Government Communications Security Bureau and Related Legislation Amendment Bill

Government Bill

Explanatory note

General policy statement

This Bill is an omnibus Bill that amends the Government Communications Security Bureau Act 2003, the Inspector-General of Intelligence and Security Act 1996, and the Intelligence and Security Committee Act 1996. It is proposed (at the close of the Bill's committee of the whole House stage in Parliament) to divide the Bill into 3 separate amending Bills.

The purposes of the Bill are to—

- provide for a clearly formulated and consistent statutory framework governing the activities of the Government Communications Security Bureau (**GCSB**); and
- update that framework to respond to the changing security environment (particularly in relation to cybersecurity and information security), and to changes in the public law environment since the GCSB Act was passed in 2003; and
- enhance the external oversight mechanisms that apply to the intelligence agencies by strengthening the office of the Inspector-General of Intelligence and Security and by improving

the operation of Parliament's Intelligence and Security Committee.

Amendments to Government Communications Security Bureau Act 2003

It is crucial that an agency exercising intrusive powers, as GCSB does, is governed by a consistent statutory framework that articulates the agency's functions and powers, as well as the applicable controls and limitations, in the clearest possible terms. This promotes robust internal management and effective external oversight of the agency's activities.

The March 2013 *Review of Compliance at the Government Communications Security Bureau* by Rebecca Kitteridge highlighted difficulties in interpreting the GCSB Act when the Bureau was providing assistance to other agencies, notably the New Zealand Security Intelligence Service. In a small jurisdiction like New Zealand, it is essential that specialised capabilities developed or acquired by agencies like GCSB should be available to meet key government priorities, where appropriate and subject to necessary safeguards. The Bill amends the GCSB Act to clarify this important support role as well as other aspects of the Bureau's functions.

At the same time, New Zealand faces a changing security environment in which threats are increasingly interconnected and national borders are less meaningful. Globalisation means New Zealand is no longer as distant from security threats as it once was. This changed environment means the legislation governing GCSB needs updating, to enable it to address the security challenges posed by the increasing importance of cyberspace.

The Bill retains the basic construct of the GCSB Act and the core principles underpinning GCSB's operations. Amendments to the objective, functions, powers, and limitation provisions are designed to address the issues above—namely, to improve clarity about the legal parameters for GCSB's activities; and to accommodate changes in the prevailing security environment.

Objective and functions of GCSB

The Bill replaces the objective of GCSB with a simple statement that it strives, through its functions, to contribute to New Zealand's national security, international relations, and economic well-being.

The Act currently provides for 3 core functions of GCSB:

- information assurance and cybersecurity:
- foreign intelligence:
- co-operation with and assistance to other entities.

These 3 functions will be retained in substance. How they are articulated will be changed to improve transparency and facilitate external oversight of GCSB's activities.

The statement of the 3 functions will be split into separate provisions (*new sections 8A, 8B, and 8C*). The information assurance and cybersecurity function will be given greater prominence, reflecting the key role GCSB plays in the wider cybersecurity domain—including its hosting of New Zealand's National Cyber Security Centre, and its responsibility to use its cybersecurity capabilities to assist a range of public entities as well as private sector organisations such as critical national infrastructure providers and organisations of national significance.

The foreign intelligence function will be described in a way that provides transparency about the nature and scope of this role, without expressly legislating the range of activities involved or the skills required in pursuit of this function.

The Act will be changed to provide a sounder basis for GCSB to offer expert advice and assistance to other entities. The Bureau will have clear legal authority to assist the New Zealand Defence Force, New Zealand Police, and New Zealand Security Intelligence Service (as well as any other department that may be specified by Order in Council) in performing their lawful functions. In providing such assistance, GCSB will be confined to activities that the other entity is lawfully able to undertake itself (though it may not have the capability), and will be subject to any limitations and restrictions that apply to the other entity.

Powers, controls, and limitations

The Act confers 3 powers of interception on GCSB:

- warrantless interception in situations not involving the physical connection of an interception device to a network; and not involving the installation of an interception device in any place in order to intercept communications in that place (sections 15 and 16):
- interception of communications by an interception device under an interception warrant granted by the responsible Minister (section 17):
- access to a computer system under a computer access authorisation granted by the responsible Minister (section 19).

This construct continues to provide the basic tools that GCSB needs to perform its functions, and it will be retained.

At present, section 13 of the Act dictates that the Bureau's powers are available for the purpose of obtaining foreign intelligence. While much of GCSB's work (including in the cybersecurity domain) can ultimately be linked to a foreign intelligence objective, the Act was conceived at a time when the nature, extent, and potential impact of the cyber threat was dramatically different from the threat posed now. The Act will be amended to make it clear that the powers can be used for both the foreign intelligence function and the information assurance and cybersecurity function, subject to appropriate controls and limitations.

The basic premise underpinning GCSB's operations is that it is not to conduct foreign intelligence activities against New Zealanders. This premise predated the GCSB Act, and was incorporated in the GCSB Act (in section 14) because of its importance. However, the way this basic premise was incorporated into the Act meant that it applied not only to the foreign intelligence function of the Bureau, but also to its other 2 functions: information assurance and assisting other entities. This has resulted in a growing number of difficulties, and is restricting GCSB's ability to effectively carry out its other 2 functions.

The basic premise in section 14 will be retained, with an adjustment to clarify that it only applies to the foreign intelligence function. As a safeguard in respect of New Zealanders' privacy, any activity under *new section 8A or 8B* that might involve intercepting the communications of New Zealanders will require an authorisation to be granted

jointly by the responsible Minister and the Commissioner of Security Warrants (appointed under the New Zealand Security Intelligence Service Act 1969). When GCSB is assisting another entity under *new section 8C*, the authorisation processes and any restrictions or limitations that apply to that entity will apply to the Bureau's assistance.

