

**Reprint
as at 28 September 2017**



Government Communications Security Bureau Act 2003

Public Act 2003 No 9
Date of assent 1 April 2003
Commencement see section 2

Government Communications Security Bureau Act 2003: repealed, on 28 September 2017, by section 242(3)(c) of the Intelligence and Security Act 2017 (2017 No 10).

Contents

	Page
1 Title	3
Part 1	
Preliminary provisions	
2 Commencement	4
3 Purpose	4
4 Interpretation	4
5 Act binds the Crown	7
5A Transitional provisions relating to amendments to Act	7
Part 2	
Organisation, objectives, and functions of Bureau	
6 Bureau continued and established as department	7
7 Objective of Bureau	7
8 Functions of Bureau	7
8A Information assurance and cybersecurity	8
8B Intelligence gathering and analysis	8
8C Co-operation with other entities to facilitate their functions	9

Note

Changes authorised by subpart 2 of Part 2 of the Legislation Act 2012 have been made in this official reprint.
Note 4 at the end of this reprint provides a list of the amendments incorporated.

This Act is administered by the Government Communications Security Bureau.

8D	Principles underpinning performance of Bureau's functions	9
8E	Director has full powers for purpose of performing Bureau's functions	10
9	Appointment of Director	10
9A	Appointment process	10
9B	Remuneration and conditions of appointment of Director	10
9C	Removal from office	11
9D	Review of performance of Director	11
10	Acting Director	11
11	Prohibition on unauthorised disclosure of information	12
12	Annual report	12

Part 3

Intercepting communications and accessing information infrastructures

Purpose of Part

13	Purpose of Part	14
----	-----------------	----

Restrictions imposed on interceptions

14	Interceptions not to target New Zealand citizens or permanent residents for intelligence-gathering purposes	14
15	Interceptions for which warrant or authorisation required	14

Authorisations to intercept communications or access information infrastructures

15A	Authorisation to intercept communications or access information infrastructures	15
15B	Involvement of Commissioner of Security Warrants	16
15C	Privileged communications	16
15D	Information that interception warrant or access authorisation must contain	17
15E	Warrant or authorisation may authorise persons to assist person giving effect to warrant or authorisation	17
15F	Expiry of warrant or authorisation not to prevent further application	18
16	Certain interceptions permitted without interception warrant or access authorisation	18

Interception warrants

[Repealed]

17	Issue of interception warrant <i>[Repealed]</i>	19
18	Persons acting under warrant <i>[Repealed]</i>	19

Register of interception warrants and access authorisations

19	Register of interception warrants and access authorisations	19
----	---	----

	<i>Urgent issue of warrants and authorisations</i>	
19A	Urgent issue of warrants and authorisations	20
	<i>Provisions applicable to warrants, authorisations, and powers under section 16</i>	
20	Director's functions in relation to warrants and authorisations not to be delegated	20
21	Immunity from civil and criminal liability	21
22	Term of warrant or authorisation [<i>Repealed</i>]	21
23	Destruction of irrelevant records obtained by interception	21
24	Duty to minimise impact of interception on third parties	22
25	When incidentally obtained intelligence may be retained and communicated to other persons	22
	<i>Protection and disclosure of personal information</i>	
25A	Formulation of policy on personal information	23
25B	Principles to protect personal information	23
	Part 3A	
	Transitional provisions relating to amendments to Act	
25C	Transitional provisions relating to amendments to Act	24
	Part 4	
	Provisions relating to other enactments	
26	Amendment to Crimes Act 1961	24
27	Amendment to Higher Salaries Commission Act 1977	24
28	Amendment to Inspector-General of Intelligence and Security Act 1996	24
29	Amendment to New Zealand Security Intelligence Service Act 1969	24
30	Amendment to Official Information Act 1982	25
31	Amendment to Public Finance Act 1989	25
32	Amendment to Radiocommunications Act 1989	25
33	Amendments to State Sector Act 1988	25
34	Certain provisions of State Sector Act 1988 not to apply	25
35	Revocation	25
	Schedule	25
	Transitional provisions relating to amendments made to Act after 1 January 2013	

1 Title

This Act is the Government Communications Security Bureau Act 2003.

Part 1

Preliminary provisions

2 Commencement

This Act comes into force on the day after the date on which it receives the Royal assent.

3 Purpose

The purpose of this Act is to—

- (a) continue the Government Communications Security Bureau and establish it as a department of State;
- (b) specify the objective and functions of the Bureau;
- (c) specify the circumstances in which the Bureau requires an interception warrant or access authorisation to intercept communications;
- (d) specify the conditions that are necessary for the issue of an interception warrant or access authorisation and the matters that may be authorised by a warrant or an authorisation;
- (e) specify the circumstances in which the Bureau may use interception devices to intercept communications without a warrant or an authorisation.

