DEPARTMENT
of the PRIME MINISTER
and CABINET

Departmental Report for the Intelligence and Security Committee

GOVERNMENT COMMUNICATIONS SECURITY BUREAU AND RELATED LEGISLATION AMENDMENT BILL

Intelligence Coordination Group

July 2013

Contents

Glossary

Bill	Government Communications Security Bureau and Related Legislation Amendment Bill
Bureau	Government Communications Security Bureau
Commissioner	Commissioner of Security Warrants
Committee	Intelligence and Security Committee
CSW	Commissioner of Security Warrants
Department	Department of the Prime Minister and Cabinet
Five Eyes	a term referring to the security partnership that exists between New Zealand, Australia, the United Kingdom, Canada and the United States of America
GCSB	Government Communications Security Bureau
GCSB Act	Government Communications Security Bureau Act 2003
IGIS	Inspector-General of Intelligence and Security
IGIS Act	Inspector-General of Intelligence and Security Act 1996
ISC	Intelligence and Security Committee
ISC Act	Intelligence and Security Committee Act 1996
Kitteridge Report	*Review of Compliance at the Government Communications Security Bureau* (Rebecca Kitteridge, March 2013
LAC	Legislation Advisory Committee
NCSC	National Cyber Security Centre (a unit within GCSB)
NZBORA	New Zealand Bill of Rights Act 1990
NZDF	New Zealand Defence Force
NZLS	New Zealand Law Society
NZSIS	New Zealand Security Intelligence Service
NZSIS Act	New Zealand Security Intelligence Service Act 1969
OIA	Official Information Act 1982
PDA	Protected Disclosures Act 2000

Introduction

1. This Report advises the Intelligence and Security Committee on the issues arising from submissions on the Government Communications Security Bureau and Related Legislation Amendment Bill.

2. The Report is divided into four parts:

   2.1. introduction (containing an overview of submissions on the Bill);

   2.2. commentary on general concerns about the Bill as a whole and the departmental response;

   2.3. commentary and the departmental response to issues raised on specific parts or clauses of the Bill;

   2.4. a summary of the recommendations in this Report.

3. A list of submissions is provided in the appendix to this Report.

Overview of submissions on the Bill

4. The Committee received 124 submissions on the Bill. Two submissions supported the Bill in principle (with either general or specific concerns), 13 submissions supported the purpose of the Bill (or the Bill in principle), but nothing more, 16 submissions supported those parts of the Bill that amend the Inspector-General of Intelligence and Security Act 1996 and the Intelligence and Security Committee Act 1996 (whilst opposing the remainder of the Bill and 3 of the 16 suggested that the Bill could go further), two submissions were neutral and 91 submissions opposed the Bill. Twenty-six submitters presented orally to the Committee.

Recommendations for amendment

5. Recommendations for amendment are made in the clause by clause analysis. They are presented as a consolidated list at the end of the report (see Summary of Recommendations). Any specific drafting proposals are subject to drafting advice from Parliamentary Counsel.

6. This Bill was introduced at the same time as the Telecommunications (Interception Capability and Security) Bill. The TICS Bill was referred to the Law and Order Committee with an instruction to report back to the House on or before 20 September 2013. There may need to be further consequential amendments to one or other of the bills to take into account any changes made as they pass through the parliamentary process.

General submissions on the Bill as a whole

7. Submitters' concerns about specific clauses or parts of the Bill are outlined in the detailed commentary on those specific clauses or parts.

Common concerns

8. The Department has identified a number of common concerns underlying the submissions generally that relate to the Bill in its entirety, or to general principles underlying the Bill. These were that:

    8.1. the Bill should be put on hold to provide more time for parliamentary consideration or for the Government to hold an independent inquiry;

    8.2. the Government should abolish the GCSB;

    8.3. the Bureau cannot be trusted to implement and follow the law;

    8.4. the Bill constitutes a considerable expansion of the powers of the Bureau;

    8.5. the Bill fails to strike the right balance between the need for national security, human rights, civil rights and privacy;

    8.6. the Bill contains insufficient safeguards;

    8.7. the Bill gives GCSB an objective that is too broad;

    8.8. there should be no spying on New Zealanders under any circumstances;

    8.9. co-operation with named New Zealand public entities should not be allowed (i.e. delete new section 8C);

    8.10. access to metadata should be protected in the same way as content;

    8.11. the Bill should require judicial authorisation of warrants, not Ministerial sign-off;

    8.12. the Five Eyes partnership is not in New Zealand's interest.

9. These overriding themes and the departmental response are discussed in the same order below.

Provide more time for parliamentary consideration or hold an independent inquiry

10. A number of submissions were concerned about the timeframe for submissions and the parliamentary process, given the subject matter of the Bill. Some submitters commented on the 2 month period for the ISC to consider the Bill, and the time made available for submissions. A number of submissions also raised concerns about the use of urgency (see for example submissions 5, 7, 9, 12, 13, 17, 19, 20, 25, 32, 43, 61, 84, 87, 92, 110, and 112).

11. Submitters argued that the passage of the Bill should be slowed to allow various reports emerging internationally, and judicial consideration of the Dotcom case to be completed and taken into account (see submissions 87 and 112).

12. Other submissions raise the desirability of holding an independent inquiry into the operation of New Zealand's intelligence agencies, and that the passage of the Bill should be put on hold until such an inquiry is completed (see for example submissions 31, 46, 58, 87, 89 and 112).

Comment

Proposed timeframe is necessary

13. The Government has proposed the Bill be passed under a tight timeframe given the need to put in place a robust and clear statutory framework under which the Bureau is able to operate. Effective oversight starts with a clearly formulated statutory framework. This will end the concerning situation of oversight bodies having to refer to interpretations of the GCSB Act being "arguable" rather than clearly prescribed.

14. Second, the need to move without delay is to reinstate a number of operations that have been put on hold due to the "arguable" nature of the legal framework. Examples of the work put on hold include assistance to the NZSIS in particular, assistance to the NZ Police and the implementation of information assurance and cybersecurity operations to protect New Zealand government departments, critical national infrastructure providers, and organisations of significance to New Zealand.

15. However, despite the need to act without delay, the Government concluded that given the issues addressed by the public input and a select committee process was necessary. The time required to undertake that process was carefully considered and a report date of 26 July 2013 was established. This allowed for a 4 week (later extended to 5 weeks) submission period, which falls within the usual 4 – 6 week submission period adopted by select committees. Meetings of the ISC were planned and scheduled to allow the ISC to undertake its consideration of submissions, advice and deliberate. This included resolving to hold the hearing of submissions in public.

Use of urgency

16. Some submitters have mistakenly concluded that the Bill will be passed under urgency. That is not correct. The use of urgency was limited to the first reading of the Bill and its referral to select committee. A full draft of the Bill was released by the Prime Minister on Monday 6 May 2013, and the Bill (unchanged from the draft) was formally tabled and read a first time on Wednesday, 8 May 2013. The debate was not curtailed in any way.

Independent inquiry

17. While a number of submitters referred to an independent inquiry, few had specific suggestions for what should be included in the terms of reference and there were a wide variety of views from those who did suggest matters to be reviewed. Matters to which submitters referred included organisational structure, legislation

governing the agencies, “illegal spying”, oversight mechanisms, and international relationships. One submitter also suggested the merger of the NZSIS and the Bureau should be considered.

18. There have also been a number of recent reviews relating to the operation and function of the New Zealand Intelligence Community. They include the reviews conducted by Michael Wintringham, Simon Murdoch, and the Kitteridge Report. In addition a PIF review of the intelligence agencies is underway.

19. The Bill is focused and narrow in terms of its scope and deals with matters of immediate concern. As noted above it provides a clear and robust statutory framework for the operations of the Bureau. The amendments do not seek to change the status quo in terms of the core roles and responsibilities of the Bureau and NZSIS. The amendments, in fact, strengthen controls on how the Bureau works with other agencies and subject the Bureau and NZSIS to greater oversight.

20. The enactment of this Bill does not preclude a wider consideration of the matters raised by submitters in the future nor does it pre-empt any future decisions or prevent any future recommendations from being made and implemented.

Abolish GCSB

21. A number of submitters advocated that GCSB should be abolished, with varying reasons given (see, for example, submissions 19, 20, 30, 44 and 119). Some submitters felt that GCSB had betrayed public trust and confidence to a degree that was beyond recovery, others felt that the organisation was solely serving international interests and not New Zealand interests (with many references to the Five Eyes or Echelon partnership), others considered that the GCSB lacked the capability to perform its role and still others rejected GCSB as the epitome of a totalitarian world that relied on pervasive State surveillance.

22. Related to the submissions above, some submitters also expressed the view that the functions currently performed by GCSB should be split between the NZSIS and/or the Police (see, for example, submissions 30, 68, 69, 70, 80, 82 and 119).

23. One submitter proposed that GCSB be merged with the New Zealand Security and Intelligence Service, as well as the National Assessments Bureau and the Intelligence Co-ordination Group (both currently within the Department of the Prime Minister and Cabinet), as a means of rationalising a disproportionately large intelligence community for a country the size of New Zealand (see submission 90).

Comment

24. Events over the last 18 months have almost certainly reduced public trust and confidence in GCSB, as reflected in the submissions described above. Some well-documented operational issues, combined with sustained media interest (driven by events here and in relation to intelligence agencies overseas), a necessary degree of operational secrecy and two recent independent reports examining aspects of legal compliance by the Bureau, have contributed to a deleterious public image and kept the public firmly focussed on the Bureau’s shortcomings.

25. That said, as noted in the recent *Review of Compliance at the Government Communications Security Bureau* (Rebecca Kitteridge, March 2013), GCSB "…plays a vital role in New Zealand's security….New Zealand needs this organisation now more than ever. The increasing threat of cyber attacks and the protective role GCSB plays is one part of this story, but the GCSB does a wide range of other things that are essential to the well-being of New Zealand" (at page 5). This view has been borne out by some of the submissions received (including the Privacy Commissioner), which (despite criticism of various aspects of the Bill) have acknowledged to varying degrees the important role played by GCSB and accepted there were a number of advantages it was able to provide (see, for example, submissions 70, 87, 90, 98, 115, 117, 120).

26. As the report highlights, GCSB undertakes many activities that benefit New Zealand and the country's need for a foreign intelligence and information assurance/cybersecurity agency is not seriously in doubt. Nations throughout history have relied on having access to such services to guard against threats to their sovereignty and physical borders, and also to shore up their long-term survival on the international stage. This is particularly the case in relation to matters of national security, international affairs and trade. The need for these services has not reduced over time. Indeed, in New Zealand's case, the use of cyberspace as a vector for espionage, intellectual property theft, cyber-crime and potentially sabotage, makes the case for GCSB more compelling than ever. Nations across the globe undertake foreign intelligence and possess some degree of signals intelligence capability.

27. Any erosion in public trust and confidence is regrettable. However, GCSB is demonstrating its commitment to improvement through its response to the Kitteridge Report. This includes a comprehensive change programme based on the recommendations in that report, as well as the publication of a regular report charting its progress in implementing the Kitteridge recommendations.

28. Separately, this Bill will introduce a number of new measures, such as increased powers and resourcing for the Office of the Inspector-General of Intelligence and Security and a new register of warrants, to bolster public confidence and once more engender public trust in GCSB. Other measures to increase transparency and oversight of the New Zealand intelligence community generally are detailed elsewhere in this Report.

Bureau not trusted to implement and follow the law

29. A number of submitters have raised concerns about the ability of the Bureau to follow the rules placed on its operations. Many submitters referred to reports about the Kim Dotcom case and the Review of Compliance at the GCSB prepared by Rebecca Kitteridge (the Compliance Review), and concluded that the Bureau could not be trusted to operate in way that complies with the law.

30. Other submitters, during their oral presentations (submissions 7, 36, 88), commented on their interactions with the Bureau. They commented on the professionalism of Bureau employees, the fact that they were dedicated public servants, and the respect they had for the work that they were doing.