Other amendments

A range of amendments designed to complement other changes, or in the interests of updating the Act generally, includes the following:

- to enable the Inspector-General of Intelligence and Security to have access to the best possible information, the Act will be amended to require GCSB to maintain a written record of all warrants and authorisations in a form readily available for inspection:
- in line with the recommendation of the Law Commission in June 2011, principles 1, 5, 8, and 9 of the Privacy Act 1993 will apply to GCSB, modified if necessary to achieve the effective and efficient performance by the Bureau of its functions:
- the appointment framework for the Director of GCSB will be modified to codify the State Service Commissioner's support for that process, as currently set out in the Cabinet Manual:
- in situations of urgency where the responsible Minister is not readily available, the Attorney-General, the Minister of Foreign Affairs or the Minister of Defence will be empowered to issue an interception warrant or an access authorisation:
- the maximum penalty for unauthorised disclosure of information will be increased to align it with the penalty for similar types of offending, for example in the Crimes Act 1961.

Amendments to Inspector-General of Intelligence and Security Act 1996

Effective and credible oversight of the intelligence agencies is crucial to provide assurance that those agencies' powers are being used in accordance with the law and with respect for New Zealanders' right to privacy. The Inspector-General of Intelligence and Security (**IGIS**) is a source of independent external oversight, responsible for examining issues of legality and propriety, efficacy and efficiency, and human rights and privacy compliance.

The Bill amends the Inspector-General of Intelligence and Security Act 1996 to strengthen the office of the IGIS, increasing the resourcing of the office to enable a greater range of activities to be carried out, expanding the IGIS's statutory work programme, and enhancing the corresponding reporting responsibilities.

The changes to the Act include the following:

- the statutory work programme of the IGIS, which includes a focus on warrants and authorisations issued to the intelligence agencies, will be extended to require regular examination of system-wide issues that impact on operational activities:
- the IGIS will be required to certify each year in his or her annual report whether the compliance systems of the intelligence agencies are sound:
- the IGIS will be able to initiate inquiries into matters of propriety without requiring the concurrence of the responsible Minister. This will enable the IGIS to undertake independent inquiries:
- the responsible Minister will be given explicit responsibility to respond to IGIS reports within a reasonable time frame. The Minister may choose to provide those responses also to the Intelligence and Security Committee:
- the IGIS will be expected to make unclassified versions of his or her reports publicly available, with appropriate precautions being taken in respect of any privacy or security concerns:
- the legislative requirement that the IGIS be a retired High Court Judge will be removed, broadening the pool of potential candidates. The 3-year term of office will remain, with the possibility of reappointment for a maximum of 1 additional term:
- a Deputy IGIS will be appointed.

Amendments to Intelligence and Security Committee Act 1996

The Intelligence and Security Committee (**ISC**) is the parliamentary mechanism for oversight of the intelligence agencies. It examines issues of efficacy and efficiency, budgetary matters, and policy-setting.

The Bill amends the Intelligence and Security Committee Act 1996 to improve the ISC's ability to provide effective oversight and accountability of the intelligence agencies.

The changes to the Act involve the following:

- the Prime Minister will be required to relinquish the ISC chair if the Committee, when conducting a financial review of an intelligence agency for which the Prime Minister is the responsible Minister, is discussing the performance of that agency:
- the Prime Minister will be permitted to nominate either the Deputy Prime Minister or the Attorney-General to act as an alternate chair in circumstances where that alternate is not already a member of the ISC:
- subject to restrictions on the publication of sensitive information, the ISC will be required to table its reports in the House and make them publicly available on an Internet site.

Regulatory impact statement

The Department of the Prime Minister and Cabinet with the Government Communications Security Bureau produced a regulatory impact statement on 22 March 2013 to help inform the main policy decisions taken by the Government relating to the contents of this Bill.

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

- http://www.gcsb.govt.nz/about-us/legislation.html
- http://www.treasury.govt.nz/publications/informationreleases/ris

Clause by clause analysis

Clause 1 states the title of the Bill. When the Bill is divided, as noted earlier, the title of each Part will refer to the principal Act being amended.

Clause 2 is the commencement clause and provides that the Bill comes into force on the day that is 1 month after the date on which it receives the Royal assent. When the Bill is divided, as noted earlier, this commencement clause will be repeated in each separate Bill.

Part 1
Amendments to Government Communications Security Bureau Act 2003

Clause 3 provides that this Part amends the Government Communications Security Bureau Act 2003.

Clause 4 amends section 3, which specifies the purpose of the Act. The amendments substitute *new paragraphs (c) to (e)*. They have been recast to be consistent with changes in terminology being made.

Clause 5 amends section 4, which defines terms used in the Act. The amendments repeal certain definitions, amend other definitions, and insert new definitions.

The new definition of incidentally obtained intelligence is important in relation to *new section 14* inserted by *clause 12* and to *new section 25* inserted by *clause 24*.

The new definition of information infrastructure is inserted to take the place of the repealed definition of computer system. The new definition includes any medium through or in which communications are carried or stored and includes the communications themselves.

Clause 6 replaces sections 7 and 8 with *new sections 7 to 8D*.

New section 7 states the objective of the Government Communications Security Bureau (the **Bureau**).

New section 8 provides that the functions of the Bureau set out in *new sections 8A to 8C* are not to be taken as specifying any order of importance or priority. It also clarifies that 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.

New section 8A sets out the function of the Bureau in relation to information assurance and cybersecurity.