Section 3(c): replaced, on 26 September 2013, by section 4 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 3(d): replaced, on 26 September 2013, by section 4 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 3(e): replaced, on 26 September 2013, by section 4 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

4 Interpretation

In this Act, unless the context otherwise requires,—

access, in relation to any information infrastructure, means instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of, the information infrastructure

access authorisation means an authorisation issued under section 15A(1)(b)

Bureau means the Government Communications Security Bureau continued by section 6

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

Director means the chief executive of the Bureau; and includes a person who, under section 10, exercises or performs the functions, duties, or powers of the Director

foreign organisation means—

- (a) a Government of any country other than New Zealand:
- (b) an entity controlled by the Government of any country other than New Zealand:
- (c) a company or 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 company or body corporate incorporated outside New Zealand:
- (d) an unincorporated body of persons consisting principally of foreign organisations or foreign persons that carry on activities wholly outside New Zealand:
- (e) an international organisation:
- (f) a person acting in his or her capacity as an agent or a representative of any Government, body, or organisation referred to in any of paragraphs (a) to (e)

foreign person means an individual who is neither a New Zealand citizen nor a permanent resident; and includes a person acting in his or her capacity as an agent or a representative of such an individual

incidentally obtained intelligence means intelligence—

- (a) that is obtained in the course of gathering intelligence about the capabilities, intentions, or activities of foreign organisations or foreign persons; but
- (b) that is not intelligence of the kind referred to in paragraph (a)

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

intercept includes hear, listen to, record, monitor, acquire, or receive a communication, or acquire its substance, meaning, or sense

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

interception warrant means a warrant issued under section 15A(1)(a)

medium means any form in which communications may be produced, sent, received, processed, or held; and includes electromagnetic, acoustic, or other energy

Minister means the Minister of the Crown who, under any warrant or with the authority of the Prime Minister, is for the time being responsible for the Bureau

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

private communication—

- (a) means a communication between 2 or more parties 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 occurring in circumstances in which any party ought reasonably to expect that the communication may be intercepted by some other person not having the express or implied consent of any party to do so

serious crime means,—

- (a) in relation to New Zealand, any offence punishable by 2 or more years' imprisonment; and
- (b) in relation to an overseas country, any offence that, if it occurred in New Zealand, would be an offence punishable by 2 or more years' imprisonment.

Section 4 **access**: amended, on 26 September 2013, by section 5(4) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 4 **access authorisation**: inserted, on 26 September 2013, by section 5(3) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 4 **communication**: amended, on 26 September 2013, by section 5(5) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 4 **computer access authorisation** or **authorisation**: repealed, on 26 September 2013, by section 5(2) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 4 **computer system**: repealed, on 26 September 2013, by section 5(2) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 4 **foreign communications**: repealed, on 26 September 2013, by section 5(2) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 4 **foreign intelligence**: repealed, on 26 September 2013, by section 5(2) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 4 **foreign organisation** paragraph (d): amended, on 26 September 2013, by section 5(6) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 4 **incidentally obtained intelligence**: inserted, on 26 September 2013, by section 5(3) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 4 **information infrastructure**: inserted, on 26 September 2013, by section 5(3) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 4 **interception warrant**: amended, on 26 September 2013, by section 5(7) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 4 **network**: repealed, on 26 September 2013, by section 5(2) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 4 **permanent resident**: amended, at 2 am on 29 November 2010, by section 406(1) of the Immigration Act 2009 (2009 No 51).

Section 4 **serious crime** paragraph (a): amended, on 1 July 2013, by section 413 of the Criminal Procedure Act 2011 (2011 No 81).

Section 4 **serious crime** paragraph (b): amended, on 1 July 2013, by section 413 of the Criminal Procedure Act 2011 (2011 No 81).

5 Act binds the Crown

This Act binds the Crown.

5A Transitional provisions relating to amendments to Act

The Schedule contains transitional provisions relating to amendments made to this Act after 1 January 2013.

Section 5A: inserted, on 26 September 2013, by section 6 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Part 2

Organisation, objectives, and functions of Bureau

6 Bureau continued and established as department

- (1) There continues to be an instrument of the Executive Government of New Zealand known as the Government Communications Security Bureau.
- (2) On and from the commencement of this Act, the Bureau is a department of State.

7 Objective of Bureau

The objective of the Bureau, in performing its functions, is to contribute to—

- (a) the national security of New Zealand; and
- (b) the international relations and well-being of New Zealand; and
- (c) the economic well-being of New Zealand.

Section 7: replaced, on 26 September 2013, by section 7 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

8 Functions of Bureau

- (1) Sections 8A to 8C set out the functions of the Bureau.
- (2) The order in which the functions are set out is not to be taken as specifying any order of importance or priority.
- (3) The performance of the Bureau's functions and the relative importance and priority of the functions, if any, are to be determined, from time to time, by the Director, subject to the control of the Minister.
- (4) Without limiting subsection (3), the performance of the Bureau's functions under section 8A (information assurance and cybersecurity) and section 8C (co-operation with other entities to facilitate their functions) is at the discretion of the Director.
- (5) In addition to the functions set out in sections 8A to 8C, the Bureau has the functions (if any) conferred on it by or under any other Act.