Comment

31. The Compliance Review highlighted a number of issues about the operation of the Bureau, and made 80 recommendations for change and improvement. Four of the recommendations related to external oversight and legislation, with the remaining 76 recommendations focused on the work of the Bureau. The recommendations can be grouped under seven broad headings:

    31.1. compliance framework and activities;

    31.2. oversight;

    31.3. information management;

    31.4. legal capability and capacity;

    31.5. measurement and reporting;

    31.6. organisational structure and culture;

    31.7. outreach capability and capacity.

32. The Director has made the response to the recommendations a top priority for the Bureau during the 2013/2014 financial year, and has committed to making quarterly progress reports publicly available. The first progress report was released on 30 June 2013, with the next report due to be published on 30 September 2013.

33. Good progress has been made in responding to the recommendations, with 25 implemented and 11 on track to be implemented during the next quarter.

34. Work is also underway to respond to the requirements of the enhanced external oversight proposed by the Bill, and establish systems to comply with statutory registers of activity.

35. In addition, the Bureau, along with the NZSIS and the security related units of DPMC will be undergoing a Performance Improvement Framework (PIF) review. This will complement the work underway to implement with Compliance Review recommendations, and the wider efforts to bed in the changes made by the Intelligence Community Shared Services (ICSS) model. The PIF review final report, like other government departments, will be published when completed.

36. The need to demonstrably improve compliance at the Bureau is a recognised priority and steady progress is being made, with the intention of having as many essential recommendations (in particular the compliance framework, legal capacity, external oversight and information management) implemented prior to the enactment and coming into force of this Bill. Together with the enhanced external oversight mechanisms, it will mean that the Bureau will be well placed to demonstrate that it abides by the law and other public service requirements to the responsible Minister, Inspector-General and ISC.

37. This can then be demonstrated to the public through the greater reporting provided by the Inspector-General and the requirement on the Inspector-General to certify whether each intelligence agency's compliance systems are sound. The

Director is also committed to continuing the quarterly reports on implementation until the programme of work is complete, and the PIF Review when published will also provide further assurance of the work underway to ensure compliance.

Concern about "expansion" of functions and powers

38. A number of submitters commented, in writing and during the oral hearings, that the Bill represented an expansion of functions and powers of GCSB. The comments included that the expansion was unnecessary, that there was no justification for the expansion, and that the functions were being changed (see, for example, submissions 1, 2, 10, 14, 15, 17, 19, 20, 24, 26, 27, 29, 34, 38, 52, 54-60, 81, 84, 88, 89, 91, 93, 95-99, 101-105, 108, 109, 112 and 116).

Comment

39. The purposes of the changes to the GCSB Act are threefold:

    39.1. to provide for a clearly formulated and consistent statutory framework;

    39.2. 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 ISC);

    39.3. to update the GCSB Act to respond to the changing security environment, cyber environment, and information security needs.

40. The changes to the GCSB Act contained in the Bill are not revolutionary. They do not involve a fundamental change to the construction of the GCSB Act or the principles under pinning it.

41. Currently the GCSB Act provides for three functions:

    41.1. foreign intelligence – see section 8(1)(a) – (d) of the GCSB Act;

    41.2. information assurance and cybersecurity – see section 8(1)(e)(i) of the GCSB Act;

    41.3. co-operation and assistance to other entities – see section 8(1)(e)(ii) and section 8(2) of the GCSB Act.

42. These three functions are retained, but the descriptions are clarified to allow for more effective oversight, and updated to respond to the changing operational environment.

43. The GCSB Act confers three types of powers:

    43.1. interception of communication without warrant in limited situations;

    43.2. interception of communications under warrant;

    43.3. access to a computer system under a computer access authorisation.

44. This construction continues to provide the basic tools the Bureau needs to perform its functions. However the language used to describe the powers has

been updated to take into account changes in technology, and the warrant and authorisation provisions have been combined to ensure that the same framework applies to both. The Bill also makes it clear that the powers can be used for both the cybersecurity and foreign intelligence functions, but not the function of assisting other agencies, subject to appropriate controls and limitations.

45. The basic premise underpinning the operations of the Bureau is that it does not conduct foreign intelligence activities against New Zealanders. The repeal of this basic premise was not contemplated by Ministers at any time. However the way it was incorporated into the GCSB Act (section 14) is less than ideal, and meant that it applied to not only the foreign intelligence function but also the information assurance and co-operation functions. Application of the basic premise to those functions means that the Bureau would not be able to deliver those functions.

46. New wording is proposed to preserve the basic premise and clarify that it only applies to GCSB's foreign intelligence function, and not to its information assurance and cooperation functions. As an additional safeguard, interception of New Zealanders communications can only take place under the information assurance function under warrants jointly issued by the Minister and CSW, and in the case of cooperation only if the limited list of requesting agencies has lawful authority to carry out the interception.

Balance between national security and human rights, civil rights, and privacy

47. A number of submissions (see for example submissions 21, 24, 25, 28, 45, 47, 59, 110, 112 and 113) are concerned about the balance between the needs of national security on one hand, and civil and human rights, and privacy interests on the other. A number of submitters disagree with the advice provided to the Attorney-General that the Bill complies with the New Zealand Bill of Rights Act 1990.

48. The NZLS (submission 84) respectfully takes a different view to the Crown Law advice and believes that the Bill is inconsistent with the rights to freedom of expression and freedom from unreasonable search or seizure, and with privacy interests recognised by New Zealand law.

Comment

49. Respect for human rights, individual privacy and traditions of free speech in New Zealand were guiding principles in undertaking the review of the GCSB Act and developing recommendations for legislative change.

50. However, in developing legislation for intelligence agencies some qualifications to these basic principles need to be considered. The approach taken was that any qualifications must be shown to be necessary, and the functions and powers must operate within a framework of a carefully formulated and consistent policy along with robust external oversight measures.

51. The CLO determined that the Bill raises questions in respect of the rights to freedom of expression, non-discrimination and against unreasonable search and seizure affirmed by sections 14, 19(1) and 21 of the NZBORA. These were the same provisions identified by submitters.

52. The advice from the Crown Law Office to the Attorney-General sets out a careful analysis of those issues, taking into account domestic and international case law, and concluded that the Bill appears consistent with that Act.

53. On that basis the Department believes that the Bill does comply with the rights affirmed by the NZBORA. In fact, additional safeguards have been added to the GCSB Act by this Bill, including greater oversight of interception of communications involving New Zealanders, and providing greater regulation of the Bureau's function of providing assistance to other domestic agencies.

54. Some submitters compared the powers of interception made available to law enforcement with those of intelligence agencies, and question why "probable cause" and "judicial authorisation is not required. There is a distinction to be drawn between law enforcement and intelligence gathering, and a different approach needs to be taken to each given the different focus of each role. This too was considered in the CLO advice and international case law affirming the appropriateness of different approaches was discussed. The issue of judicial versus ministerial authorisation of intelligence warrants is discussed below, as is the role to be played by the Commissioner for Security Warrants in the application for, and issue of, warrants and authorisations (see the commentary on new section 15B, found in clause 14 of the Bill).

The Bill contains insufficient safeguards

55. Whilst several submitters were supportive of the proposed amendments to oversight legislation and indicated that the proposals would strengthen public confidence (see, for example, submissions 34, 49, 57, 58, 69, 84, 86, 103, 110, 112, 113, 115, 117, 118, 119 and 122), a large number had concerns about the extent and effectiveness of the oversight regime (see, for example, submissions 1, 27, 44, 49, 50-52, 54-56, 60, 64, 69, 72, 73, 80, 83, 92, 95, 97, 102, 108, 109, 112, 116, 118, 120, 121, 122, 123 and 124).

56. A number of submitters expressed general concerns about the adequacy of safeguards and oversight arrangements and identified that appropriate checks and balances need to be established when providing the GCSB with surveillance powers.

57. There were various specific suggestions for amendment to the oversight legislation to strengthen its effectiveness, which have been addressed in the clause by clause analysis. This section provides an overview of the enhanced oversight regime proposed by the Bill.

Comment

58. The Bill puts in place more robust and effective safeguards and oversight mechanisms in two ways. First, by providing for a clearly formulated and consistent statutory framework, and second by enhancing the external oversight mechanisms that apply to the Bureau and NZSIS.

59. In addition, GCSB's internal management and oversight is being strengthened, through the implementation of the Kitteridge Report recommendations. This is discussed further in the section on the Bureau not being trusted to implement and follow the law.

Clear and consistent statutory framework

60. The foundation of effective safeguards and oversight regime is having a clearly formulated and consistent statutory framework. The current lack of such a framework makes management and oversight of the Bureau very difficult, having to rely as it does on extensive and complex analysis of the GCSB Act.

61. The Bill removes inconsistency and contradictions between various provisions, makes it very clear what the three functions of the Bureau involve, and provides a consistent statement on powers, and clarifies the nature and application of the limitations on the use of those powers. This will avoid the unfortunate situation of there being multiple and "arguable" interpretations.

Enhanced external oversight regime

62. The Bill has been designed to build on and further strengthen existing oversight arrangements. Effective oversight of the intelligence and security agencies is important for assuring New Zealanders that the agencies continues to operate in accordance with the law, including in a manner consistent with privacy and human rights values embedded in New Zealand legislation.

63. Previous Parliaments have specifically configured the existing system of governance and accountability arrangements (embodied in the GCSB, IGIS, NZSIS and ISC Acts) to be effective in a necessarily covert environment. These special arrangements substitute for mainstream state sector performance oversight processes.

64. These accountability and oversight arrangements are established at several different levels:

    64.1. the accountabilities of the GCSB Director (internal oversight and safeguards);

    64.2. the role of the responsible Minister in providing policy direction and Ministerial oversight;

    64.3. the role of the IGIS (independent external oversight);

    64.4. the role of the ISC in providing Parliamentary oversight of policy, administration, and expenditure of the intelligence agencies.

65. While these measures substitute for some mainstream oversight mechanisms, additional performance oversight continues to be provided in certain areas by the State Services Commissioner (organisational performance), Controller and Auditor General (probity and organisational performance), Privacy Commissioner (privacy), and Ombudsman (public accountability).

66. This multi-layered framework is consistent with international best practice. In particular similar oversight arrangements apply to the intelligence services in Australia and in the United Kingdom.

67. The Government carefully considered the oversight regime, and concluded that the structure and organisation of the regime was sound but specific enhancements were needed to address matters relating to transparency,

independence and perceived gaps. In addition to the amendments proposed in the Bill, the Government has made a commitment to ensure that the IGIS has the resources necessary to carry out the functions of that Office effectively and efficiently.

68. In summary the changes to strengthen the office of the IGIS are as follows:

68.1. the IGIS will have an extended the statutory work programme, which includes system-wide issues that impact on operational activity whilst also retaining a focus on warrants and authorisations;

68.2. the IGIS will be required to certify each year in his or her annual report that the compliance systems of the intelligence agencies are sound;

68.3. the IGIS will be able to initiate inquiries into matters of propriety without requiring concurrence by the Responsible Minister (thereby enabling the IGIS to undertake independent inquiries);

68.4. the Responsible Minister will be given explicit responsibility to respond to IGIS reports within a reasonable time-frame (and the Minister may choose to provide those responses to the ISC);

68.5. the IGIS will be expected to make unclassified versions of his or her reports public, with appropriate precautions also taken in respect of any privacy concerns;

68.6. the legislative requirement that the IGIS be a retired High Court Judge will be removed, to broaden the pool of potential candidates. The three year term will remain but any further reappointment will be restricted to allow a maximum of one additional term;

68.7. a deputy IGIS will be appointed, on the same basis as the IGIS.

69. Changes to the way the ISC operates are also proposed, to improve its ability to provide oversight of the Bureau and NZSIS:

69.1. the Prime Minister will be required to relinquish the ISC chair (to one of his or her existing nominees on that Committee) when the Committee is discussing the performance of an agency (in the course of conducting a financial review) for which the Prime Minister is the Responsible Minister;

69.2. as a separate measure, the Prime Minister will be permitted to nominate either the Deputy Prime Minister or the Attorney-General to act as an alternate chair of the Committee, at times and for periods of his or her choosing, even when that alternate is not already a member of the ISC;

69.3. 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 via a website;

70. In addition to these legislative changes the Department of the Prime Minister and Cabinet has been directed to discuss with ISC members how best the Department could support the Committee's work.