New section 8B sets out the function of the Bureau in relation to gathering and analysing intelligence about the capabilities, intentions, and activities of foreign persons and foreign organisations, and in relation to gathering and analysing intelligence about information infrastructures.

New section 8C sets out the function of the Bureau in relation to co-operation with certain other entities to facilitate the performance

of their functions. *New subsection (2)* provides limits on the extent of the co-operation provided, but clarifies that the co-operation may be provided even though the advice and assistance provided 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.

New section 8D gives the Director all the powers that are necessary or desirable for the purpose of performing the functions of the Bureau, but this is subject to the Act, any other enactment, and the general law.

Clause 7 replaces section 9 with *new sections 9 to 9D* dealing with the appointment of the Director, the appointment process, remuneration and conditions of appointment, removal from office, and review of the Director's performance.

Clause 8 amends section 11, which makes it an offence for current or past employees of the Bureau to unlawfully disclose information gained in connection with the Bureau. The amendments increase the maximum penalties from 2 years' to 3 years' imprisonment and from a $2,000 to a $5,000 fine.

Clause 9 amends section 12, which provides for the Bureau's annual report. The amendments are drafting amendments.

Clause 10 replaces the Part 3 heading to update terminology and reflect that the Part deals with both intercepting communications and accessing information infrastructures.

Clause 11 replaces section 13, which sets out the purpose of Part 3. The purpose is recast to be consistent with the recasting of the Bureau's functions and with amendments made to other provisions in Part 3.

Clause 12 replaces section 14, which provides that interceptions are not to target New Zealand citizens or permanent residents of New Zealand. The *new section 14* is expressly linked to the Bureau's intelligence-gathering function in *new section 8B* and provides that any incidentally obtained intelligence is not obtained in breach of *new section 8B*, but must not be retained or disclosed except in accordance with section 23 and *new section 25*.

Clause 13 amends section 15, which prohibits, unless authorised, the connecting or installing of interception devices. The amendments are

technical to reflect the change in terminology from computer systems to information infrastructures.

Clause 14 inserts *new sections 15A and 15B*.

New section 15A provides for the Director, for the purpose of performing the Bureau's functions under *new section 8A or 8B*, to apply to the Minister for an interception warrant to intercept communications or an access authorisation to access information infrastructures. The new section sets out the matters that the Minister must be satisfied about before issuing a warrant or an authorisation.

New section 15B requires the Commissioner of Security Warrants (appointed under the New Zealand Security Intelligence Service Act 1969) to be involved if anything that may be done under a warrant or an authorisation issued under *new section 15A* is for the purpose of intercepting the private communications of a New Zealand citizen or permanent resident of New Zealand under *new section 8A* or *new section 8B* to the extent that intercepting the person's private communications under that section is not precluded by *new section 14*.

Clause 15 amends section 16, which permits certain interceptions without an interception warrant or an access authorisation.

The amendments—

- specify that the section applies to interceptions for the purposes of the Bureau's functions in *new sections 8A and 8B*:
- specify that it does not authorise the interception of private communications of New Zealand citizens or permanent residents of New Zealand.

Clause 16 repeals section 17 and the cross-heading above section 17. Section 17 has been assimilated into *new section 15A* inserted by *clause 14*.

Clause 17 amends section 18, which provides for certain matters about interception warrants. The amendments widen the application of the section to include access authorisations.

Clause 18 replaces section 19 with *new sections 19 and 19A*. *New section 19* requires the Director to keep a register of interception warrants and access authorisations that have been issued. *New section 19A* provides for the urgent issue of interception warrants or access authorisations by the Attorney-General, the Minister of Defence, or the Minister of Foreign Affairs if the Minister is unavailable and it is necessary to issue them before the Minister is available.

Clause 19 makes a drafting amendment to section 20.

Clause 20 replaces section 21 with a new section that confers immunity from civil and criminal liability for certain things done under the Act if done in good faith and in a reasonable manner.

Clauses 21 to 23 make drafting amendments to sections 22, 23, and 24 respectively.

Clause 24 replaces section 25. The new section specifies when and to whom incidentally obtained intelligence about New Zealand citizens or permanent New Zealand residents may be retained and communicated. The ground in the current section 25 of preventing or detecting serious crime in New Zealand or any other country is retained and the following 2 new grounds are added:

- preventing or responding to threats to human life in New Zealand or any other country:
- identifying, preventing, or responding to threats or potential threats to the national security of New Zealand or any other country.

Clause 25 inserts *new sections 25A and 25B* dealing with the protection and disclosure of personal information. *New section 25A* requires the Director, in consultation with the Inspector-General of Intelligence and Security and the Privacy Commissioner, to formulate a policy on the protection and disclosure of personal information that complies with the principles set out in *new section 25B*. *New section 25B* sets out the principles about collecting, using, storing, and retaining personal information.

Clause 26 makes consequential amendments to other Acts as set out in the *Schedule*.

Part 2
Amendments to Inspector-General of Intelligence and Security Act 1996

Clause 27 provides that this Part amends the Inspector-General of Intelligence and Security Act 1996.

Clause 28 amends section 2(1), which contains definitions of terms, and inserts a definition of Deputy Inspector-General.

Clause 29 replaces section 5 with *new section 5*, which provides for the appointment of an Inspector-General of Intelligence and Se-

curity and a Deputy Inspector-General of Intelligence and Security. The Deputy Inspector-General has all the powers and functions of the Inspector-General, subject to the control and direction of the Inspector-General. The Deputy Inspector-General has all the powers and functions of the Inspector-General if there is a vacancy in the office of the Inspector-General or if the Inspector-General is absent from duty for any reason.