Section 8: replaced, on 26 September 2013, by section 7 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

8A Information assurance and cybersecurity

This function of the Bureau is—

- (a) to co-operate with, and provide advice and assistance to, any public authority whether in New Zealand or overseas, or to any other entity authorised by the Minister, on any matters relating to the protection, security, and integrity of—
 - (i) communications, including those that are processed, stored, or communicated in or through information infrastructures; and
 - (ii) information infrastructures of importance to the Government of New Zealand; and
- (b) without limiting paragraph (a), to do everything that is necessary or desirable to protect the security and integrity of the communications and information infrastructures referred to in paragraph (a), including identifying and responding to threats or potential threats to those communications and information infrastructures; and
- (c) to report on anything done under paragraphs (a) and (b) and provide any intelligence gathered as a result and any analysis of the intelligence to—
 - (i) the Minister; and
 - (ii) any person or office holder (whether in New Zealand or overseas) authorised by the Minister to receive the report or intelligence.

Section 8A: inserted, on 26 September 2013, by section 7 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

8B Intelligence gathering and analysis

- (1) This function of the Bureau is—
 - (a) to gather and analyse intelligence (including from information infrastructures) in accordance with the Government's requirements about the capabilities, intentions, and activities of foreign persons and foreign organisations; and
 - (b) to gather and analyse intelligence about information infrastructures; and
 - (c) to provide any intelligence gathered and any analysis of the intelligence to—
 - (i) the Minister; and
 - (ii) any person or office holder (whether in New Zealand or overseas) authorised by the Minister to receive the intelligence.
- (2) For the purpose of performing its function under subsection (1)(a) and (b), the Bureau may co-operate with, and provide advice and assistance to, any public authority (whether in New Zealand or overseas) and any other entity authorised by the Minister for the purposes of this subsection.

Section 8B: inserted, on 26 September 2013, by section 7 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

8C Co-operation with other entities to facilitate their functions

- (1) This function of the Bureau is to co-operate with, and provide advice and assistance to, the following for the purpose of facilitating the performance of their functions:
 - (a) the New Zealand Police; and
 - (b) the New Zealand Defence Force; and
 - (c) the New Zealand Security Intelligence Service.
- (2) To avoid doubt, the Bureau may perform its function under subsection (1)—
 - (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 their functions and exercise their powers; and
 - (c) even though the advice and assistance might involve the exercise of powers by, or the sharing of the capabilities of, the Bureau that the Bureau is not, or could not be, authorised to exercise or share in the performance of its other functions.
- (3) Any advice or assistance provided by the Bureau under subsection (1) to another entity is subject to—
 - (a) the jurisdiction of any other body or authority to the same extent as the other 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 of Intelligence and Security under his or her functions in section 11 of the Inspector-General of Intelligence and Security Act 1996.

Section 8C: inserted, on 26 September 2013, by section 7 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

8D Principles underpinning performance of Bureau's functions

- (1) In performing its functions under this Act, the Bureau acts—
 - (a) in accordance with New Zealand law and all human rights standards recognised by New Zealand law, except to the extent that they are, in relation to national security, modified by an enactment;
 - (b) in the discharge of its operational functions, independently and impartially;
 - (c) with integrity and professionalism;
 - (d) in a manner that facilitates effective democratic oversight.
- (2) Subsection (1) does not impose particular duties on, or give particular powers to, the Bureau, the Director, or any employee of the Bureau.

- (3) The Director must take all reasonable steps to ensure that—
- (a) the activities of the Bureau are limited to those that are relevant to the discharge of its functions;
 - (b) the Bureau is kept free from any influence or consideration that is not relevant to its functions;
 - (c) the Bureau does not take any action for the purpose of furthering or harming the interests of any political party in New Zealand.
- (4) The Director must consult regularly with the Leader of the Opposition for the purpose of keeping him or her informed about matters relating to the Bureau's functions under sections 8A to 8C.

Section 8D: inserted, on 26 September 2013, by section 7 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

8E Director has full powers for purpose of performing Bureau's functions

- (1) The Director has all the powers that are necessary or desirable for the purpose of performing the functions of the Bureau.
- (2) Subsection (1) applies subject to this Act, any other enactment, and the general law.

Section 8E: inserted, on 26 September 2013, by section 7 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

9 Appointment of Director

- (1) The Director of the Bureau is appointed by the Governor-General, on the recommendation of the Prime Minister, for a term not exceeding 5 years, and may from time to time be reappointed.
- (2) To avoid doubt, the mere fact that a person holds the position of Director does not entitle the person to be reappointed or to expect to be reappointed.

Section 9: replaced, on 26 September 2013, by section 8 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

9A Appointment process

The State Services Commissioner—

- (a) is responsible for managing the process for the appointment of the Director; and
- (b) must provide advice on the nominations for Director to the Prime Minister.

Section 9A: inserted, on 26 September 2013, by section 8 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

9B Remuneration and conditions of appointment of Director

- (1) The Director is paid the remuneration and allowances determined by the Remuneration Authority.

- (2) The other terms and conditions of the Director's appointment are determined from time to time by the State Services Commissioner.