Policy on privacy

71. The Bill will create new obligations for the Bureau in respect of the handling of personal information, based on the principles under the Privacy Act. Under section 57 of the Privacy Act 1993, the Bureau (and NZSIS) are exempt from all privacy principles except principles 6 (access to personal information), 7 (correction of personal information) and 12 (unique identifiers). The Law Commission recommended, in its June 2011 review of the Privacy Act, that the Act be amended to make a further four principles applicable to the intelligence agencies:

    71.1. principle 1 (purpose of collection of personal information);

    71.2. principle 5 (storage and security of personal information);

    71.3. principle 8 (accuracy of personal information to be checked before use);

    71.4. principle 9 (agency not to keep personal information for longer than necessary).

72. Due to the unique requirements of national security and the nature of intelligence gathering it was considered best to require the Bureau, in consultation with the IGIS and Privacy Commissioner, to formulate a policy that recognises the principles to the extent possible, with such modifications as may be necessary. Compliance will be regularly audited, with results communicated to the Privacy Commissioner. The policy will also be reviewed on a regular basis and updated as required.

Scope of the objective of the Bureau

73. A number of submissions (see for example submissions 49, 51, 52, 54, 55, 109 and 115) were concerned about the reference to "economic wellbeing" and "international relations" in the objective of the Bureau. Some submitters expressed the view that economic wellbeing was and international relations were the responsibility of New Zealand's diplomats and the Bureau had no role to play in such matters. They submitted that the objective of the Bureau should, therefore, be confined to national security alone.

74. Other submissions commented on the breadth of the term "national security" and referenced publication on the DPMC website *New Zealand National Security System* which sets out a wide ranging statement of what the concept of national security encompasses.

Comment

75. The references to economic wellbeing and international relations are not new concepts. The current objective of the Bureau in section 7 of the GCSB Act refers to the "international relations of the Government of New Zealand" and to "New Zealand's international well-being or economic well-being".

76. In common with most other nations, New Zealand needs the widest possible sources of intelligence to support its defence, trade and international policies.

New Zealand also needs to make sure that its own classified and sensitive information is protected from unauthorised access and exploitation.

77. Consistent with these needs, the objective of the Bureau in new section 7 reads:

> *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.*

78. It is important to note that the Bureau's objective is to contribute to, not be responsible for, national security, economic wellbeing and international relations as some submitters seem to believe.

79. All three matters that are listed need to be specified as the intelligence gathered by the Bureau is used to inform decisions-makers who are responsible for those matters. Intelligence about trade is important to our trade policies and matters relevant to international relations contribute to diplomatic engagements with other nations. Intelligence contributes to these activities and helps those responsible for those matters discharge their functions more effectively.

80. The following example, provided by Sir Geoffrey Palmer in "Securing our Nations Safety" published in 2000, illustrates how the Bureau's intelligence contributed to both New Zealand's national security (in the broad sense), international relations and economic wellbeing:

> *In 1989 and 1990 as Prime Minister and Minister for the Environment, I launched a campaign against driftnet fishing. In those years, New Zealand devoted substantial diplomatic and political resource to stopping this practice. Japan, Taiwan and the Republic of Korea all had large driftnet fleets working in the Pacific. Albacore tuna was the main commercial target in the South Pacific driftnet fishery. This is a species that was at risk of becoming depleted.*
>
> *New Zealand spoke out against the practice at the United Nations and established an initiative through the Pacific Forum to negotiate a regional convention banning driftnetting in the South Pacific.*
>
> *This was not an easy campaign because albacore tuna are valuable. They could, at that time, fetch US$1,000 per tonne in the United States. Short-term gain was very attractive for the driftnet fishers.*
>
> *A conference was held in Wellington in November 1989 that resulted in the successful completion of an international convention among all the 22 participating South Pacific countries and territories to ban driftnets in the South Pacific. In December 1989 a United Nations resolution was also passed against the practice.*
>
> *In the campaign against driftnet fishing some of the nations whose fishing fleets were operating in the South Pacific were prone to deny the problem was serious, or at least as serious as New Zealand argued. But the king hit for New Zealand was specific and detailed intelligence provided by GCSB concerning the activities of those fishing boats, which disclosed the extent of their catches. That meant the New Zealand Government had correct facts upon which to base its campaign. The facts could not credibly be denied.*
>
> *The campaign was successful. The Wellington Convention entered into force on 17 May 1991. Its effect was to prohibit driftnet fishing on the high seas and in the Exclusive Economic Zones of countries lying within a large area of the Pacific defined by the convention. The important gains of this treaty were greatly assisted by sound intelligence. And that is just one example.*

81. New Zealand needs independent sources of information on which to base its foreign policy, its defence posture, and its wider economic and trade policies. A significant source of such information is derived from the interception by the Bureau of the communications of foreign entities.

No spying on New Zealanders

82. A broad theme common to a substantial number of the submissions received was a general call to 'stop GCSB spying on New Zealanders'. This theme encompassed not only opposition to the co-operation permitted by new section 8C as detailed later in this Report, but also GCSB's information assurance and cybersecurity role under new section 8A, and its ability to target New Zealanders who come within the definitions of "foreign person" or "foreign organisation" for the purpose of its foreign intelligence role under new section 8B (see, for example, submissions 5-7, 9, 12, 13, 16, 39, 42, 44, 49, 51, 52, 54-57, 60, 63-65, 67-69, 72, 76, 80, 83, 84, 91-93, 97-99, 102, 103, 105, 113, 115-117, 119 and 122-124).

83. A small number of submitters also proposed that GCSB's cybersecurity role should be taken off GCSB and undertaken by a separate agency (see, for example, submissions 70, 108, 120).

84. In its oral presentation, the New Zealand Law Society (submission 84) expressed the view that more detail was needed in relation to the actual activities of GCSB, in order to assess the extent to which the privacy of New Zealanders was at risk and design adequate controls to mitigate this risk.

Comment

<u>New section 8A</u>

85. New section 8A builds on an existing function of GCSB and gives the Bureau responsibility for using 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), on matters relating to the protection, security and integrity of communications and information infrastructures of importance to the Government.

86. Information assurance and cybersecurity services are critical for modern governments, because they help to mitigate the threat posed by malicious actors in the cyber environment. This is important as communication channels, personal interactions, business transactions and data storage increasingly shift online, thereby exposing users and participants to the risk that vulnerabilities in online platforms and hardware will be exploited by third parties to the detriment of those users and participants.

87. At the same time as this shift to online services is occurring, globally there is increased reporting of cybersecurity threats (see, for example, the NCSC incident report for 2012), with the potential to inflict damage on a large scale. New Zealand, like the rest of the developed world, requires a coherent strategy and well-developed tools to protect the assets at greatest risk from such threats. Essentially this means protecting the communications, the information conveyed by such communications, the intellectual property shared by such

communications and the information and intellectual property stored on information infrastructures of importance to the government.

88. To give this practical effect, when attacks on New Zealand communications or key information infrastructures occur, the entity charged with protection needs to be able to examine the target of the attacks (essentially the New Zealand 'victim'), in order to understand how network and other vulnerabilities are being exploited. Such examination may also involve monitoring of the victim's computer and related communications. If such victim analysis cannot occur, the protective function is significantly curtailed, if not rendered nugatory for the individual/entity concerned. It also significantly hampers GCSB's ability to build up a wider 'threat picture' and protect other individuals and entities from similar attacks. This is not surveillance of New Zealanders for its own sake, or for the sake of domestic intelligence at all; this is essential analysis that enables GCSB to protect New Zealand and New Zealanders.

89. GCSB already has information assurance as one of its core functions, and it is uniquely placed with its advanced capabilities developed through its intelligence work to contribute to responses to cybersecurity issues. New section 8A is, therefore, a key government platform for protecting the assets at greatest risk from cybersecurity threats.

90. Locating the information assurance and cybersecurity function in another agency would require duplication of effort and, thus, a greater (and inefficient) call on scarce public funds, due to the fact that GCSB will have an ongoing need for the same assets and capabilities to service its foreign intelligence function in new section 8B.

91. There is also a valid question as to whether those responsible for defensive and protective work under new section 8A might ultimately lose currency in the evolution of cyber exploitation techniques, if the information assurance and cybersecurity part of GCSB were to be separated from the foreign intelligence gathering part of the business. Whilst the skills needed for each function are different, there is no doubt that some degree of cross-pollination occurs, with each side better able to perform its allotted role by learning from the techniques and methodologies of the other. Thus, understanding the ways and means of New Zealand's foreign intelligence collection also enriches New Zealand's ability to subvert attempts by an adversary to achieve the same outcome (and vice versa). This dynamic is perhaps best captured by the motto of GCSB's Australian counterpart, the Australian Signals Directorate, which is "Reveal Their Secrets – Protect Our Own".

92. Regarding the view expressed by the NZLS that more detail is needed here and in new sections 8B and 8C in relation to the actual activities of GCSB, officials have considered this proposal but, on balance, have determined that the Bill provides the right level of detail as drafted. Following recent events overseas, there have been public reports of adversaries changing their behaviour in response to the public release of detailed information regarding the activities of the National Security Agency (see, for example, "Al Qaeda Changing Tactics After NSA Leaks" published in *The Huffington Post*, 8 July 2013).

New section 8B

93. New section 8B contains GCSB's foreign intelligence gathering function and generally cannot be used to deliberately undertake surveillance of New Zealanders by reason of amended section 14. This provision prohibits GCSB from targeting the private communications of New Zealand citizens or permanent residents, *unless and to the extent that the person comes within the definition of "foreign person" or "foreign organisation"* in section 4 of the Act.

94. Together, the twin arms of the exception noted above are referred to colloquially as "agents of a foreign power" and these individuals can be legitimately targeted for surveillance as legitimate and deliberate exceptions to section 14, because of known roles acting at the direction of a foreign person or foreign organisation.

95. This exception aside, under section 8B surveillance can only be done for the purpose of gathering intelligence, in accordance with the government's requirements, *about the capabilities, intentions, and activities of foreign persons and foreign organisations*. In other words, this surveillance is not a law enforcement activity. It is not even focussed on the *agent* of the foreign power per se. The limited surveillance of New Zealanders that is authorised by this provision is solely for the purpose of discovering information about third party *foreign* persons and *foreign* organisations – it just so happens that a particular type of New Zealander (the agent of the foreign power) is able to provide the lens for that discovery to occur.

96. In any event, there is an important safeguard at play here, in the form of the Commissioner of Security Warrants, who (among other things) must be involved in the application for, and the issue of, a warrant or authorisation under new section 8B that targets a New Zealander who is an agent of a foreign power. This is discussed in more detail later in this Report in relation to new section 15B (found in clause 14 of the Bill).

New section 8C

97. New section 8C is discussed separately below.

No co-operation with named New Zealand entities (new section 8C)

98. A number of submissions were strongly in favour of preventing GCSB from co-operating with the New Zealand Police, the New Zealand Defence Force and the New Zealand Security Intelligence Service (essentially, removing new section 8C from the Bill).

99. Submitters noted that allowing GCSB to undertake this role would allow it to "spy on New Zealanders", which they believed to be fundamentally wrong and outside the scope of what they considered to be GCSB's 'core' role – that of providing foreign intelligence (see, for example, submissions 5, 6, 7, 9, 12, 13, 26, 39, 56, 72, 92, 95, 116, 118, 122 and 123). The New Zealand Law Society (submission 84) expressed the view that (at paragraph 29):

> *…if the GCSB is called upon to assist another specified agency (such as the Police) by performing activities instead of that other agency, the activities performed by the GCSB in that capacity will receive the imprimatur and secrecy and immunity protections of the GCSB Act, when the same activities engaged in by the specified other agency itself would not do so in*

terms of the other agency's empowering legislation. In that way, enlistment of GCSB "co-operation" may confer on the activities undertaken a protected legal status which they would not otherwise receive.