Clause 30 amends section 6, which provides for the Inspector-General's term of office. The amendments—

- add a reference to the Deputy Inspector-General:
- provide a maximum term of appointment of 3 years for each:
- provide that each can be reappointed, but in the case of the Inspector-General only once.

Clause 31 amends section 11, which specifies the functions of the Inspector-General. The amendments replace subsection (1)(c), (d), and (da) with new paragraphs. Paragraph (c) is replaced with 2 new paragraphs. The effect of this is to permit the Inspector-General to inquire into the propriety of particular activities of an intelligence and security agency without needing the agreement of the Minister.

Paragraphs (d) and (da) are replaced with 2 new paragraphs. *New paragraph (d)* requires the Inspector-General to review, at intervals of not more than 12 months,—

- the effectiveness and appropriateness of procedures adopted by each intelligence and security agency to ensure compliance with its governing legislation in relation to the issue and execution of warrants and authorisations:
- the effectiveness and appropriateness of compliance systems concerning operational activity, including supporting policies and practices of each intelligence and security agency relating to certain matters, including risk management and legal compliance generally.

New paragraph (da) requires the Inspector-General to conduct unscheduled audits of the procedures and compliance systems described in *new paragraph (d)*.

This clause also repeals section 11(2). That subsection placed limitations on the ability of the Inspector-General to do anything of his or her own motion in relation to a complaint about any activity of an intelligence and security agency.

Clause 32 amends section 12, which authorises the Inspector-General to consult certain public office holders and disclose information necessary for that purpose.

The effect of the amendments is to add a reference to the Independent Police Conduct Authority as one of the public offices that may be consulted.

Clause 33 amends section 15 consequential on the amendments to section 12.

Clause 34 amends section 25, which specifies what the Inspector-General must do on completing an inquiry. The amendments—

- require the Minister to provide his or her response to the report to the Inspector-General and the chief executive of the intelligence and security agency concerned:
- permit the Minister to provide his or her response to the Intelligence and Security Committee.

These amendments do not apply to the extent that a report relates to employment matters or security clearance issues.

Clause 35 inserts *new section 25A*, which requires the Director-General, as soon as practicable after forwarding a report as required under section 25(1), to make a copy of the report publicly available on an Internet site maintained by the Inspector-General. The new section specifies matters that must not be disclosed in the report made available under this section.

Clause 36 amends section 27, which provides for the Inspector-General's annual report. The amendments—

- require the Inspector-General to certify whether each intelligence and security agency's compliance systems are sound:
- require the Inspector-General, as soon as practicable after his or her annual report is presented to Parliament, to make a copy of his or her report (as presented to Parliament) publicly available on an Internet site maintained by the Inspector-General.

Part 3
Amendments to Intelligence and Security Committee Act 1996

Clause 37 provides that this Part amends the Intelligence and Security Committee Act 1996.

Clause 38 amends section 6, which specifies the functions of the Committee. Section 6(1)(e) specifies one of the Committee's functions to be to report to the House of Representatives on the activities of the Committee. The amendment substitutes a *new paragraph (e)*, which requires the Committee to present an annual report to the House of Representatives and to make an annual report publicly available on the Internet site of the New Zealand Parliament.

Clause 39 inserts *new section 7A*, which contains further provisions about the chairperson of the Committee. The new section provides—

- that the Prime Minister is not to chair a meeting of the Committee while it is discussing, in the course of a financial review of an intelligence and security agency, any matter relating to the performance of the intelligence and security agency if the Prime Minister is the responsible Minister of the agency. In that case, one of the members of the Committee appointed under section 7(1)(c) must act as chairperson:
- that the chairperson of the Committee may appoint either the Deputy Prime Minister or the Attorney-General (if not already a member of the Committee) to act as chairperson in the absence of the chairperson.

Clause 40 makes amendments to section 18 that are consequential on the amendment made by *clause 38*.

Rt Hon John Key

Government Communications Security Bureau and Related Legislation Amendment Bill

Government Bill

Contents

The Parliament of New Zealand enacts as follows:

1 Title

This Act is the Government Communications Security Bureau and Related Legislation 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.

Part 1
Amendments to Government Communications Security Bureau Act 2003

3 Principal Act

This **Part** 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 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 to the following on anything done under **paragraphs (a) and (b)** and any intelligence gathered as a result:

"(i) the Minister; and

"(ii) any person or office holder (whether in New Zealand or overseas) authorised by the Minister to receive the report.

"**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 communicate 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; and

"(d) any department (within the meaning of the Public Finance Act 1989) specified for the purposes of this section by the Governor-General by Order in Council made on the recommendation of the Minister.

"(2) To avoid doubt, the Bureau may perform its function under **subsection (1)**—

"(a) to the extent that the advice and assistance is provided for the purpose of activities that the entities may lawfully undertake; and

"(b) subject to 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.

"**8D 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."

7 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."

8 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".

9 Section 12 amended (Annual report)

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

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

10 Part 3 heading replaced

Replace the Part 3 heading with:

"**Part 3**

"**Intercepting communications and accessing information infrastructures**".

11 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."

12 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**."

13 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".

14 New sections 15A and 15B 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 **sections 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."

15 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**."

16 Section 17 and cross-heading repealed

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

17 Section 18 amended (Persons acting under warrant)

(1) In the heading to section 18, after "**warrant**", insert "**or access authorisation**".

(2) Replace section 18(1) with:

"(1) Every interception warrant and access authorisation must specify the person or class of persons who may make the interception or obtain the access authorised by the warrant or the authorisation."

(3) In section 18(2),—

(a) after "A warrant", insert "or an authorisation"; and

(b) after "the warrant", insert "or authorisation".

