Reprint
as at 28 September 2017

Government Communications Security Bureau Amendment Act 2013

Public Act	2013 No 57
Date of assent	26 August 2013
Commencement	see section 2

Government Communications Security Bureau Amendment Act 2013: repealed, on 28 September 2017, pursuant to section 242(3)(c) of the Intelligence and Security Act 2017 (2017 No 10).

Contents

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 and Security Bureau.

The Parliament of New Zealand enacts as follows:

1 Title

This Act is the Government Communications Security Bureau Amendment Act 2013.

2 Commencement

This Act comes into force on the day that is 1 month after the date on which it receives the Royal assent.

3 Principal Act

This Act amends the Government Communications Security Bureau Act 2003 (the **principal Act**).

4 Section 3 amended (Purpose)

Replace section 3(c) to (e) with:

(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.

5 Section 4 amended (Interpretation)

(1) This section amends section 4.

(2) Repeal the definitions of **computer access authorisation** or **authorisation**, **computer system**, **foreign communications**, **foreign intelligence**, and **network**.

(3) Insert in their appropriate alphabetical order:

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

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

(4) In the definition of **access**, replace "computer system" with "information infrastructure".

(5) In the definition of **communication**, after "sounds,", insert "information,".

(6) In the definition of **foreign organisation**, paragraph (d), replace "exclusively" with "principally".

(7) In the definition of **interception warrant**, replace "section 17" with "section 15A(1)(a)".

6 New section 5A inserted (Transitional provisions relating to amendments to Act)

After section 5, insert:

5A Transitional provisions relating to amendments to Act

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

7 Sections 7 and 8 replaced

Replace sections 7 and 8 with:

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.

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.

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.

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.

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.

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.

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.

8 Section 9 replaced (Director of Bureau)

Replace section 9 with:

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.

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.

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.

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.

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.

9 Section 11 amended (Prohibition on unauthorised disclosure of information)

In section 11(2),—

(a) replace "2 years" with "3 years"; and

(b) replace "$2,000" with "$5,000".

10 Section 12 amended (Annual report)

(1) In section 12(2), replace "without delay" with "as soon as practicable".

(2) After section 12(3)(b), insert:

(ba) if any interception warrants have been issued during the year to which the report relates, the number of warrants issued; and

(3) In section 12(3)(c), delete "computer".

(4) After section 12(3)(c), insert:

(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

11 Part 3 heading replaced

Replace the Part 3 heading with:

Part 3
Intercepting communications and accessing information infrastructures

12 Section 13 replaced (Purpose of Part)

Replace section 13 with:

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.

13 Section 14 replaced (Interceptions not to target domestic communications)

Replace section 14 with:

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.

14 Section 15 amended (Interceptions for which warrant or authorisation required)

(1) In section 15(1)(a), replace "a network" with "an information infrastructure".

(2) In section 15(2),—

(a) replace "a computer access authorisation" with "an access authorisation"; and

(b) replace "a computer system" with "an information infrastructure".

15 New sections 15A to 15F and cross-heading inserted

After section 15, insert:

Authorisations to intercept communications or access information infrastructures

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.

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.

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.

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.

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).

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.

16 Section 16 amended (Certain interceptions permitted without interception warrant or computer access authorisation)

(1) In the heading to section 16, delete "**computer**".

(2) In section 16, before subsection (1), insert:

(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.

(3) In section 16(1), delete "foreign".

(4) Replace section 16(2) with:

(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.

17 Section 17 and cross-heading repealed

Repeal section 17 and the cross-heading above section 17.

18 Section 18 repealed (Persons acting under warrant)

Repeal section 18.

19 Section 19 and cross-heading replaced

Replace section 19 and the cross-heading above section 19 with:

Register of interception warrants and access authorisations

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.

Urgent issue of warrants and authorisations

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.

20 Section 20 amended (Director's functions in relation to warrants and authorisations not to be delegated)

In section 20, replace "section 17 or section 19" with "section 15A".

21 Section 21 replaced (Action taken in accordance with warrant or authorisation justified)

Replace section 21 with:

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.

22 Section 22 repealed (Term of warrant or authorisation)

Repeal section 22.

23 Section 23 amended (Destruction of irrelevant records obtained by interception)

(1) In section 23(1), delete "computer".

(2) In section 23(1), after "except to the extent", insert "permitted by section 25 or to the extent".

(3) In section 23(1)(a), replace "section 7(1)(a)" with "section 7".

(4) In section 23(1)(b), replace "section 8" with "section 8A or 8B".

24 Section 24 amended (Duty to minimise impact of interception on third parties)

In section 24, replace "a computer" with "an".

25 Section 25 replaced (Prevention or detection of serious crime)

Replace section 25 with:

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.

26 New sections 25A and 25B and cross-heading inserted

After section 25, insert:

Protection and disclosure of personal information

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.

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.

27 New Part 3A inserted

Before Part 4, insert:

Part 3A
Transitional provisions relating to amendments to Act

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.

28 Schedule inserted

Insert the Schedule set out in Schedule 1.

29 Consequential amendments

The Acts listed in Schedule 2 are consequentially amended in the manner indicated in that schedule.

Schedule 1
New Schedule inserted

s 28

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

ss 5A, 25C

(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.

Schedule 2
Consequential amendments

s 29

Radiocommunications Act 1989 (1989 No 148)

In section 133A(2)(c)(ii), replace "foreign intelligence" with "intelligence about the capabilities, intentions, and activities of foreign persons and foreign organisations".

Repeal section 133A(3)(a).

Search and Surveillance Act 2012 (2012 No 24)

In section 47(1)(c)(ii), replace "17" with "15A(1)(a)".

Telecommunications (Interception Capability) Act 2004 (2004 No 19)

In section 3(1), definition of **interception warrant**, paragraph (c), replace "17" with "15A(1)(a)".

In section 3(1), definition of **other lawful interception authority**, replace paragraph (a)(ii) with:

(ii) to access an information infrastructure (within the meaning of the Government Communications Security Bureau Act 2003) that is granted under section 15A(1)(b) of that Act; and

Reprints notes

1 General

This is a reprint of the Government Communications Security Bureau Amendment Act 2013 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)

Wellington, New Zealand:
Published under the authority of the New Zealand Government—2017