100. A small number of submitters also suggested that the three other agencies in question should be permitted to develop their own surveillance capabilities (see, for example, submissions 56 and 72).

101. A small number of submitters, including the LAC, suggested placing restrictions on section 8C, such the development of criteria as to the type of agency that may be assisted and when, or requiring that co-operation only occur under the oversight of the Commissioner for Security Warrants (see, for example, submissions 22, 91 and 93).

Comment

102. New section 8C allows GCSB to co-operate with, and provide advice and assistance to, each of the New Zealand Police, the New Zealand Defence Force and the New Zealand Security Intelligence Service, "for the purpose of facilitating the performance of their functions" in limited circumstances only, as outlined in the statute.

103. Co-operation may only occur to the extent that the advice and assistance is provided for the purpose of activities that the requesting entity may lawfully undertake itself. This means that the requesting entity will need to have a very clear mandate (i.e. in the form of a warrant, or statutory or other form of legal authority) to undertake an activity before GCSB will agree to act on its behalf. If the requesting entity is currently not permitted by law to undertake surveillance in a given set of circumstances, this Bill will not change that important starting position.

104. Co-operation will also be subject to the same limitations, restrictions and protections under which the requesting entity performs its functions and exercises its powers. This means that, contrary to the view expressed by the New Zealand Law Society (submission 84), GCSB will not be able to "perform any activities that it chooses" under section 8C (at paragraph 28 of the submission). Once GCSB has agreed to assist, it will be acting under the direction of the requesting agency and will not have carte blanche to select targets, direct operations, or otherwise act at will.

105. Contrary also to the view of the NZLS (submission 84) and echoed by InternetNZ (submission 120), the activities performed by the GCSB under section 8C will *not* "receive the imprimatur and secrecy and immunity protections of the GCSB Act". It is clear from new section 8C(2) that in exercising this function, GCSB will be subject to the same regulatory regime that applies to the requesting entity. Moreover, the immunity provided to GCSB employees by new section 21 clearly applies only to warrants or authorisations under the GCSB Act. Thus, it will *not* apply to actions taken under new section 8C. Section 8C is intended as an efficient use of scarce (and expensive) resources (i.e. in the form of capability and assets), that will circumvent the need to duplicate the same capability and assets across multiple government agencies.

106. In essence, the policy underpinning new section 8C is an example of Better Public Services in action. A need for such a provision was identified early on in

the legislation review process, due to the high end technological capability located within GCSB, which needs to be called upon in a limited number of circumstances involving sophisticated threats. GCSB's role is as the agent of the requesting entity and will consist of assisting that entity to go about its lawful activities. It is acknowledged that at least two of those entities are legally able to undertake surveillance of New Zealanders.

107. Whilst some submitters proposed allowing the three agencies listed in new section 8C(1) to develop their own surveillance capabilities, on balance, officials consider that confining this advanced capability to a single agency will act as a safeguard against burgeoning surveillance by an ever greater number of individual State agencies.

108. Some submitters have expressed frustration that no evidential basis (in the form of cost/benefit analysis or similar) has been provided in support of statements that it would be costly to duplicate the capabilities of the Bureau across other government departments.

109. Most government departments are able to work with other government departments where interests coincide and there is an advantage to the taxpayer of services being delivered in a co-ordinated way. A good example is the social sector, where the Ministries of Social Development, Health and Education work together closely. The Government is promoting greater collaboration under its Better Public Services policy, which includes legislative change to facilitate collaborative work.

110. In the case of agencies that have statutory powers and functions, to avoid any doubt and provide for safeguards in the exercise of powers and use of capabilities, the law needs to specify what the agency is able to do. For example, the NZDF is provided with a domestic role in instances of natural disaster, assisting the Department of Corrections and the Police. When and what powers the NZDF has in those situations is careful prescribed. Similarly, Police officers are designated Fisheries Officers to enable them to enforce the relevant regulations and exercise the necessary powers in relation to those regulations.

111. The Bureau, in performing its core functions of cyber security and foreign intelligence, has unique capabilities. They are costly to establish and maintain. Police, NZDF and NZSIS have their own capabilities to intercept communications and access information to support their functions and powers. However, in a small number of cases more advanced capabilities are required. The Kitteridge Report (at paragraphs 18 and 29) notes that since 2003 GCSB has assisted NZSIS on 55 occasions and the Police on 4 occasions. The assistance in those cases is important. In essence, duplicating those resources in Police, NZSIS and NZDF would involve expending a large proportion of GCSB's appropriation three times to cater for a handful of cases.

112. Some submitters also commented that in order to meet the needs of other agencies, GCSB would need to increase its resources. This is not correct. Whether assistance is provided or not is a matter for the Director to determine (see new section 8). That decision is subject to the oversight of the IGIS, who can also assess the propriety of those decisions. If other matters take precedence, or there are competing demands for resources, or for other good reason, the Director may decline to provide assistance.

113. Finally, the approach the Government is proposing, of holding the Crown's advanced capabilities in one agency for which a single Director is accountable, provides an additional safeguard for the public.

114. The fact that GCSB will be assisting other agencies to perform their legitimate roles is pertinent to the suggestion that co-operation only occur under the oversight of the Commissioner for Security Warrants. Section 8C has been crafted in such a way that when GCSB performs this function, it will be acting solely under the requesting agency's mandate – in whatever legal form that might take – and not its own. Thus, for example, in the case of the Police, this will likely involve a particular kind of warrant. If the requesting agency has a warrant or other mandate to undertake surveillance, then there is a reasonable argument to be made that that is all that is required. GCSB might need to consider its resourcing and priorities, but it does not also need approval to act as an agent of that other agency.

115. Importantly, GCSB will not 'own' or be able to control any of the information that is acquired as a result of the support it provides to a requesting entity. Such information will belong to the requesting entity and will need to be handled in accordance with the legal framework (i.e. both laws and policies) applying to that entity. Thus, for example, information acquired by GCSB when acting on behalf of the New Zealand Police will need to be handled in accordance with the detailed requirements of the Search and Surveillance Act 2012.

Access to metadata

116. A number of submitters expressed strong views against allowing GCSB to have access to the metadata of New Zealand citizens or permanent residents. They argue that, given its reach and the wide range of information that can be deduced as a result of metadata, it should be protected in the same way as content is protected under the legislation, i.e. under amended section 14 (see, for example, submissions 35, 43, 73, 91, 107, 108 and 116).

117. In the alternative, two submitters suggested that metadata collection should only occur under additional safeguards, such as a specific warrant (see submissions 36, 87 and 88). The Privacy Commissioner (submission 87) noted the importance of effective oversight to ensure that metadata was used appropriately.

118. One submitter proposed that the term "metadata" should be defined, for greater clarity and transparency (submission 36).

119. Keith Locke (submission 30) emphasised the need for greater discussion around GCSB's access to and use of metadata, before formalising any rules in this area.

Comment

<u>Provide the same protection as content</u>

120. The definition of "communication" in the GCSB Act, both currently and as amended by the Bill is necessarily very wide, due to the nature of GCSB's work and incorporates metadata as a result. To that extent, both content and metadata are treated exactly the same under the statutory framework. That said,

"metadata" does not explicitly feature in the Act and the Bill does not change this fact.

121. Content and metadata are also intended in the Bill to be treated exactly the same in terms of the protection offered by section 14. Under that provision (as amended), GCSB cannot "do anything for the purpose of intercepting the private communications of a person who is a New Zealand citizen or permanent resident". There is no separate test for metadata. Thus, in view of the definition of "private communication", in each case it will come down to a question of whether there is a reasonable expectation of interception (or, put conversely, a reasonable expectation of privacy)? In all likelihood, some metadata will not meet this test – but neither will some content.

122. Further discussion regarding the term "private communication" is found later in this Report, as part of the discussion on the amended interpretation section, set out in clause 5 of the Bill.

Include a definition of "metadata"

123. The term "metadata" is not commonly defined in any legislation in New Zealand – although the Telecommunications (Interception Capability) Act 2004 does define the narrower concept of "call associated data". This lack of definition has come about for three key reasons.

124. First, communications networks split "metadata" from content when a message is transmitted and the type of data that can be intercepted as metadata varies widely depending on the network and the interception tool being used. Second, there is currently no shared and widely held view on what "metadata" captures. Third (and related to the lack of a shared understanding), data that is not content, but which is generated as part of some automated process (e.g. a telephone call, the use of a swipe card, or the creation or transmission of an email), is constantly evolving, meaning any definition would be soon out of date.

125. This was ably demonstrated by Dr Joel Pitt (submission 45) in his oral presentation, when describing the ever increasing numbers of "devices" that connect to, and send signals/information over, the internet to a variety of possible recipients (e.g. the owner of the device and/or the installer of the device and/or the manufacturer of the device). Refrigerators and light bulbs were just two of the real life examples given.

Ministerial versus judicial authorisation of warrants

126. The LAC (submission 22) invited the ISC to consider establishing a judicial process for the issue of warrants relating to New Zealanders. Other submitters (see submissions 23, 35 and 37) also recommended that judicial authorisation should be the basis for any interception of communications by GCSB.

Comment

127. Executive involvement in the process of granting intelligence warrants aligns with the fundamental responsibility of government to protect the country from threats to national security, such as foreign inference and covert attempts to subvert democratic processes.

128. Since the enactment of legislation to govern their intelligence agencies, the United Kingdom, Australia and New Zealand have all retained the responsibly for issuing intelligence warrants with the Executive rather than assigning the function to the judiciary. In New Zealand and Australia the issuing authority is the relevant responsible Minister, and in the United Kingdom it is the relevant Secretary of State. Prior to the intelligence agency enactments in New Zealand (1969 in the case of the NZSIS and 1984 in the case of GCSB) the Executive power to intercept communications had no statutory basis.

129. Although starting at a similar point to that of the United Kingdom, Australia and New Zealand, Canada has now moved to a partial system of judicially-issued warrants for certain types of national security related surveillance. This judicial involvement arose in response to the Canadian Charter of Rights. In the Canadian system national-security related warrants are now issued by designated Federal Court Judges. The designated Judges operate in a completely secure environment designed specifically for hearing intelligence warrant applications, separate from the criminal or civil courts. Because of security requirements, the Canadian system incurs high financial costs.

130. This system of judicially issued warrants applies to warrants that are issued to the Canadian Security Intelligence Service (the equivalent of the NZSIS), but does not apply to the Communications Security Establishment Canada (the equivalent of the GCSB), which operates under a system of Ministerial authorisation similar to the system in New Zealand.

131. New Zealand has taken steps to provide additional protections for New Zealanders' privacy and human rights interests in a different manner to that adopted in Canada.

132. The Commissioner of Security Warrants was introduced in 1999 as a co-approver of NZSIS' domestic warrants alongside the Minister in Charge of the NZSIS. The CSW's role is to advise the Minister on NZSIS applications for warrants concerning New Zealanders, and to jointly issue the warrants. The addition of the CSW was made in response to a call for a greater level of independent input into the process, though the involvement of the Minister was retained because of the desire to retain a strong link to Ministerial accountability for surveillance associated with national security. The Commissioner of Security Warrants is required, by statute, to be a retired High Court Judge.

133. Section 15 of the Bill proposes to extend the involvement of the Commissioner of Security Warrants to include interception warrants or access authorisations if the authority is required by the GCSB for the purpose of intercepting the communications of New Zealand citizens or permanent residents. This extension mirrors the framework in the NZSIS Act that has existed since 1999 for domestic intelligence warrants. It will require review of certain GCSB warrant applications and access authorisation applications by the Commissioner of Security Warrants in a joint authorising role alongside the responsible minister. This change will ensure there is a strong focus on the relevant legal requirements.

Five Eyes partnership is not in New Zealand's interests

134. A substantial number of submitters are of the view that the international partnership referred to variously as the Five Eyes, Echelon and/or UKUSA

agreement is not in New Zealand's best interests and exists solely to advance international interests – those of the United States in particular (see, for example, submissions 19, 20, 27, 30, 41, 48, 50, 53, 54, 68, 69, 71, 78, 80, 82, 85, 112 and 119). Some of these submissions call for New Zealand to withdraw from the partnership.