(4) In section 18(3), after "warrant", insert "or authorisation".

(5) In section 18(4),—

(a) after "a warrant", insert "or an authorisation"; and

(b) after "the warrant", insert "or the authorisation".

18 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 each interception warrant and access authorisation issued under this Part:

"(a) the date of issue:

"(b) the period for which the warrant or authorisation is issued:

"(c) the function or functions of the Bureau to which the warrant or authorisation relates:

"(d) in the case of a warrant, the interception device or interception devices specified:

"(e) in the case of an authorisation,—

"(i) any person specified in the authorisation:

"(ii) any place specified in the authorisation:

"(iii) the information infrastructure or information infrastructures specified in the authorisation:

"(iv) any conditions specified in the authorisation.

"(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.

"*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."

19 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**".

20 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."

21 Section 22 amended (Term of warrant or authorisation)

In section 22(1), delete "computer".

22 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**".

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

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

24 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 responding to threats to human life in New Zealand or any other country:

"(c) identifying, preventing, or responding to threats or potential threats to the national security 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 other person that the Director thinks fit to receive the information."

25 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; and

"(c) the Director to advise the Privacy Commissioner of the results of audits conducted under the policy.

"(3) The Director must regularly review the policy 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."

26 Consequential amendments

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

Part 2
Amendments to Inspector-General of Intelligence and Security Act 1996

27 Principal Act

This **Part** amends the Inspector-General of Intelligence and Security Act 1996 (the **principal Act**).

28 Section 2 amended (Interpretation)

In section 2(1), insert in its appropriate alphabetical order:

"**Deputy Inspector-General** means the Deputy Inspector-General of Intelligence and Security holding office under **section 5**".

29 Section 5 and cross-heading replaced

Replace section 5 and the cross-heading above section 5 with:

"Inspector-General and Deputy Inspector-General of Intelligence and Security

"5 Inspector-General and Deputy Inspector-General of Intelligence and Security

"(1) There must be—

"(a) an Inspector-General of Intelligence and Security; and

"(b) a Deputy Inspector-General of Intelligence and Security.

"(2) The Inspector-General and Deputy Inspector-General must be appointed by the Governor-General on the recommendation of the Prime Minister following consultation with the Intelligence and Security Committee established by section 5 of the Intelligence and Security Committee Act 1996.

"(3) The Deputy Inspector-General has and may exercise and perform the powers and functions of the Inspector-General (whether under this Act or any other enactment), but subject to—

"(a) the control and direction of the Inspector-General; and

"(b) to avoid doubt, the same duties, obligations, restrictions, and terms under which the Inspector-General exercises and performs his or her powers and functions.

"(4) Sections 7 to 9 and 18 apply to the Deputy Inspector-General as if references in those sections to the Inspector-General were references to the Deputy Inspector-General.

"(5) 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 exercise and perform all the powers, functions, and duties of the Inspector-General for as long as the vacancy or absence continues.

"(6) The fact that the Deputy Inspector-General exercises or performs any power, function, or duty of the Inspector-General is, in the absence of proof to the contrary, conclusive evidence of the Deputy Inspector-General's authority to do so."

30 Section 6 amended (Term of office)

(1) Replace section 6(1) with:

"(1) Every person appointed as the Inspector-General or Deputy Inspector-General—
"(a) is to be appointed for a term not exceeding 3 years; and
"(b) may be reappointed, but in the case of the Inspector-General only once."

(2) In section 6(2) and (3), after "Inspector-General", insert "or Deputy Inspector-General" in each place.

31 Section 11 amended (Functions of Inspector-General)

(1) Replace section 11(1)(c), (d), and (da) with:

"(c) to inquire at the request of the Minister or the Prime Minister or of the Inspector-General's own motion, but subject to the concurrence of the Minister, into any matter where it appears that a New Zealand person has been or may be adversely affected by any act, omission, practice, policy, or procedure of an intelligence and security agency:

"(ca) to inquire at the request of the Minister or the Prime Minister or of the Inspector-General's own motion into the propriety of particular activities of an intelligence and security agency:

"(d) without limiting paragraph (a), to review at intervals of not more than 12 months—
"(i) the effectiveness and appropriateness of the procedures adopted by each intelligence and security agency to ensure compliance with its governing legislation in relation to the issue and execution of warrants and authorisations; and
"(ii) the effectiveness and appropriateness of compliance systems concerning operational activity, including all supporting policies and practices of an intelligence and security agency relating to—
"(A) administration; and
"(B) information management; and
"(C) risk management; and
"(D) legal compliance generally:

"(da) to conduct unscheduled audits of the procedures and compliance systems described in **paragraph (d)**:".

(2) Repeal section 11(2).

(3) In section 11(3), replace "(1)(c)(ii)" with "**(1)(ca)**".

32 Section 12 amended (Consultation)

Replace section 12(2) with:

"(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 under section 11; and

"(b) despite section 26(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 Controller and Auditor-General:

"(b) an Ombudsman:

"(c) the Privacy Commissioner:

"(d) a Human Rights Commissioner:

"(e) the Independent Police Conduct Authority."

33 Section 15 amended (Jurisdiction of courts and other agencies not affected)

In section 15(3), replace "or of the Privacy Commissioner" with ", the Privacy Commissioner, a Human Rights Commissioner, or the Independent Police Conduct Authority".

34 Section 25 amended (Reports in relation to inquiries)

After section 25(5), insert:

"(6) As soon as practicable after receiving a report from the Inspector-General, the Minister—

"(a) must provide his or her response to the Inspector-General and the chief executive of the intelligence and security agency concerned; and

"(b) may provide his or her response to the Intelligence and Security Committee established under section 5 of the Intelligence and Security Committee Act 1996.