Section 9B: inserted, on 26 September 2013, by section 8 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

9C Removal from office

- (1) The Governor-General may at any time for just cause, on the recommendation of the Prime Minister, remove the Director from office.
- (2) The removal must be made by written notice to the Director.
- (3) The notice must—
 - (a) state the date on which the removal takes effect, which must not be earlier than the date on which the notice is received; and
 - (b) state the reasons for the removal.
- (4) The State Services Commissioner is responsible for advising the Prime Minister on any proposal to remove the Director from office.
- (5) In this section, **just cause** includes misconduct, inability to perform the functions of office, and neglect of duty.

Section 9C: inserted, on 26 September 2013, by section 8 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

9D Review of performance of Director

- (1) The Minister may direct the State Services Commissioner or another person to review, either generally or in respect of any particular matter, the performance of the Director.
- (2) The person conducting a review under subsection (1) must report to the Minister on the manner and extent to which the Director is fulfilling all of the requirements imposed on the Director, whether under this Act or otherwise.
- (3) No review under this section may consider any security operations undertaken, or proposed to be undertaken.

Section 9D: inserted, on 26 September 2013, by section 8 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

10 Acting Director

- (1) When there is a vacancy in the position of Director or when the Director is (for whatever reason) absent from duty, the functions, duties, and powers of the Director must be exercised or performed by a person whom the Minister directs to exercise or perform those functions, duties, and powers.
- (2) The Minister may give a direction before the occurrence of any vacancy or absence referred to in subsection (1) or while the vacancy or absence continues.
- (3) No direction and no act done by a person acting under a direction given under this section may, in a proceeding, be questioned on the ground that the occasion

for the direction had not arisen or had ceased, or on the ground that the person had not been appointed to a position to which the direction relates.

11 Prohibition on unauthorised disclosure of information

- (1) A person who is or was an employee of the Bureau may not disclose or use any information gained by or conveyed to the person through the person's connection with the Bureau except in the strict course of the person's official duties or as authorised by the Minister.
- (2) Every person commits an offence and is liable on conviction to imprisonment for a term not exceeding 3 years or to a fine not exceeding \$5,000 who contravenes subsection (1).

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

Section 11(2): amended, on 26 September 2013, by section 9(a) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 11(2): amended, on 26 September 2013, by section 9(b) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 11(2): amended, on 1 July 2013, by section 413 of the Criminal Procedure Act 2011 (2011 No 81).

12 Annual report

- (1) As soon as practicable after each year ending on 30 June, the Director must deliver to the Minister a report on the activities of the Bureau during that year as if it were an annual report under the Public Finance Act 1989.
- (2) When the Minister receives a copy of a report under subsection (1), the Minister must, as soon as practicable, submit a copy of the report to the members of the Intelligence and Security Committee established under the Intelligence and Security Committee Act 1996.
- (3) Within 30 sitting days after receiving the report under subsection (1), the Minister must present to the House of Representatives a copy of the report that accords with any directions given under subsection (4), and includes—
 - (a) *[Repealed]*
 - (b) a statement as to whether or not any interception warrants were in force during the year to which the report relates; and
 - (ba) if any interception warrants have been issued during the year to which the report relates, the number of warrants issued; and
 - (c) a statement as to whether or not any access authorisations were in force during the year to which the report relates; and
 - (ca) if any access authorisations have been issued during the year to which the report relates, the number of authorisations issued; and
 - (cb) a statement as to whether the Bureau has, under its function specified in section 8C(1), provided during the year to which the report relates any

- advice or assistance and, if so, the number of instances on which advice or assistance has been provided; and
- (d) a statement setting out—
 - (i) a summary of the Bureau’s equal employment opportunities programme for the year to which the report relates; and
 - (ii) an account of the extent to which the Bureau was able to meet, during the year to which the report relates, the equal employment opportunities programme for that year.
- (4) Before presenting a copy of the report to the House of Representatives under subsection (3), the Minister may direct that any material (other than the material referred to in section 45E(1)(c)(i) of the Public Finance Act 1989 and subsection (3)(b) to (d)) be deleted from the report if the Minister considers that the material is 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; or
 - (e) to prejudice unreasonably the privacy of an individual.

Compare: 1969 No 24 s 4J

Section 12(1): amended, on 25 January 2005, by section 37(1) of the Public Finance Amendment Act 2004 (2004 No 113).

Section 12(2): amended, on 26 September 2013, by section 10(1) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 12(3)(a): repealed, on 25 January 2005, by section 37(1) of the Public Finance Amendment Act 2004 (2004 No 113).

Section 12(3)(ba): inserted, on 26 September 2013, by section 10(2) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 12(3)(c): amended, on 26 September 2013, by section 10(3) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 12(3)(ca): inserted, on 26 September 2013, by section 10(4) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 12(3)(cb): inserted, on 26 September 2013, by section 10(4) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 12(4): amended, on 25 January 2005, by section 37(1) of the Public Finance Amendment Act 2004 (2004 No 113).

Part 3

Intercepting communications and accessing information infrastructures

Part 3 heading: replaced, on 26 September 2013, by section 11 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Purpose of Part

13 Purpose of Part

The purpose of this Part is—

- (a) to authorise the Bureau to intercept communications and access information infrastructures for the purpose of performing its functions under sections 8A and 8B; and
- (b) to place restrictions and limitations on—
 - (i) the interception of communications and the accessing of information infrastructures; and
 - (ii) the retention and use of information derived from the interception of communications and the accessing of information infrastructures.