135. On a related note, a number of submitters are concerned that the Bill gives GCSB too much freedom to share information it has gathered with international partners. These submitters are of the view that the Bill does not contain sufficient safeguards to either prevent GCSB from sharing information in respect of New Zealanders, or to prevent a particular partner from sharing information with the GCSB in respect of a New Zealander (see, for example, submissions 30, 70, 92, 95, 97 and 123). Most of these submitters propose that all sharing between the GCSB and any other international entity – Government or otherwise – must stop.

136. As well as a general desire to shut down the international partnership described above, many of these submitters are also concerned that unless there is a strict prohibition on the flow of information, GCSB will use its international networks to circumvent the domestic prohibition in amended section 14 of the Bill, which prohibits GCSB from targeting the private communications of New Zealand citizens or permanent residents, unless they are an agent of a foreign power (as described above).

Comment

Acting in New Zealand's interests

137. Many submitters appear to be unaware of the standard legal and constitutional restrictions that operate in respect of GCSB (and other government departments) and which ensure it remains focussed on New Zealand's interests, regardless of what partnerships it might form and agreements it might sign.

138. As a matter of constitutional principle, the operation of the Bureau (as a Department of State) is directed solely by the New Zealand Government. This is placed beyond doubt by section 32 of the State Sector Act 1988, which sets out the responsibilities of chief executives of government departments. Moreover, as stated in the Bill, and the current GCSB Act, GCSB acts in accordance with the Governments requirements in respect of foreign intelligence. These are in turn reflected in national intelligence priorities, which at an administrative level guide the deployment of resources across the New Zealand Intelligence Community.

139. The New Zealand-centric focus outlined above is emphasised in the Bill by way of the various references to New Zealand in the Bureau's statutory objective (found in new section 7), the emphasis on structures of importance to the Government of New Zealand (in new section 8A), the reference to the Government's requirements (in new section 8B), the restriction to New Zealand agencies regarding co-operation (in new section 8C) and the protection afforded New Zealand citizens and permanent residents (in amended section 14).

140. As is known, however, GCSB is also a member of a long-standing collaborative international partnership for the exchange of foreign intelligence and the sharing of communications security technology. The other members of the partnership are the USA's National Security Agency, the UK's Government Communications

Headquarters, Australia's Australian Signals Directorate and Canada's Communications Security Establishment.

141. New Zealand gains considerable benefit from this arrangement, as it would be impossible for New Zealand to generate the effectiveness of the five nation partnership on its own. Whilst GCSB is hampered in its ability to provide an evidence base for this assertion (due to the need for operational secrecy), a simple comparison with the significantly greater assets and resources of each of the five partners individually attests to the logic of this statement.

142. A former IGIS commented on this point precisely, in his annual report for the year ending June 1999, noting that (at pages 9 and 10):

> *There is a substantial balance in favour of New Zealand and its intelligence requirements in the collaboration and sharing of information and intelligence between the partners.*

143. As is the case for any other government department, however, GCSB must (and, indeed, does) remain focussed on New Zealand's interests, despite the fact of an agreement or arrangement with a public entity in another country. Whilst there are not many examples that can be publicly discussed, former Prime Minister Sir Geoffrey Palmer has provided one example concerning driftnet fishing in the South Pacific (see "Securing our Nations Safety", published in 2000 and mentioned elsewhere in this Report). It illustrates how the Bureau's intelligence contributes to each of New Zealand's national security, international relations and economic wellbeing.

144. If any Government of the day was unhappy with the direction being taken by GCSB, that Government has a number of levers available to it, to compel change and a refocusing of priorities. For example, the Government has the ability to engage in discussions with the chief executive (led by the Responsible Minister) to persuade on the need for change, to reset government priorities to provide greater emphasis in a given area, to adjust the conditions of employment of the chief executive to reflect new or altered priorities, to adjust appropriations year on year to the same effect, to utilise the oversight function of the Intelligence and Security Committee and, ultimately, to remove the chief executive by and through the State Services Commissioner (where a persistent failure to adhere to government direction is assessed as just cause).

<u>Controls on sharing of information gathered under section 8A</u>

145. The need for the information assurance and cybersecurity function found in section 8A has been discussed at length elsewhere in this Report. As part of this function, GCSB may indeed need to share information with international partners. They in turn share relevant information on advanced persistent cybersecurity threats with us. This is what helps both sides build up a comprehensive and credible threat picture – an understanding of the landscape and likely sources of attack – without which it would be difficult to formulate a defensive plan and sound mitigation strategies. These in turn enable New Zealand (and our partners) to act to prevent future attacks.

<u>Controls on sharing of information gathered under section 8B</u>

146. Turning to look at new section 8B, it bears repeating that amended section 14 is a prohibition on GCSB that applies to all foreign intelligence gathering activities

conducted under section 8B. According, GCSB will not hold information about a New Zealand citizen or permanent resident unless, either, that person is an agent of a foreign power, or the information was collected incidentally in the course of foreign intelligence gathering. Scope to share information in the latter category is limited by reference to purpose and recipient, as detailed in new sections 25(2) and (3) (found in clause 24 of the Bill).

147. Nor can GCSB request an agency of another country to intercept communications of New Zealand citizens or permanent residents with a view to then sharing in the resulting intelligence: any such request would itself constitute a violation of section 14 because it would equate to intelligence gathering by the GCSB – albeit put into effect by a partner acting on the Bureau's behalf.

148. As far as preventing other countries from gathering intelligence on New Zealand citizens and permanent residents is concerned, this Bill can have no effect. This Bill can only regulate activity within New Zealand and section 14 can only regulate GCSB. In this respect, the Bill is broadly framed. Section 14 would continue to prohibit the authorisation or doing of "anything" for the purpose of intercepting the private communications of New Zealand citizens or permanent residents. This is broad enough to extend to action by the Director or an employee of GCSB that might amount to approval of interception of New Zealand private communications, including tacit approval arising from sharing in the resulting intelligence.

<u>GCSB does not hold information gathered under section 8C</u>

149. In relation to new section 8C, as discussed elsewhere, GCSB will not own any information acquired as a result of the support it provides to a requesting entity. This information will be controlled by that entity and handled in accordance with the legal framework applying to that entity. GCSB will not be able to share such information with any other entity or individual, in New Zealand or overseas.

Preliminary provisions

Clauses 1 and 2

150. These clauses set out the title and commencement of the Bill.

Comment

151. No submissions were received on these clauses and no changes are recommended.

Part 1 – Amendments to the Government Communications Security Bureau Act 2003

152. This part contains amendments to the GCSB Act 2003.

Clause 4 – Section 3 amended (Purpose)

153. This clause amends section 3, which sets out the purpose of the GCSB Act. The section is amended to be consistent with changes in terminology being made.

Submissions

154. There were no submissions on the amendments however there was one submission suggesting an addition to the preliminary clauses of the GCSB Act.

155. The Legislation Advisory Committee (LAC)(submission 22) suggest that a statement of principles be added to the GCSB Act, similar to section 4AAA of the New Zealand Security Intelligence Service Act 1969 (NZSIS Act) which was inserted in 2011. The LAC also note that another consideration is whether there should be an express statement of political neutrality, as per section 4AA of the NZSIS Act.

Comment

156. The Bureau, unlike entities such as the NZSIS and the NZ Police, is listed in schedule 1 of the State Sector Act 1988 which means that it is a public service department and subject to all the provisions of the State Sector Act. In particular, the Code of Conduct issued by the State Services Commissioner applies to the Bureau and its staff. In addition, the Bureau must maintain policies and procedures that are consistent with it.

157. The standards of integrity and conduct set out in the Code of Conduct are:

157.1. fairness – including being professional and responsive, and striving to make a difference to the well-being of New Zealand and all its people;

157.2. impartiality – including maintaining the political neutrality required to enable us to work with current and future governments;

157.3. responsibility – including acting lawfully and objectively, using an organisation's resources carefully and only for intended purposes, and treating information with care and using it only for proper purposes;

157.4. trustworthiness – including being honest, ensuring actions are not affected by our personal interests or relationships, and working to the best of our abilities.

158. Consequently it would be duplicative and potentially confusing to include principles covering similar ground into the GCSB Act. The Code of Conduct is also updated from time to time to take into account emerging issues. Relying on specific statutory provisions could put the Bureau out of step with the rest of the core public service. The first Code of Conduct was issued in 2007 and it was most recently updated in 2010.

Recommendation

159. The Department does not recommend any change to this clause.

Clause 5 – Section 4 amended (Interpretation)

160. This clause repeals, inserts and amends definitions of some important terms in the Bill.

Definition of "information infrastructure"

161. Section 4 of the GCSB Act is amended to include the following definition:

> ***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.*

162. This definition replaces the repealed definition of "computer system". The term computer system has become outmoded, and the new definition takes into account the new ways in communications are now carried and stored. The new definition includes any medium through which or in which communications are carried or stored and includes the communications themselves.

Submissions

163. A number of submitters commented on the breadth of the term "information infrastructure". Others were concerned by the fact that the definition is non-exhaustive (by using the word "includes") rather than definitive (by using the word "means") (NZLS submission 84). They were also concerned that the term covered not only the emissions, systems or networks (infrastructure as commonly understood) but also the communications carried on, stored in, or relating to them.

164. Submitters felt that the broad nature of the term allowed the Bureau to intercept a far greater range of communication systems than previously was the case.

Comment

165. Submitters are correct, in that the term is broad and expansive to capture the broad and expansive range of systems that are used by people to communicate with each other. The functions of the Bureau are based on the collection of information through the interception of communications.

166. This amendment updates the Act consistent with its purpose of allowing the interception of communications. Communications are carried over a broad range of infrastructure and the Act needs to keep pace with that. The purpose and function is clear, and that should not be frustrated by the technology being used to carry communications not being caught by the language of the Act. This is important because, amongst other things, cybersecurity threats exploit changes to communications technology. Any doubt about whether communications on a certain type of infrastructure can be intercepted or accessed is removed. However, any access or interception will still be required to be authorised under the Act.

167. The use of an inclusive rather than an exhaustive list is to allow some flexibility to capture communication media that have yet to be developed. The pace of change in communications is considerable, and this provides the ability for the Act to keep pace with those changes in the medium term.

Recommendation

168. The Department does not recommend any changes to the definition of "information infrastructure".

Definition of "private communication"

169. The definition of "private communication" is already contained in the GCSB Act and is not amended by the Bill, but is now used in new section 14 in place of the undefined phrase "communication of a person".

Submissions

170. The LAC (submission 22) and the NZLS (submission 84) in their written and oral submissions raised some concerns about the nature of this definition. The LAC submitted that the term is technologically outmoded and may pose some interpretation difficulties. The LAC notes that the definition of this term was discussed in the Law Commission's 2010 report *Invasion of Privacy: Penalties and Remedies* (NZLC R113).

Comment

171. The Law Commission, in NZLC R113, considered the term "private communication" in the context of recommending a Surveillance Devices Act which would address criminal and civil liability in relation to unlawful surveillance. Such an Act would complement the Search and Surveillance Act 2012, which sets out the power of law enforcement to undertake surveillance activities. The Law Commission states explicitly that the criminal and civil offences they were recommending should not be inconsistent with the Search and Surveillance Act.

172. At paragraph 3.59 the Law Commission states that:

> *"Private communication" is a statutory term that has been used in New Zealand since 1978 and is also a familiar term in the listening device offences of the majority of Australian states and territories. While the current definition, by virtue of its longevity, has acquired a degree of orthodoxy, it is not straightforward and its difficulties have been judicially noted.*

173. After a detailed discussion taking into account case law and academic writing, the Law Commission concludes that "On balance, we prefer the option of restating the two current criteria as a single objective reasonable expectation of privacy test". The Commission goes on to recommend (Recommendation 10):

> *The definition of "private communication" for the purposes of the interception offences should be amended to replace the two current criteria with a single "reasonable expectation of privacy" test.*

174. As noted in the LAC's submission, the term is used in a wide variety of New Zealand statutes, and the Government is still considering the Law Commission's recommendations arising from its reports on Privacy. In addition, the consideration of "private communication" was in the context of developing a Surveillance Device Act rather than looking at law enforcement and intelligence powers.