"(7) **Subsection (6)** does not apply to the extent that a report relates to employment matters or security clearance issues."

35 New section 25A inserted (Publication of Inspector-General's reports under section 25)

After section 25, insert:

"**25A Publication of Inspector-General's reports under section 25**

"(1) As soon as practicable after forwarding a report as required by section 25(1), the Inspector-General must make a copy of 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 copy of a report made publicly available under **subsection (1)**, disclose—

"(a) information the public disclosure of which 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) information the public disclosure of which 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 chief executive, or any information from which the identity of such a person could reasonably be inferred; or

"(d) information the public disclosure of which would be likely to prejudice—

"(i) the continued discharge 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."

36 Section 27 amended (Reports by Inspector-General)

(1) After section 27(2)(b), insert:

"(ba) certify whether each intelligence and security agency's compliance systems are sound; and".

(2) In section 27(3), replace "lay a copy of the report before" with "present a copy of the report to".

(3) In section 27(4) and (6), replace "laid before" with "presented to".

(4) After section 27(6), insert:

"(6A) As soon as practicable after a copy of the 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."

Part 3
Amendments to Intelligence and Security Committee Act 1996

37 Principal Act

This **Part** amends the Intelligence and Security Committee Act 1996 (the **principal Act**).

38 Section 6 amended (Functions of Committee)

Replace section 6(1)(e) with:

"(e) subject to section 18,—

"(i) to present an annual report to the House of Representatives on the activities of the Committee; and

"(ii) to make an annual report publicly available on the Internet site of the New Zealand Parliament."

39 New section 7A inserted (Further provisions relating to chairperson)

After section 7, insert:

"**7A Further provisions relating to chairperson**

"(1) **Subsection (2)** applies 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 the intelligence and security agency; and

"(b) the Prime Minister is the responsible Minister under the legislation governing the intelligence security agency.

"(2) If the Prime Minister is chairing the meeting of the Committee at which the matter is discussed,—

"(a) the Prime Minister must not act as chairperson of the Committee; and

"(b) another member of the Committee nominated by the Prime Minister, being one of the 2 members appointed under section 7(1)(c), must act as chairperson.

"(3) The chairperson of the Committee may appoint either of the following (if not already a member of the Committee) to be an alternate chairperson to act as chairperson at the discretion of the chairperson in the absence of the chairperson at a meeting of the Committee:

"(a) the Deputy Prime Minister:

"(b) the Attorney-General."

40 Section 18 amended (Restrictions on reports to House of Representatives)

In section 18(1), replace "reporting" with "presenting an annual report or other report".

Schedule

s 26

Consequential amendments

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".

Wellington, New Zealand:
Published under the authority of the New Zealand Government—2013

This paper has been redacted for public release.

REGULATORY IMPACT STATEMENT

Government Communications Security Bureau Act Review

Agency Disclosure Statement

1. This regulatory impact statement has been prepared by the Department of Prime Minister and Cabinet with the Government Communications Security Bureau.
2. It provides an analysis of options to update and amend the Government Communications Security Bureau Act 2003 (the GCSB Act) to respond to the findings and recommendations of the recent review of compliance at GCSB carried out by Rebecca Kitteridge, and to respond to changes in GCSB's operating environment.
3. The analysis of options was conducted as part of a wider New Zealand Intelligence Community Policy and Legislation Review project, which included an existing review of the New Zealand Security Intelligence Service Act 1969 and a review of legislation providing for oversight mechanisms (the Intelligence and Security Committee Act 1996 and the Inspector-General of Intelligence and Security Act 1996). The analysis of options took into account the work on these other reviews, and the compliance review.
4. The GCSB Act contains intrusive state powers. Consequently any review of the GCSB Act will involve the consideration of human rights and privacy matters. Respect for human rights, and individual privacy and traditions of free speech in New Zealand were guiding principles in undertaking the review and developing recommendations.

Rajesh Chhana
Intelligence Co-ordination Group
Department of Prime Minister and Cabinet

22 March 2013

This paper has been redacted for public release.

Status quo and problem definition

5. The GCSB has a vital role to play in protecting the security and safety of New Zealanders. Together with the other New Zealand Intelligence Community agencies, the GCSB contributes to the protection of the national security of New Zealand.

6. The GCSB was continued and established as a department of State by the Government Communications Security Bureau Act 2003 (GCSB Act). The GCSB Act has not been amended since its enactment in 2003.

7. The GCSB Act sets out the objectives and functions of the GCSB, specifies the intrusive powers Parliament has necessarily provided to the GCSB to fulfill its functions and the related authorisation processes. The ability to exercise such powers comes with responsibility – responsibility to operate within the law and consequently to maintain the confidence of everyday New Zealanders.

8. In October 2012 Rebecca Kitteridge was seconded from the Cabinet Office to the GCSB to undertake a review of compliance at GCSB to provide assurance to the GCSB Director that the GCSB's activities are undertaken within its powers and that adequate safeguards are in place. Ms Kitteridge briefed officials working on the New Zealand Intelligence Community Policy and Legislation Review project about her review, and her findings have been taken into account in developing the proposals referred to in this paper.

9. Two broad problems with the GCSB Act have been identified. First, while the GCSB Act provides for and authorises its current activities, it is not easy to determine whether any given activity falls within the scope of the prescribed functions of the GCSB or not. A considerable amount of legal analysis about the interplay of different provisions within the GCSB Act is needed to arrive at any such conclusion.

