate alphabetical order:

national security has the meaning given to it by **section 5 of the New Zealand Intelligence and Security Act 2016**

Corrections Act 2004 (2004 No 50)

In section 3(1), definition of **official agency**, after paragraph (d), insert:

(da) the Inspector-General of Intelligence and Security; or

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) **Parts 1 to 7 of the New Zealand Intelligence and Security Act 2016**; 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:

Criminal Records (Clean Slate) Act 2004 (2004 No 36)—*continued*

(iii) the exercise of the protective security advice and assistance function of the New Zealand Security Intelligence Service under **section 14 of the New Zealand Intelligence and Security Act 2016**; or

Customs and Excise Act 1996 (1996 No 27)

In section 280M(1), delete "the New Zealand Security Intelligence Service and".

Repeal section 280M(2)(a) and (b).

Replace section 280M(3) with:

(3) Before allowing access to a database in accordance with subsection (2), the chief executive must enter into a written agreement with the Commissioner of Police.

In section 280M(5), delete "Director of Security and the".

In section 280M(6), repeal the definition of "Director of Security".

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).

Health and Safety at Work Act 2015 (2015 No 70)—*continued*

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 120 of the New Zealand Intelligence and Security Act 2016**".

In section 8(9), definition of **Inspector-General**, paragraph (b), replace "section 5 of the Act" with "**section 120 of the New Zealand Intelligence and Security Act 2016**".

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 9 of the New Zealand Intelligence and Security Act 2016**.

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 **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 (No 2008 No 1)

In section 79(1B), definition of **law enforcement purposes**, replace paragraph (g) with:

(g) the investigation of matters relating to New Zealand's national security under **Parts 1 to 7 of New Zealand Intelligence and Security Act 2016**:

In section 79(1B), insert in its appropriate alphabetical order:

national security has the meaning given to it by **section 5 of the New Zealand Intelligence and Security Act 2016**

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 120 of the New Zealand Intelligence and Security Act 2016**".

In section 17C(3), replace "the Inspector-General of Intelligence and Security Act 1996" with "**Parts 1 to 7 of the New Zealand Intelligence and Security Act 2016**".

In section 21C, replace "section 5 of the Inspector-General of Intelligence and Security Act 1996" with "**section 120 of the New Zealand Intelligence and Security Act 2016**".

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 "**Parts 1 to 7 of the New Zealand Intelligence and Security Act 2016**".

Privacy Act 1993 (1993 No 28)—*continued*

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 New Zealand Intelligence and Security Act 2016**

In section 14, replace "the Inspector-General of Intelligence and Security Act 1996" with "**Parts 1 to 7 of the New Zealand Intelligence and Security Act 2016**".

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 154 of the New Zealand Intelligence and Security Act 2016**".

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 13 of the New Zealand Intelligence and Security Act 2016**; or

Replace section 133A(2)(e)(ii) and (iia) with:

> (ii) **Parts 1 to 7 of the New Zealand Intelligence and Security Act 2016**; 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.

Remuneration Authority Act 1977 (1977 No 110)—*continued*

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 the authority of an intelligence warrant issued under **Parts 1 to 7 of the New Zealand Intelligence and Security Act 2016**:

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 New Zealand Intelligence and Security Act 2016**

In section 3(1), definition of **Minister responsible for the Government Communications Security Bureau**, replace "for the department of State established under the 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 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**".

Telecommunications (Interception Capability and Security) Act 2013 (2013 No 91)—*continued*

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 New Zealand Intelligence and Security Act 2016**

Commissioner means a Commissioner of Intelligence Warrants within the meaning of **section 4 of the New Zealand Intelligence and Security Act 2016**.

Terrorism Suppression Act 2002 (2002 No 34)

In section 4(1), definition of **intelligence and security agency**, paragraph (b), delete "; or".

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 13 or 14 of the New Zealand Intelligence and Security Act 2016**:

After regulation 15(2), insert:

(3) In this section, **intelligence and security agency** has the meaning given to it by **section 4 of the New Zealand Intelligence and Security Act 2016**.

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 given to the Authority by the Director-General of the New Zealand Security Intelligence Service under **section 14 or 91 of the New Zealand Intelligence and Security Act 2016**; or

Wellington, New Zealand:
Published under the authority of the New Zealand Government—2016