175. The better approach in our view is to maintain the consistency across the statute book, particularly between the Crimes Act, Search and Surveillance Act and the GCSB Act, and look at any amendments after the Government's consideration of the Law Commission's recommendations is complete.

176. We recognise that the term "private communication" is not straightforward. However, it is being used in place of a more problematic phrase, "communications of a person", which has no developed jurisprudence or case law supporting it. Because the Government is still considering the wider implications of the Law Commission's recommendations and given that the term "has acquired a degree of orthodoxy" we do not recommend that it be amended by this Bill.

Recommendation

177. The Department does not recommend that the definition of "private communication" be amended by this Bill.

Clause 6 – Sections 7 and 8 replaced (Objective and functions of the Bureau)

178. This clause replaces sections 7 and 8 with several new clauses.

<u>New section 7 – Objective of the Bureau</u>

179. This section states the objective of the Bureau. It is based on its current objective, but simplified.

Submissions

180. A number of submitters raised concerns about the reference to the Bureau performing its functions to contribute to "economic wellbeing" and "international relations".

Comment

181. This is discussed above in the section on general themes.

Recommendation

182. The Department does not recommend any change to new section 7.

New section 8A – Information assurance and cybersecurity

183. Section 8A outlines GCSB's information assurance and cybersecurity function. It builds on GCSB's existing information assurance and cybersecurity function – permitting the Bureau to give advice and assistance to public sector agencies in New Zealand – whilst also clarifying that advice and assistance may be given to public authorities overseas (a source of some confusion in the current Act) and expanding the function it to explicitly include assistance to the private sector on the authorisation of the Responsible Minister.

Submissions

184. Many submitters raised concerns about this provision, describing it as allowing the Bureau to spy on New Zealanders and characterising it as a significant step along the path to transforming the Bureau from a foreign intelligence agency to one conducting a mix of foreign and domestic surveillance. In a similar vein, a number of submitters raised concerns regarding the implications of this function on New Zealand citizens' and permanent residents' right to privacy. Some submitters proposed separating this function out from the foreign intelligence function in new section 8B and locating it within a new agency, or transferring it to the New Zealand Police, or the New Zealand Security Intelligence Service.

Comment

185. These proposals are discussed above in the section on general themes. The Department does not recommend any change as a result of these concerns.

186. In addition, officials have undertaken a comparison of new sections 8A and 8B and consider that there would be value in ensuring consistency between the language used in these provisions (in particular, between new section 8A(c) and new section 8B(1)(c)). The current lack of uniformity is not ideal because these sections are intended to allow the same type of activity, albeit for two separate functions – i.e. the communication of intelligence gathered.

187. If the issue is not addressed, a court could determine that Parliament intended to allow two quite different activities under each one (i.e. "reporting" versus "analysing" and "communicating"). As currently drafted, a court might not only reasonably conclude that Parliament had intended these activities to be different, but also that Parliament had intended the term "intelligence" to have a narrow meaning, confined to raw material gathered. On the contrary, the Bill has been prepared on the premise that the term can be applied across all stages of the information-gathering process, from raw collect, to end product report.

Recommendation 1

188. The Department recommends that officials work with PCO to reconsider new section 8A(c) in light of new section 8B(1)(c) and develop any necessary amendments to better align these provisions.

New section 8B – Intelligence gathering and analysis

189. Section 8B outlines GCSB's foreign intelligence function. It is based on GCSB's existing foreign intelligence function – permitting the Bureau to perform a number of detailed tasks in the pursuit of intelligence collection and dissemination – whilst not going into the same level of detail as the existing Act.

190. The intention is to keep the function at a high level, with no reference to the individual steps required, so that there is flexibility to perform the foreign intelligence gathering function in any way necessary. The current Act is very process-driven, whereas, so long as it stays within the law, GCSB should be able to employ such processes (e.g. use such technology and skills) as are necessary to perform its function efficiently. Thus, for example, if some future advancement in technology results in the need to run another process over intercepted data in order to make it useable (i.e. some process that was unlike the deciphering, decoding and translating processes permitted now), that would be possible without throwing GCSB's entire legal mandate into question.

Submissions

191. Submissions received did not focus on the reduced level of detail in respect of GCSB's foreign intelligence function, although many stated generally that they were opposed to the Bill. Some submitters recognised the need for the State to have an agency that performed a foreign intelligence function, although there were mixed views on whether this should be performed by GCSB, or another agency. On a related note, some submitters explicitly proposed separating the foreign intelligence function out from the information assurance and cybersecurity function in new section 8A and locating it within a new agency, or transferring it to the New Zealand Police, or the New Zealand Security Intelligence Service.

Comment

192. These proposals are discussed above in the section on general themes.

Recommendation

193. The Department does not recommend any change to new section 8B.

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

194. Section 8C outlines GCSB's co-operation function, thereby clarifying what has been a vexed issue and the source of some confusion in the current Act.

Submissions

195. Many submitters were strongly opposed to the retention of this function and requested that it be removed from the Bill. In a similar vein to new section 8A, it was described as allowing the Bureau to spy on New Zealanders and seen as a significant step along the path to transforming the Bureau to a domestic surveillance agency. A number of submitters also raised concerns regarding the implications of this function on New Zealand citizens' and permanent residents' right to privacy. Some submitters suggested that the performance of this function should be carried out under the oversight of the Commissioner for Security Warrants.

Comment

196. These issues are discussed above in the section on general themes. Officials consider that some fine-tuning to the language of new section 8C(2) would be beneficial, to provide greater clarity regarding the limits and oversight applying to the Bureau when it exercises its section 8C function.

197. Officials also note that there is a some awkwardness of language in new section 8C(2)(b) between the opening words "subject to", which fits with those parts of the list that follows and which consist of controls on the Bureau, but not one part of the same list that is essentially a benefit to the Bureau, i.e. "protections". Officials consider that this should be addressed.

Recommendation 2

198. The Department recommends in relation to new section 8C that:

198.1. the opening words of subsection (2) be tightened by inserting "only" before "perform";

198.2. paragraph (2)(b) begin with the words "in accordance with" instead of "subject to";

198.3. PCO be asked to include a separate provision to the effect that any advice or assistance provided under section 8C(1) to another entity is subject to 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 co-operation with Police); and

198.4. PCO be asked to include a provision clarifying that it is intended that the IGIS would continue to have an oversight role in respect of activities undertaken by the Bureau under new section 8C.

<u>New section 8D – Director has full powers for purpose of performing Bureau's functions</u>

Submissions

199. Some submitters expressed a view that this provision further widened the scope of the Bureau's powers (see, for example, submission 93).

Comment

200. Section 8D is an avoidance of doubt provision and reflects section 34(2) of the State Sector Act 1988 which provides that:

> *The chief executive of a department shall have the powers necessary to carry out the functions, responsibilities, and duties imposed on that chief executive by or under this Act, as well as the powers necessary to carry out the functions, responsibilities, and duties imposed on that chief executive or that department by or under any other Act*

201. The effect of this provision is to ensure that the Director has the ability to carry out the day to day functions of the Bureau including the corporate and administrative duties that support the core functions of the Bureau. It does not in any way authorise the Director to act "beyond the law" – in fact section 8D expressly states that the section is subject to the GCSB Act, any other enactment and the general law. Any interception of communications can only occur if authorised under the Act.

Recommendation

202. The Department does not recommend any change to new section 8D.

Clause 7 – Section 9 replaced (Director of Bureau)

203. This clause replaces section 9 with new sections 9 to 9D dealing with the appointment of the Director.

204. This change gives effect to Cabinet's decision in 2010 that the appointment framework for the chief executive of the Bureau (and NZSIS) be adjusted to:

204.1. provide the State Services Commissioner with a statutory mandate to manage and advise on the selection process;

204.2. define the term of office of up to five years;

204.3. provide for the reappointment of chief executives; and

204.4. establish the role of the State Services Commissioner in setting conditions of service and the process for termination.

205. These decisions were given effect through non-legislative measures until such time as it was practicable to make the necessary legislative amendments.

Submissions

206. The Environment and Conservation Organisations of New Zealand (ECO) (submission 118) welcome the addition of these clauses and the involvement of the State Services Commissioner in the appointment process. However, ECO has recommended the following amendments:

206.1. the appointment and removal of the Director should be made on the joint recommendation of the Prime Minister and the Leader of the Opposition;

206.2. new section 9D be deleted because, in ECO's view, it would preclude the investigation of cases of illegal activity, such as the Dotcom case.

207. Professor Kevin Broughan (submission 106) recommended that the term of the director should be limited to a maximum of two terms.

Comment

208. Public servants and public service chief executives are part of the executive arm of government. The appointment of public service chief executives is, in most cases, made by the State Services Commissioner under the State Sector Act 1988. In some cases appointments are made on the recommendation of Ministers. In all cases the appointments are a matter for the executive. It would not be appropriate to involve members of the legislature in such matters.

209. New section 9D would not preclude an investigation of illegal activity. The purpose of the new section is to provide for a performance management regime which mirrors the State Service Commissioner's standard performance management regime for public service chief executives, subject to limitations regarding operational matters. Any operational matters would be investigated by the Inspector-General in the first instance, and any matters of illegality would ultimately be determined by the courts.

210. The number of terms of appointment will be addressed in the advice provided by the State Services Commissioner, as is the case of any other public service chief executive.

Recommendation

211. The Department does not recommend any change to clause 7.

Clause 8 – Section 11 amended (Prohibition on unauthorised disclosure of information)

212. This clause 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.

213. This amendment updates the maximum penalty for this offence in line with equivalent provisions elsewhere in the statute book, commensurate with the seriousness of disclosing information affecting national security and New Zealand's international reputation (see, for example, section 78A of the Crimes Act 1961).

Submissions

214. Annemarie Thorby (submission 44) recommends section 11 be deleted as the disclosure of information is already covered by the Protected Disclosures Act 2000 (PDA).

Comment

215. The offence in section 11 and the requirements of the PDA complement each other. There is a restriction on disclosure except in the course of a person's official duties unless authorised by the Minister. The PDA provides a mechanism

for concerned employees to alert their managers, the Director, Minister or Inspector-General as appropriate of any concerns about the operation of the Bureau. The Bureau, as required by the PDA, has a policy in place informing all employees of the PDA requirements and how they can make any disclosures.

Recommendation

216. The Department does not recommend any change to clause 8.

Clause 9 – Section 12 amended (Annual report)

217. This clause amends section 12, which provides for the Bureau's annual report. The amendments are drafting amendments.

Submissions

218. The Human Rights Foundation (submission 91) queried whether the change from "without delay" to "as soon as practicable" would result in the ISC being less effective in its oversight role.

Comment

219. The amendment is not intended to change the practice and procedure of the ISC. The change is a drafting matter to make this provision consistent with other statutory provisions that provide for the publication of reports. The proposed formulation is found in many statutes, including, for example, the Electoral Act 1993, Privacy Act 1993, Public Finance Act 1989, and the Search and Surveillance Act 2012.

Recommendation

220. The Department does not recommend any change to clause 9.

Clauses 10 and 11 – Part 3 heading and section 13 replaced (Purpose of Part)

221. These clauses are amended to be consistent with the recasting of the Bureau's functions and with amendments made to other provisions in Part 3.

Comment

222. No submissions were received on these clauses and the Department does not recommend any change to clauses 10 and 11.

Clause 12 – Section 14 replaced (Interceptions not to target domestic communications)

223. This clause replaces existing section 14 and outlines the protection that exists in respect of the private communications of New Zealand citizens and permanent residents when GCSB is performing its foreign intelligence function under new section 8B. It is closely based on the existing section 14 of the GCSB Act, but has been updated to clarify that it applies only to the foreign intelligence function in section 8B, and then only in respect of "private communications".