10. This situation is not satisfactory. The foundation of effective oversight is having a clearly formulated and consistent statutory framework. The lack of such a framework makes management and oversight of the GSCB very difficult, having to rely as it does on extensive and complex analysis of the meaning of the GCSB Act. The only responsible course of action when dealing with intrusive powers is to make the legislation clearer and more transparent.

11. Second, since the enactment of the GCSB Act in 2003 there have been a number of changes in the threat environment facing New Zealand, particularly in the area of cyber security, and developments in the law relating to privacy and search and surveillance. The issues that require the GCSB Act to be updated can be summarised under four headings.

Changing information security requirements

12. The cyber environment continues to innovate at a remarkable pace, fueling economic growth and international trade opportunities. Consequently, there is an increasing shift of activity, both business and government, to that environment. To counter the threat to business and government information the Government launched the New Zealand Cyber Security Strategy in June 2011 (NZCSS).

13. The GCSB currently has as one of its core functions information security and assurance. [text removed] That is why, as part of the NZCSS, the National Cyber Security Centre

(NCSC) was created within the GCSB. The Cabinet has indicated its expectation that the GCSB will considerably enhance its cyber security capabilities and use its expertise to assist a range of organisations (government, state sector, critical national infrastructure providers, and key economic contributors). However, the implementation of the NCSC has highlighted limitations on the ability of GCSB to contribute to this work because of the provisions of the GCSB Act (for example it is not clear that the GCSB can provide advice and assistance to private sector entities in New Zealand).

14. The impact of cyber threats is difficult to quantify precisely, but the NZCSS sets out some of the potential impacts, as well as some estimates suggesting New Zealanders lose up to $500m annually due to cyber-borne frauds and scams. Recent statistics on the NCSC website indicate that in the last 12 months cyber crime against New Zealanders cost $625m, and the global cost was estimated at up to $460 billion.

15. More broadly, the monetized cost of loss of intellectual property as a result of cyber intrusions into private sector entities is exceptionally difficult to quantify, in part because companies are reluctant to report losses or may not even know their property has been stolen. However, based on the scale of intrusions and exfiltrations seen in other jurisdictions and the number of intrusions reported in New Zealand the potential costs to New Zealand of cyber-based industrial espionage are likely to be significant.

16. Internationally the trend has been described as shifting from "exploitation" to "disruption" and "destruction". In other words the cyber threat is changing from theft of personal and intellectual property, to denial of service attacks and destruction of computer networks.

17. The NCSC 2012 Incident Summary reported that there was a significant increase (from 90 to 134) in the number of reported serious attacks against New Zealand government agencies, critical national infrastructure and private sector organisations.

18. If a major attack was directed at government agencies, critical national infrastructure providers (for example telecommunications networks and water supply) or companies that drive New Zealand's economy, there could be significant disruption to commercial and personal activities. It would also put at risk New Zealand's political and business reputation.

Changing security environment

19. The security environment New Zealand faces today presents new challenges. Globalisation means that New Zealand is no longer as distant from security problems as it was in the past. Security issues are increasingly interconnected and national borders are less meaningful. The increasing level of innovation in the cyber environment and the ubiquity of internet-based services is giving rise to new security threats and vulnerabilities. The GCSB Act was enacted 10 years ago when cyber matters were less sophisticated and prominent.

Changing public law environment

20. The legal environment in which the GCSB Act is interpreted has developed since its enactment. The courts' consideration of law enforcement cases has provided further guidance about how intrusive state powers should be set out in statute, and highlight areas where powers may no longer be effective given the change in the telecommunications environment. For law enforcement agencies these issues were

reviewed comprehensively over a number of years, and were addressed in the Search and Surveillance Act 2012.

Better Public Services

21. In addition to the issues above, the GCSB plays a crucial role in the support of other government agencies, in particular the New Zealand Defence Force and the NZSIS. The GCSB also supports the New Zealand Police in the detection and investigation of serious crime. The GCSB's unique capabilities are an invaluable resource for those agencies to draw upon.

22. The GCSB Act review considered that in a small jurisdiction such as New Zealand we cannot afford to duplicate expensive and sophisticated assets, and there are limited numbers of people that can work with such assets. Consistent with the Better Public Services programme, the capabilities such as those developed or acquired by the GCSB, where appropriate and subject to necessary safeguards, should be available to assist in meeting key Government priorities. This too should be addressed in the update of the GCSB Act.

Objectives

23. The objectives of the GSCB Act review are:

    - To provide for greater and more effective oversight at all levels (internally by the Director, at ministerial level by the responsible Minister and externally by the Inspector-General and the Intelligence and Security Committee).
    - To enable the GCSB to respond to the changing security environment, cyber and information security environment, and the changes in the public law environment since the GCSB Act was passed in 2003.

Regulatory Impact Analysis

24. Three policy options were assessed:

    - non-legislative solutions;
    - amending the GCSB Act;
    - repealing and replacing the GCSB Act.

Non-legislative solutions

25. As noted above the GCSB Act is a piece of legislation that sets out and provides safeguards for the use of intrusive state powers. The GCSB cannot address any new threats beyond those it is permitted to address in its legislation.

26. The difficulties associated with the interpretation of the GCSB Act could be addressed by developing detailed guidance material, but it would be of limited benefit and consume considerable time and expenditure on legal advice to develop. This would not substantially address the need to improve management and external oversight of the GSCB.

27. Non-legislative solutions cannot satisfactorily meet the two objectives.

This paper has been redacted for public release.