Section 13: replaced, on 26 September 2013, by section 12 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Restrictions imposed on interceptions

14 Interceptions not to target New Zealand citizens or permanent residents for intelligence-gathering purposes

- (1) In performing the Bureau's function in section 8B, the Director, any employee of the Bureau, and any person acting on behalf of the Bureau must not authorise or do anything for the purpose of intercepting the private communications of a person who is a New Zealand citizen or a permanent resident of New Zealand, unless (and to the extent that) the person comes within the definition of foreign person or foreign organisation in section 4.
- (2) Any incidentally obtained intelligence obtained by the Bureau in the performance of its function in section 8B—
 - (a) is not obtained in breach of section 8B; but
 - (b) must not be retained or disclosed except in accordance with sections 23 and 25.

Section 14: replaced, on 26 September 2013, by section 13 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

15 Interceptions for which warrant or authorisation required

- (1) Unless authorised by an interception warrant to do so, neither the Director, nor an employee of the Bureau, nor a person acting on behalf of the Bureau may—

- (a) physically connect an interception device to any part of an information infrastructure; or
 - (b) install an interception device in a place for the purpose of intercepting communications that occur in the place.
- (2) Unless authorised by section 16 or by an access authorisation to do so, neither the Director, nor an employee of the Bureau, nor a person acting on behalf of the Bureau may access an information infrastructure that the person concerned is not otherwise authorised to access.

Section 15(1)(a): amended, on 26 September 2013, by section 14(1) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 15(2): amended, on 26 September 2013, by section 14(2)(a) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 15(2): amended, on 26 September 2013, by section 14(2)(b) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

*Authorisations to intercept communications or access information
infrastructures*

Heading: inserted, on 26 September 2013, by section 15 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

**15A Authorisation to intercept communications or access information
infrastructures**

- (1) For the purpose of performing the Bureau's functions under section 8A or 8B, the Director may apply in writing to the Minister for the issue of—
- (a) an interception warrant authorising the use of interception devices to intercept communications not otherwise lawfully obtainable by the Bureau of the following kinds:
 - (i) communications made or received by 1 or more persons or classes of persons specified in the authorisation or made or received in 1 or more places or classes of places specified in the authorisation;
 - (ii) communications that are sent from, or are being sent to, an overseas country;
 - (b) an access authorisation authorising the accessing of 1 or more specified information infrastructures or classes of information infrastructures that the Bureau cannot otherwise lawfully access.
- (2) The Minister may grant the proposed interception warrant or access authorisation if satisfied that—
- (a) the proposed interception or access is for the purpose of performing a function of the Bureau under section 8A or 8B; and
 - (b) the outcome sought to be achieved under the proposed interception or access justifies the particular interception or access; and
 - (c) the outcome is not likely to be achieved by other means; and

- (d) there are satisfactory arrangements in place to ensure that nothing will be done in reliance on the warrant or authorisation beyond what is necessary for the proper performance of a function of the Bureau; and
 - (e) there are satisfactory arrangements in place to ensure that the nature and consequences of acts done in reliance on the warrant or authorisation will be reasonable, having regard to the purposes for which they are carried out.
- (3) Before issuing a warrant or an authorisation, the Minister must consult the Minister of Foreign Affairs about the proposed warrant or authorisation.
 - (4) The Minister may issue a warrant or an authorisation subject to any conditions that the Minister considers desirable in the public interest.
 - (5) This section applies despite anything in any other Act.

Section 15A: inserted, on 26 September 2013, by section 15 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

15B Involvement of Commissioner of Security Warrants

- (1) An application for, and issue of, an interception warrant or access authorisation under section 15A must be made jointly to, and issued jointly by, the Minister and the Commissioner of Security Warrants if anything that may be done under the warrant or authorisation is for the purpose of intercepting the private communications of a New Zealand citizen or permanent resident of New Zealand under—
 - (a) section 8A; or
 - (b) section 8B, to the extent that intercepting the person's private communications under that section is not precluded by section 14.
- (2) For the purposes of subsection (1), section 15A applies—
 - (a) as if references to the Minister were references to the Minister and the Commissioner of Security Warrants; and
 - (b) with any other necessary modifications.
- (3) In this section, **Commissioner of Security Warrants** means the Commissioner of Security Warrants appointed under section 5A of the New Zealand Security Intelligence Service Act 1969.

Section 15B: inserted, on 26 September 2013, by section 15 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

15C Privileged communications

- (1) No interception warrant or access authorisation is to be issued under section 15A, and no powers are to be exercised under an interception warrant or access authorisation issued under section 15A, for the purpose of intercepting the privileged communications of New Zealand citizens or permanent residents of New Zealand.

- (2) In subsection (1), **privileged communications** means communications that are privileged in proceedings in a court of law under section 54, 56, 58, or 59 of the Evidence Act 2006.