Submissions

224. Many submitters criticised the use of the phrase "private communications" in amended section 14, because of concerns about difficulties in interpretation. Some submitters described it as "circular" and bringing about the very outcome (permissible interception) that section 14 was intended to guard against in respect of New Zealand citizens and permanent residents. This is because of the test used i.e. "reasonable expectation of interception", and the context against which that test is set, i.e. legislation outlining permissible interception.

225. In a similar vein to new sections 8A and 8C, it was described as allowing the Bureau to spy on New Zealanders and seen as a significant step along the path to transforming the Bureau to a domestic surveillance agency. A number of submitters also raised concerns regarding the implications of this function on New Zealand citizens' and permanent residents' right to privacy.

Comment

226. These proposals are discussed above in the section on general themes.

Recommendation

227. The Department does not recommend any change to clause 12.

Clause 13 – Section 15 amended (Interceptions for which warrant or authorisation required)

228. This clause amends section 15, which describes the interceptions for which warrants or authorisations are required. The amendments are drafting amendments.

Comment

229. No submissions were received on this clause and no changes are recommended.

Clause 14 – New section 15A and 15B and cross-heading inserted (Authorisation to intercept communications or access information infrastructures)

230. This clause inserts new sections 15A and 15B, which together replace existing sections 17 and 19 regarding the issue of warrants and authorisations by the Minister and also create a new role for the Commissioner for Security Warrants.

<u>New section 15A – Authorisation to intercept communications or access information infrastructures</u>

231. Section 15A outlines the scope of the interception warrants and access authorisations that may be sought by the Director of GCSB.

232. As well as carrying over current types of warrant and authorisation permitted by existing sections 17 and 19, it also introduces several categories of class warrant. The existing standing conditions on warrants and authorisations have been combined and refreshed to reflect the structure of the new Bill, advancements in technology and additional safeguards, as well as to avoid unnecessary repetition

within the Bill. The current requirement to consult the Minister of Foreign Affairs has been retained, as has the ability of the Responsible Minister to impose additional conditions on a warrant or authorisation. Section 15A is also stated to apply "despite anything in any other Act".

Submissions

233. Many submitters have reacted strongly against new section 15A and proposed that the phrase "not otherwise lawfully obtainable" in subsection (1)(a) should be deleted from this provision (see, for example, submissions 5, 6, 7, 9, 12, 13, 18, 26, 39, 40, 56, 71, 72, 82, 95, 106, 112, 118, 119, 122 and 123).

234. A number of submitters have opposed the Responsible Minister's ability to issue warrants and authorisations suggesting that they should instead be issued by a Judge (see, for example, submissions 23, 35, 37, 120 and 122).

235. Submitters have also voiced opposition to subsection (5), which clarifies that section 15A is "applies despite anything in any other Act" and proposed that it also be deleted from the Bill. Particular mention was made of the fact that this would give section 15A primacy over the New Zealand Bill of Rights Act 1990 (see, for example, submissions 5, 6, 7, 9, 12, 13, 26, 39, 40, 56, 71, 72, 82, 95, 112, 118 and 122).

236. One submitter thought that warrants and authorisations that did not name a particular person should be "matters of public record" (submission 66).

Comment

237. The issue of judicial versus ministerial warrants is discussed above in the section on general themes.

238. Opposition to the phrase "not otherwise lawfully obtainable" in new section 15A(1)(a) appears to be based on a misapprehension as to the existing legislation, as well as the purpose for having such a phrase generally.

239. Section 17 of the GCSB Act already provides that "The Director may apply in writing to the Minister for the issue of an interception warrant authorising the use of interception devices to intercept communications *not otherwise lawfully obtainable by the Bureau*". Thus, the use of this phrase in section 15A is a straight carryover of an existing permission framework.

240. Furthermore, there is good reason to retain this phrase. First, it causes the Bureau to consider what other lawful means might be available to it in order to gain access to certain communications before seeking a warrant or authorisation to intercept such communications. Examples might include a request being made to an organisation or Government, or using search techniques across open source databases or publicly available information. Second, the phrase reflects the fact that, in the normal run of things, the interception of communications is illegal (as reflected in section 216B of the Crimes Act 1961) and that Parliament intended section 15A to be a permitted exception to the normal legal position.

241. Removal of the phrase from new section 15A(1)(a) would still enable the Bureau to seek Ministerial approval for a warrant or authorisation, just without the ring-fencing measures described above.

242. As regards section 15A(5), this provision has been inserted for the avoidance of doubt. It reflects the fact that the Bill explicitly empowers the Bureau to act in ways that otherwise are, or might be, contrary to various Acts of Parliament (for example, covert surveillance and the use of interception devices, planning for the same and thereby conspiring to commit offences) and otherwise places limits on various protected rights and freedoms. In view of the rights and freedoms at stake, the inclusion of such a provision seemed prudent. It also mirrors the position under section 4A of the New Zealand Security Intelligence Service Act 1969, which allows for the issue of intelligence warrants.

243. On the issue of having warrants and authorisations on the public record, existing sections 12(3)(b) and (c) of the GCSB Act require the Bureau to state in its annual report whether any warrants and/or authorisations were in force during the year to which the report relates. Moreover, new section 19 (found in clause 18 of the Bill) establishes a new register of warrants and authorisations, which must be available on request to the Responsible Minister and the Inspector-General of Intelligence and Security.

244. These matters aside, officials have identified some gaps in section 15A, in terms of the type of information that should be captured in any given warrant or authorisation. Greater specificity here will aid compliance outcomes, enhance accountabilities and transparency generally, and also assist in the ongoing management of the new register of warrants and authorisations, required by new section 19 (found in clause 18 of the Bill).

Recommendation 3

245. The Department recommends that a new provision be inserted here (either in new section 15A itself a standalone provision immediately following), listing the information to be captured in each warrant / authorisation. The provision will need to–

245.1. capture the items described as needing to be specified in section15A(1), i.e. the authorised interception device or devices, the persons or classes of persons whose communications may be intercepted, the places or classes of places where communications made or received may be intercepted;

245.2. also capture the items listed in section 15A(2) that could usefully be included in a warrant / authorisation, e.g. the function under which the Bureau is proposing to act;

245.3. capture the items currently listed at new section 19(2), i.e. the date of issue, the term of the warrant, any relevant information infrastructure or information infrastructures or classes thereof.

<u>New section 15B – Authorisation to intercept communications or access information infrastructures</u>

246. Section 15B requires the Commissioner of Security Warrants to be involved in the application for, and the issue of, a warrant or authorisation under the GCSB Act, 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 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 amended section 14.

Submissions

247. Several submitters expressed doubt about the role of the Commissioner for Security Warrants (see, for example, submissions 84, 91, 112). Two submitters felt it was inadequate as a safeguard, either because they wanted to see "more extensive protections" (submission 84) or because the appointment of the Commissioner was made on the recommendation of the Prime Minister and, regardless of the role of the Commissioner, warrants and authorisations could be issued to intercept communications that were not otherwise lawfully obtainable and section 15A took precedence over the New Zealand Bill of Rights Act 1990 (submission 112). One submitter suggested that the Commissioner for Security Warrants should also be involved when GCSB exercised its function under new section 8C, as well as the issue of urgent warrants and authorisations (submission 91).

Comment

248. The Commissioner of Security Warrants is a statutory position, established in 1999 under section 5A of the New Zealand Security Intelligence Service 1969. The Commissioner is appointed by the Governor-General on the recommendation of the Prime Minister following consultation with the Leader of the Opposition. The Commissioner must have previously held office as a Judge of the High Court.

249. The Commissioner is already responsible for advising on and issuing domestic intelligence warrants jointly with the Minister Responsible for the NZSIS. This role has proven valuable to both current and past Responsible Ministers and no issue has arisen regarding the Commissioner's judgement in performing this role.

250. As regards the proposal that the Commissioner for Security Warrants should also be involved in the issue of urgent warrants and authorisations, that is already the case under new section 19A(3) (found in clause 18 of the Bill).

251. The suggestion regarding an expanded role for the Commissioner under new section 8C is discussed above in the section on general themes.

Recommendation

252. The Department does not recommend any change to new section 15B.

<u>Privilege</u>

Submissions

253. The LAC (submission 22) notes that the Bureau will be subject to statutory provisions relating to the protection of privilege under the Search and Surveillance Act in circumstances where they carry out interception on behalf of the Police under new section 8C. In the case of assistance to the NZSIS, privileged material is protected under section 4A(3) of the NZSIS Act.

254. The LAC goes on to note that where the Bureau intercepts the communications of New Zealander in relation to its other functions (under new sections 8A and 8B), the extent to which privileged material is protected will depend on the common law.

255. The LAC recommends that for legislative consistency and ease of operation the ISC may wish to consider including privilege measures such in the Bill.

256. The Human Rights Foundation (submission 91) also raises the issue of protection of legal professional privilege.

Comment

257. Privilege is not currently addressed in the GCSB Act, though it does feature in the NZSIS Act.

258. Section 4A(3) of the NZSIS Act, provides that an intelligence warrant may be issued subject to the condition that any communication sought to be intercepted under the proposed warrant is not subject to legal professional privilege. There is also protection of privilege for communications with Ministers of religion and privilege relating to information obtained by medical practitioners and clinical psychologists.

259. Section 4G of the NZSIS Act also requires the destruction of irrelevant records obtained by interception as soon as practicable after the interception, although there is no specific reference in section 4G to privileged communications.

260. New section 8C will require the GCSB to take account of matters such as privilege, if it is requested to provide assistance to other agencies, under new section 8C(2) which provides that the Bureau may perform the assistance function subject to any limitations, restrictions, and protections under which those entities perform their functions and exercise their powers.

261. We agree with the LAC that it is preferable to address the matter of privilege, in relation to the communications of New Zealanders, in the bill rather than leaving it to the common law. This is consistent with the purpose of the bill in providing a clearly formulated and consistent statutory framework.

262. The bill currently provides that the any interception of the communication of a New Zealander for the purposes of the functions in section 8A and 8B must be jointly issued by the Minister and the CSW. As an added safeguard for New Zealanders, and to avoid any debate, in those cases where the CSW must be involved we propose that an additional criteria to be satisfied before the warrant or authorisation is granted is that the communication to be intercepted is not privileged. The provision would be modelled on section 4A(3) of the NZSIS Act.

Recommendation 4

263. The Department recommends that a new provision be inserted to apply when a warrant or authorisation must be issued jointly by the Minister and the CSW. As an added safeguard for New Zealanders an additional criteria to be satisfied before the warrant or authorisation is granted is that the communication to be intercepted is not privileged. The provision would be modelled on section 4A(3) of the NZSIS Act.

Clause 15 – Section 16 amended (Certain interceptions permitted without interception warrant or computer access authorisation)

264. This clause amends section 16, which permits certain interceptions without an interception warrant or an access authorisation. The amendments specify that:

264.1. the section applies to interceptions for the purpose of the Bureau's functions in new sections 8A (information assurance and cybersecurity) and 8B (foreign intelligence);

264.2. warrantless interception of the private communications of New Zealand citizens and permanent residents cannot be undertaken.

Submissions

265. Some submitters (submissions 84, 106, 112) questioned whether the power to intercept communications without warrant or authorisation should be retained.

266. The LAC (submission 22) notes that it would be desirable for the Committee to assess the scope of the activity permitted under the warrantless powers of interception as it is unclear the extent to which the criteria in section 16 provide a substantive limitation on warrantless activities. Another submitter noted that section 16 was impenetrable, which made it difficult to assess its scope and effect (submission 66). The NZLS suggested that there be a new register of warrantless intercepts under section 16 (submission 84).

Comment

267. The amendments to section 16 are largely consequential on other changes in the Bill (namely making it clear that the powers can be used for both section 8A and 8B functions) and do not substantively change the threshold for when they may be used.

268. Regarding the proposal to delete section 16 entirely, this has been considered but rejected on the basis that it would deprive the Bureau of a necessary interception power in certain limited circumstances. Warrantless powers are particularly required in react in emergencies when immediate action is necessary.

269. Regarding the proposal to establish a new register of warrantless intercepts, this is not considered necessary in light of the recommendations of the Kitteridge Report and the new compliance framework and record-keeping obligations to

which the Bureau has already demonstrated its commitment, as discussed above in the section on general themes.