Amending the GCSB Act

28. The GCSB Act currently provides for three functions;

    - Foreign intelligence
    - Information security and assurance
    - Co-operation and assistance to other entities

29. The two objectives could be met by updating and clarifying the current functions set out in the GCSB Act. It is not considered that any new functions need to be added, but a refresh of the way in which the functions are articulated would ensure that the functions fit the changing operational environment, as well as providing greater clarity about what GCSB's functions actually are. These changes would complement and amplify the proposals to strengthen oversight by the Inspector-General of Intelligence and Security.

30. In the case of the foreign intelligence and cooperation functions, both would need to be clarified to allow for more effective oversight, and in the case of co-operation a ministerial authorisation process could be included in the GCSB Act to provide a way of determining who GCSB can work with and under what circumstances.

31. The information security and assurance function in the GCSB Act focuses almost entirely on providing protective services to public sector entities. However, threats in the cyber environment also put at grave risk our critical infrastructure and businesses that drive our economy. This function needs to be given more prominence. So too the expectations of the GCSB in safeguarding New Zealand information, in both public and private sectors, needs to be made clear.

32. The GCSB Act currently sets out three types of powers:

    - Warrantless powers of interception and access
    - Interception warrants
    - Computer network access authorisations

33. These powers are contained in Part 3 of the GCSB Act along with other provisions that control the use of those powers.

34. The objective of greater and more effective oversight would be met by still requiring the current range of authorisations but amending the GCSB Act so the authorisation processes are more transparent and consistent.

35. In order to meet the second objective, while the range of powers available to the GCSB does not need to be expanded the GCSB Act would be amended to make it clear that the powers can be used for both the foreign intelligence function and the information security and assurance function. The powers are needed to support the information security and assurance function to give the GCSB the ability to respond effectively to emerging cyber threats against New Zealanders.

36. The basic premise underpinning the operations of the GCSB that it does not conduct foreign intelligence activities against New Zealanders will be retained (currently contained in section 14 of the GCSB Act). However, because the information security and assurance function is about protecting New Zealanders, an amendment will also be required to allow the GCSB to see who (namely New Zealand individuals and

companies) is being attacked. This would allow the GCSB to determine where the threats are being generated from and develop measures to counter those threats.

37. Finally, amendments could be made to update the description of the powers to accommodate changes in how communications are now carried and routed around the world. This would be similar to the work undertaken for law enforcement powers in the Search and Surveillance Act 2012.

38. The costs of developing and drafting the proposed amendments and implementing them fall on the Government. The GCSB Act applies to the operation of the GCSB consequently the costs are part of its core operating expenses, and no compliance costs for business arise.

39. This approach would have the following outcomes and benefits:

Outcomes	**Benefits**
Greater clarity of the law governing the operation and administration of the GCSB	Provides basis for more effective oversight by external oversight bodies, thereby enhancing public trust and confidence.
	Responds to changes in the public law environment so that the law reflects current jurisprudence and is relevant to the current technological environment.
	Provides clarity to the public on the functions and powers of the GCSB.
	Provides clarity to staff and enhances management oversight of GCSB activities.
GSCB functions updated to allow GCSB to meet new threats, in particular cyber security.	Enables GCSB to support private sector in addition to public sector entities to counter cyber threats, which currently have an estimated impact on New Zealanders of over $0.50 billion in terms of cyber crime alone.
	Enables GCSB to more effectively detect and respond to cyber threats by allowing it to use the powers in the GCSB Act when undertaking its information security and assurance function.
	Allow GCSB to better fulfill the functions of the NCSC and play an effective part in the delivery of the NZCSS along with the other agencies tasked with its delivery.
GCSB able to assist and advise other Government agencies fulfill their lawful functions with its technical capabilities and	Other agencies will not have to duplicate technical capabilities and expertise already held by the Crown, and make effective and

expertise.	efficient use of the GCSB's capabilities.

Repealing and replacing the GCSB Act

40. The two objectives could be achieved by taking a more expansive approach to updating the GCSB's establishment statute, by repealing it and replacing it with a new statute.

41. The benefit of this approach, over and above the option to amend the GCSB Act, is that it would result in a new Act that would pick up the changes described in the discussion of the option to amend the GCSB Act as well as providing an opportunity to reenact all other existing provisions with updated drafting where necessary. However, as discussed above, the number of changes required to achieve the objectives can be targeted at particular parts and sections of the GCSB Act and the basic construction of the GCSB Act does not need to change to accommodate those amendments.

42. Consequently there does not seem to be any great benefit associated with dedicating additional time and resources to redrafting and re-enacting provisions that do not need to be changed.

Consultation

43. The policy development process was undertaken by the New Zealand Intelligence Community (DPMC – lead, with GCSB, and NZSIS). The agencies consulted were the Ministry of Foreign Affairs and Trade, New Zealand Defence Force, New Zealand Police, New Zealand Customs Service, Ministry of Defence, Ministry of Justice, Office of the Privacy Commissioner, State Services Commission and the Treasury.

44. Given the nature of the issues being dealt with and the national security classifications associated with the material, there was no public consultation process. Public consultation on the proposals will occur during the parliamentary consideration of the amending legislation.

Conclusions and recommendations

45. As discussed above, the identified problems do not require a change to the scheme of the GCSB Act and the objectives of the review can be met by amendments to targeted provisions. The benefits of dedicating resources to a full redrafting of the Act are consequently limited. The recommended option is to amend the GCSB Act to address the identified issues and meet the objectives of the reform.

Implementation

46. The compliance review of the GCSB has a range of recommended changes to the compliance framework and operations of the GCSB. The GCSB is developing an implementation plan to respond to those recommendations, and the implementation of the amendments to the GCSB Act will be incorporated into that plan.

Monitoring, Evaluation and Review

47. The GCSB will monitor the effectiveness of the amendments and advise the Minister about any issues arising.