Section 15C: inserted, on 26 September 2013, by section 15 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

15D Information that interception warrant or access authorisation must contain

- (1) Every interception warrant and access authorisation must specify the following information:
- (a) the date of issue:
 - (b) the person, persons, or classes of persons authorised to make the interception or obtain the access:
 - (c) the period for which the warrant or authorisation is issued, being a period not exceeding 12 months:
 - (d) the function or functions of the Bureau to which the warrant or authorisation relates:
 - (e) the purpose of the warrant or authorisation:
 - (f) any conditions under which interception may be made or access may be obtained.
- (2) Every interception warrant must also specify the following information:
- (a) if the purpose of the warrant is to authorise the interception of the communications of 1 or more persons, the person, persons, or classes of persons whose communications may be intercepted:
 - (b) if the purpose of the warrant is to intercept communications at 1 or more places, the place, places, or classes of places that the warrant applies to.
- (3) Every access authorisation must also specify the information infrastructure, information infrastructures, or classes of information infrastructures that the authorisation applies to.

Section 15D: inserted, on 26 September 2013, by section 15 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

15E Warrant or authorisation may authorise persons to assist person giving effect to warrant or authorisation

- (1) A warrant or an authorisation may request 1 or more persons or classes of persons to give any assistance that is reasonably necessary to give effect to the warrant or authorisation.
- (2) If a request is made, under subsection (1), to 1 or more persons or classes of persons who are employees (the **employees**), the warrant or authorisation must also request the persons who are the employers of the employees, or any other persons in any way in control of the employees, to make the services of the employees available to the Bureau.

- (3) On an application made in writing by the Director, the Minister may amend a warrant or authorisation (as appropriate)—
- (a) by substituting a person, persons, or classes of persons for the person, persons, or classes of persons specified in the warrant under section 15D(2)(a):
 - (b) by substituting another person, other persons, or other classes of persons for a person, persons, or classes of persons requested under subsection (1):
 - (c) by adding any person, persons, or classes of persons to the persons requested under subsection (1).

Section 15E: inserted, on 26 September 2013, by section 15 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

15F Expiry of warrant or authorisation not to prevent further application

The expiry of an interception warrant or of an authorisation does not prevent a further application for an interception warrant or an authorisation in respect of the same subject matter.

Section 15F: inserted, on 26 September 2013, by section 15 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

16 Certain interceptions permitted without interception warrant or access authorisation

- (1A) This section—
- (a) applies to the interception of communications for the purpose of the Bureau's functions in sections 8A and 8B; but
 - (b) does not authorise anything to be done for the purpose of intercepting the private communications of a New Zealand citizen or permanent resident of New Zealand.
- (1) The Director, or an employee of the Bureau, or a person acting on behalf of the Bureau may, without an interception warrant, or, as the case requires, without a computer access authorisation, intercept communications only if the interception is authorised by this Act or by another enactment.
- (2) The Director, or an employee of the Bureau, or a person acting on behalf of the Bureau may, without an interception warrant, or, as the case requires, without an access authorisation, intercept communications by using an interception device or by accessing an information infrastructure, but only if—
- (a) the interception does not involve any activity specified in section 15(1); and
 - (b) any access to an information infrastructure is limited to access to 1 or more communication links between computers or to remote terminals; and

- (c) the interception is carried out by the Director or with the authority of the Director for the purpose of performing the Bureau's function in section 8A or 8B.
- (3) This section is subject to section 14.
- Section 16 heading: amended, on 26 September 2013, by section 16(1) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).
- Section 16(1A): inserted, on 26 September 2013, by section 16(2) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).
- Section 16(1): amended, on 26 September 2013, by section 16(3) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).
- Section 16(2): replaced, on 26 September 2013, by section 16(4) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Interception warrants

[Repealed]

Heading: repealed, on 26 September 2013, by section 17 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

17 Issue of interception warrant

[Repealed]

Section 17: repealed, on 26 September 2013, by section 17 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

18 Persons acting under warrant

[Repealed]

Section 18: repealed, on 26 September 2013, by section 18 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Register of interception warrants and access authorisations

Heading: replaced, on 26 September 2013, by section 19 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

19 Register of interception warrants and access authorisations

- (1) The Director must keep a register of interception warrants and access authorisations issued under this Part.
- (2) The following information must be entered in the register in relation to every interception warrant and access authorisation issued under this Part:
- (a) the information specified in section 15D; and
 - (b) whether the warrant or authorisation contains a request to give assistance under section 15E(1); and
 - (c) any person, persons, or classes of persons substituted or added under section 15E(3).

- (3) The Director must make the register available to the Minister or the Inspector-General of Intelligence and Security as and when requested by the Minister or the Inspector-General.
- (4) As soon as practicable after information specified in section 15D(2)(a) is entered in the register, the Director must notify the Inspector-General of Intelligence and Security if the information relates to a New Zealand citizen or a permanent resident of New Zealand.

Section 19: replaced, on 26 September 2013, by section 19 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Urgent issue of warrants and authorisations

Heading: inserted, on 26 September 2013, by section 19 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

19A Urgent issue of warrants and authorisations

- (1) This section applies if—
 - (a) the Minister is unavailable to issue an interception warrant or access authorisation; and
 - (b) circumstances make it necessary to issue a warrant or an authorisation before the Minister is available to do so.
- (2) Any of the following may issue a warrant or an authorisation:
 - (a) the Attorney-General;
 - (b) the Minister of Defence;
 - (c) the Minister of Foreign Affairs.
- (3) A person issuing a warrant or an authorisation under subsection (2) may do so only to the same extent and subject to the same terms and conditions as apply to the issue of a warrant or an authorisation by the Minister.
- (4) A person issuing a warrant or an authorisation under subsection (2) must, as soon as practicable after the Minister becomes available, advise the Minister about the issue of the warrant.

Section 19A: inserted, on 26 September 2013, by section 19 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Provisions applicable to warrants, authorisations, and powers under section 16

20 Director's functions in relation to warrants and authorisations not to be delegated

Despite section 41 of the State Sector Act 1988, the Director may not delegate to any person the Director's functions under section 15A.

Section 20: amended, on 26 September 2013, by section 20 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

21 Immunity from civil and criminal liability

- (1) Every person is immune from civil or criminal liability—
 - (a) for any act done in good faith in order to obtain a warrant or an authorisation under this Act:
 - (b) for anything done in good faith under a warrant or an authorisation under this Act or under section 16, if done in a reasonable manner.
- (2) Every person is immune from civil and criminal liability for any act done in good faith and in a reasonable manner in order to assist a person to do anything authorised by a warrant or an authorisation under this Act or under section 16.
- (3) In any civil proceeding in which a person asserts that he or she has an immunity under this section, the onus is on the person to prove the facts necessary to establish the basis of the claim.
- (4) Section 86 of the State Sector Act 1988 applies to the Director and any employee of the Bureau subject to this section.

Section 21: replaced, on 26 September 2013, by section 21 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

22 Term of warrant or authorisation

[Repealed]

Section 22: repealed, on 26 September 2013, by section 22 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

23 Destruction of irrelevant records obtained by interception

- (1) Every person who intercepts any communication under section 16 or under an interception warrant or a access authorisation must, as soon as practicable after the interception, destroy any copy that he or she may make of the communication, or any part of the communication, and any record, whether in writing or otherwise, of the information obtained by that interception, except to the extent permitted by section 25 or to the extent that the information recorded in the copy or record relates directly or indirectly to—
 - (a) the protection or advancement of 1 or more of the interests specified in section 7; or
 - (b) any of the Bureau's functions under section 8A or 8B.
- (2) Every person commits an offence and is liable on conviction to a fine not exceeding \$1,000 who knowingly fails to comply with subsection (1).

Compare: 1969 No 24 s 4G

Section 23(1): amended, on 26 September 2013, by section 23(1) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 23(1): amended, on 26 September 2013, by section 23(2) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 23(1)(a): amended, on 26 September 2013, by section 23(3) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 23(1)(b): amended, on 26 September 2013, by section 23(4) of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Section 23(2): amended, on 1 July 2013, by section 413 of the Criminal Procedure Act 2011 (2011 No 81).

24 Duty to minimise impact of interception on third parties

Every person who, in accordance with section 16 or with an interception warrant or with an access authorisation, intercepts or assists in intercepting the communications of 1 or more persons must take all practicable steps that are reasonable in the circumstances to minimise the likelihood of intercepting communications that are not relevant to the persons whose communications are to be intercepted.

Compare: 1969 No 24 s 4F(1)

Section 24: amended, on 26 September 2013, by section 24 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

25 When incidentally obtained intelligence may be retained and communicated to other persons

- (1) Despite section 23, the Director may—
 - (a) retain incidentally obtained intelligence that comes into the possession of the Bureau for 1 or more of the purposes specified in subsection (2); and
 - (b) communicate that intelligence to the persons specified in subsection (3).
- (2) The purposes are—
 - (a) preventing or detecting serious crime in New Zealand or any other country;
 - (b) preventing or avoiding the loss of human life on the high seas;
 - (c) preventing or responding to threats to human life in New Zealand or any other country;
 - (d) identifying, preventing, or responding to threats or potential threats to the security or defence of New Zealand or any other country.
- (3) The persons are—
 - (a) any employee of the New Zealand Police;
 - (b) any member of the New Zealand Defence Force;
 - (c) the Director of Security under the New Zealand Security Intelligence Service Act 1969;
 - (d) any public authority (whether in New Zealand or overseas) that the Director thinks fit to receive the information.

Section 25: replaced, on 26 September 2013, by section 25 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Protection and disclosure of personal information

Heading: inserted, on 26 September 2013, by section 26 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

25A Formulation of policy on personal information

- (1) As soon as is reasonably practicable after the commencement of this section, the Director must, in consultation with the Inspector-General of Intelligence and Security and the Privacy Commissioner, formulate a policy that applies to the Bureau (in a manner compatible with the requirements of national security) the principles set out in section 25B.
- (2) The policy must require—
 - (a) all employees and persons acting on behalf of the Bureau to comply with the policy; and
 - (b) the level of compliance with the policy to be regularly audited.
- (3) The Director must advise the Privacy Commissioner of the results of audits conducted under the policy.
- (4) The Privacy Commissioner may provide a report to the Inspector-General of Intelligence and Security if the results of the audits disclose issues that need to be addressed.
- (5) The Director must regularly review the policy at intervals of not more than 3 years and, if he or she considers it appropriate to do so, revise the policy in consultation with the Inspector-General of Intelligence and Security and the Privacy Commissioner.

Section 25A: inserted, on 26 September 2013, by section 26 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

25B Principles to protect personal information

The principles referred to in section 25A(1) are as follows:

- (a) the Bureau must not collect personal information unless—
 - (i) the information is collected for a lawful purpose connected with a function of the Bureau; and
 - (ii) the collection of the information is reasonably necessary for that purpose, having regard to the nature of intelligence gathering:
- (b) the Bureau must ensure—
 - (i) that any personal information it holds is protected by such security safeguards as it is reasonable in the circumstances to take against—
 - (A) loss; and
 - (B) access, use, modification, or disclosure, except with the authority of the Bureau; and
 - (C) other misuse; and

- (ii) that if it is necessary for any personal information that it holds to be given to a person in connection with the provision of a service to the Bureau, everything reasonably within the power of the Bureau is done to prevent unauthorised use or unauthorised disclosure of the information:
- (c) the Bureau must not use personal information without taking such steps (if any) as are, in the light of the interests and constraints of national security and the nature of intelligence gathering, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading:
- (d) the Bureau must not keep personal information longer than is required for the purposes for which the information may be lawfully used.

Section 25B: inserted, on 26 September 2013, by section 26 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Part 3A

Transitional provisions relating to amendments to Act

Part 3A: inserted, on 26 September 2013, by section 27 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

25C Transitional provisions relating to amendments to Act

The transitional provisions set out in the Schedule, which relate to amendments made to this Act after 1 January 2013, have effect for the purposes of this Act.

Section 25C: inserted, on 26 September 2013, by section 27 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

Part 4

Provisions relating to other enactments

26 Amendment to Crimes Act 1961

Amendment(s) incorporated in the Act(s).

27 Amendment to Higher Salaries Commission Act 1977

Amendment(s) incorporated in the Act(s).

28 Amendment to Inspector-General of Intelligence and Security Act 1996

Amendment(s) incorporated in the Act(s).

29 Amendment to New Zealand Security Intelligence Service Act 1969

Amendment(s) incorporated in the Act(s).

30 Amendment to Official Information Act 1982

Amendment(s) incorporated in the Act(s).

31 Amendment to Public Finance Act 1989

Amendment(s) incorporated in the Act(s).

32 Amendment to Radiocommunications Act 1989

Amendment(s) incorporated in the Act(s).

33 Amendments to State Sector Act 1988

Amendment(s) incorporated in the Act(s).

34 Certain provisions of State Sector Act 1988 not to apply

Sections 30, 40, 58(2), and 68 of the State Sector Act 1988 do not apply to the Government Communications Security Bureau.

35 Revocation

The Crimes (Exemption of Listening Device) Order 1997 (SR 1997/145) is revoked.

Schedule

**Transitional provisions relating to amendments made to Act after 1
January 2013**

ss 5A, 25C

Schedule: inserted, on 26 September 2013, by section 28 of the Government Communications Security Bureau Amendment Act 2013 (2013 No 57).

- (1) Clauses (2) and (3) apply to computer access authorisations and interception warrants issued under this Act and in force immediately before the commencement of the Government Communications Security Bureau Amendment Act 2013.
- (2) The computer access authorisations and interception warrants continue in force as if the amendments made by the Government Communications Security Bureau Amendment Act 2013 had not come into force.
- (3) The computer access authorisations and interception warrants are to be treated as having expired at the close of the third month after the date on which the Government Communications Security Bureau Amendment Act 2013 received the Royal assent, unless they have expired earlier.

Reprints notes

1 *General*

This is a reprint of the Government Communications Security Bureau Act 2003 that incorporates all the amendments to that Act as at the date of the last amendment to it.

2 *Legal status*

Reprints are presumed to correctly state, as at the date of the reprint, the law enacted by the principal enactment and by any amendments to that enactment. Section 18 of the Legislation Act 2012 provides that this reprint, published in electronic form, has the status of an official version under section 17 of that Act. A printed version of the reprint produced directly from this official electronic version also has official status.

3 *Editorial and format changes*

Editorial and format changes to reprints are made using the powers under sections 24 to 26 of the Legislation Act 2012. See also <http://www.pco.parliament.govt.nz/editorial-conventions/>.

4 *Amendments incorporated in this reprint*

Intelligence and Security Act 2017 (2017 No 10): section 242(3)(c)

Government Communications Security Bureau Amendment Act 2013 (2013 No 57)

Criminal Procedure Act 2011 (2011 No 81): section 413

Immigration Act 2009 (2009 No 51): section 406(1)

Public Finance Amendment Act 2004 (2004 No 113): section 37(1)