Recommendation

270. The Department does not recommend any change to clause 15.

Clause 16 – Section 17 and cross-heading repealed

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

Comment

272. No submissions were received on this clause and no changes are recommended.

Clause 17 – Section 18 amended (Persons acting under warrant)

273. Section 18 provides for certain matters about the content of warrants, namely the specification of persons or classes of person who may assist in executing a warrant.

274. Clause 17 amends section 18 to widen its application to include access authorisations to take into account the amendments made to the warrant and authorisation provisions.

Submissions

275. No submissions were received on this section.

Comment

276. We recommend, above, to insert a new section that sets out in statute a more comprehensive list of what must be included in a warrant or authorisation. If that recommendation is accept we propose that section 18 be repealed and the requirements on specification of persons assisting be incorporated into the new section.

Recommendation 5

277. The Department recommends, subject to the agreement of the Committee to recommendation 3, that section 18 be repealed and the requirements regarding the specification of persons assisting be incorporated into the new proposed section.

Clause 18 – Section 19 and cross-heading replaced (Register of interception warrants and access authorisations and urgent issue of warrants and authorisations)

278. This clause replaces section 19 with new sections 19 and 19A. (The current section 19 has been assimilated into new section 15A, inserted by clause 14.)

New section 19

279. New section 19 requires the Director to keep a register of interception warrants and access authorisations that have been issued.

Submissions

280. The CTU (submission 58), the NZLS (submission 84) and the Human Rights Foundation (submission 91) all strongly support new section 19, although the NZLS considers that the register could be more comprehensive and include instances of warrantless intercept under section 16.

Comment

281. Officials note that some amendment is needed to fine-tune the information held on the register in respect of warrants and authorisations, to accord with the changes suggested in respect of new section 15A (found in clause 14 of the Bill).

Recommendation 6

282. The Department recommends that new section 19(2) be amended:

282.1. subject to the agreement of the Committee to recommendation 3, to refer to the need to capture the same information on the Register as is recommended in this Report for inclusion in a warrant/authorisation (i.e. by reference to the section number); and

282.2. to ensure that paragraph (e) also applies to warrants.

New section 19A

283. New section 19A provides for the urgent issue of warrants or 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.

Submissions

284. Numerous submitters suggested that the Responsible Minister should be informed as soon as reasonably practicable after an urgent warrant or authorisation had been issued (see, for example, submissions 5, 6, 7, 9, 12, 13, 16, 39, 56, 66, 72, 82, 92, 95, 119, 122 and 123).

Comment

285. Officials consider that the suggestion regarding urgent warrants should be adopted. It will further enhance the accountabilities under the Act.

Recommendation 7

286. The Department recommends that new section 19A be amended to require that the Responsible Minister be informed as soon as reasonably practicable after an urgent warrant or authorisation had been issued.

Clause 19 – Section 20 amended (Director's functions in relation to warrants and authorisations not to be delegated)

287. This clause makes drafting amendments to section 20.

Comment

288. No submissions were received on this clause and no changes are recommended.

Clause 20 – Section 21 replaced (Action taken in accordance with warrant or authorisation justified)

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

Submissions

290. Some submitters recommend that this clause should be deleted.

Comment

291. The purpose of immunity provisions, which are found in a number of enactments, is to protect the individual public servants that execute the warrants from legal proceedings. While there is a need to ensure that public servants exercising intrusive powers take due care, the threat of personal legal action may unduly reduce the willingness of public servants to exercise the State's coercive powers in appropriate cases.

292. We consider that new section 21 strikes the balance between ensuring appropriate exercise of powers and protection for individual public servants. It is modelled, in particular, on sections 165 and 166 of the Search and Surveillance Act 2012, which sets out the immunities for officials obtaining and exercising warrants for entry, search or surveillance.

293. The immunity provided is not absolute. An individual Bureau employee will still be subject to legal proceedings if they act in bad faith, unreasonably or outside their powers. In addition, Bureau employees would still face employment action and disciplinary procedures. Finally, in most cases they are acting according to departmental systems and policies. This immunity does not change the accountability of the department or prevent proceedings that may be taken against it directly (as in the current proceedings against the Bureau in the Kim Dotcom et al cases).

Recommendation

294. The Department does not recommend any change to this clause.

Clause 21 – Sections 22 amended (term of warrant or authorisation)

295. This clause makes drafting amendments to section 22.

Submissions

296. No submissions were received on this clause.

Comment

297. We recommend, above, that a new section should be inserted setting out more comprehensively what must be specified in each warrant or authorisation. If that recommendation is agreed to we recommend that section 22 be repealed and the requirements on the term of warrants and authorisations (unchanged) be incorporated into the new section.

Recommendation 8

298. The Department recommends, subject to the agreement to recommendation 3 that section 22 be repealed and the requirements regarding the term of warrants and authorisations be incorporated in the new proposed section.

Clauses 22 and 23 – Sections 23 to 24 amended

299. These clauses make drafting amendments to sections 23 and 24.

Comment

300. No submissions were received on these clauses and no changes are recommended.

Clause 24 – Section 25 replaced (Prevention and detection of serious crime)

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

301.1. preventing or responding to threats to human life in New Zealand or any other country

301.2. identifying, preventing, or responding to threats or potential threats to the national security of New Zealand or any other country.

Submissions

302. Several submitters wanted to see greater limits places on the use of incidentally obtained intelligence (see, for example, submissions 19, 20, 22, 25, 28, 43, 84, 95, 99 and 119). In this regard, some submitters proposed that the ISC should have oversight of all incidentally collected information shared under section 25 (see, for example, submissions 56, 72, 119 and 122, whilst submissions 84 and 118 thought the ISC should have greater oversight powers generally).

303. James Cone (submission 66) noted that it did not currently appear that incidentally obtained intelligence could be communicated to anyone else for the purpose of avoiding the loss of life at sea in international waters.

304. The New Zealand Law Society (submission 84) commented that the basis for sharing information had been expanded and was particularly concerned with proposed new section 25(2)(c) which refers to "threats or potential threats to the national security of New Zealand or any other country". The NZLS stated that while they accept the intelligence gathering role of GCSB plays a crucial or critical role in protecting New Zealand from threats this formulation falls short of what is required under NZBORA and privacy interests. Some other submissions also referred to similar concerns about this section, and that the term "national security" was so broad as to capture almost anything of relevance or importance to the government.

305. Other submissions highlighted new section 25(3)(d) which allows the Director to communicate the intelligence to "any other person that the Director thinks fit to receive the information". Submitters felt that this was class was too wide and made the listing of specific agencies in the paragraphs above redundant.

306. The NZLS also recommended that requirements should be placed on the Director regarding the retention of incidentally obtained intelligence.

Comment

<u>Expanded grounds for communicating information</u>

307. The proposed amendments do expand the reasons for communicating incidentally obtained intelligence from the prevention and detection of serious crime, to threats or potential threats to the national security of New Zealand or any other country, and preventing or responding to threats to human life.

308. Threat to human life was added to account for situations where the threat to life may not be associated with a serious crime. Such situations may be relevant in cases of search and rescue or natural disaster. While it is difficult to provide specific examples, saving the life of a person was seen as a sufficient justification for communicating relevant intelligence. James Cone (submission 66) in this respect notes that the provision refers to threats to life "…in New Zealand or any other country", which could exclude situations which occur in international waters which particularly relevant to search and rescue situations. We recommend, therefore, that the provision be amended, if necessary, to capture this situation.

309. We agree with the concerns about the new ground of threats or potential threats to the national security. The term "national security" is used in new section 7

(Objective of the Bureau), which is a carryover from the GCSB Act. However, the term "national security" is used in the way proposed in this section before.

310. National security is a term that has a broad meaning and can encompass a wide range of interests. Its use in the objective section is appropriate as the Bureau contributes to those broad interests (see discussion above on the scope of the objective of the Bureau). What the Bureau can do is then governed by the provisions setting out functions, powers and limitations on those powers.

311. However, in this section, which sets out what the Bureau can do with incidentally obtained intelligence we agree that a more specific formulation should be used. We therefore recommend that the term "national security" be replaced with "security or defence". This term is found in a number of other statutes, for example in the Official Information Act 1982 in the grounds for withholding information.

Person to whom intelligence can be communicated

312. We agree that section 25(3)(d) in referring to "any other person that the Director thinks fit" is too wide. The intention was to allow the intelligence to be communicated to authorities who could take steps to respond to the identified purposes. In addition to the listed bodies (NZ Police, NZDF and NZSIS) they could include other law enforcement agencies, search and rescue authorities, and the overseas equivalents where the threat was in another country. We propose, therefore, to limit the class of persons to whom the intelligence can be given, to public authorities in New Zealand or overseas.

Retention of information

313. The information within the scope of section 25 falls outside the retention of information regime in section 23 of the GCSB Act. The Bureau is currently exempt from privacy principle 9 (agency not to keep information for longer than necessary). The NZLS makes some specific recommendations about putting in place such a regime.

314. Under new sections 25A and 25B the Bureau is required to develop a policy on personal information, which all employees and person acting on behalf of the Bureau must comply. The policy must address the requirement that the Bureau must not keep personal information for longer than is required for the purposes for which the information may lawfully be used. This policy making process will address the retention of all information held by the Bureau including incidentally obtained intelligence.

Recommendation 9

315. The Department recommends that new section 25(2) be amended to allow the communication of incidentally obtained intelligence for the purpose of avoiding the loss of life at sea in international waters.

Recommendation 10

316. The Department recommends that new section 25(2)(c) be amended to replace the term "national security" with the term "security or defence".

Recommendation 11

317. The Department recommends that new section 25(3)(d) be amended to remove references to "any other person" and replace it with "any other public authority in New Zealand and any other country".

Clause 25 – New section 25A and 25B and cross-heading inserted (Protection and disclosure of personal information)

318. This clause 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 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.

Submissions

319. A number of submissions supported the requirement to formulate privacy policy. The CTU (submission 58) strongly supported this clause. The NZLS (submission 84) also supported this clause, but thought that the Bill could have gone further, for example, by providing clearer monitoring powers and sanctions. The Environment and Conservation Organisations of New Zealand (submission 118) voiced cautious support, but noted that it would be critical to see the policy as drafted.

320. The Privacy Commissioner (submission 87) welcomed these provisions as a start but noted that some matters remain unclear and raised some matters that could be clarified or made explicit in the legislation.

321. First, the Privacy Commissioner identified that the Bill is not clear on what actions she could take if she had concerns arising from an audit of compliance with the policy reported to her under new section 25A(2)(c).

322. The Privacy Commissioner makes two specific suggestions about how this could be addressed through an explicit statement about who is the enforcement authority, and an ability for the Privacy Commissioner to report matters of significant concern directly to the Prime Minister.

323. Second, the Privacy Commissioner notes that the Bill is silent on the frequency and nature of the review of the privacy policy. She recommends consideration be given to whether the Privacy Commissioner and Inspector-General could trigger a review, if they become concerned about the policy or its implementation.

Comment

324. We agree with the comments made by the Privacy Commissioner about the Bill not explicitly addressing the consequences resulting from concerns arising from the results of audits provided to the Privacy Commissioner and Inspector-General.

325. The Privacy Commissioner observes at paragraph 4.6:

> *…the Bill currently appears to anticipate that the IGIS will be the sole enforcement authority. The role of the Privacy Commissioner would probably be to inform the IGIS of any concerns, so the IGIS in turn could consider the issue and report if required. If this is the intention, I note in passing that the legislation should set this out more clearly.*

326. This captures the intention underlying the Bill. We propose, therefore, that the Bill be amended to make this clear.

327. The Privacy Commissioner has also suggested that, while working through the IGIS would often be the most appropriate approach, a backstop measure would be useful. The measure suggested is the ability for the Privacy Commissioner to report serious matters directly to the Prime Minister. Section 81 of the Privacy Act is suggested as a model. The Privacy Commissioner in support of this proposal says such a backstop measure would be useful "for example if the IGIS were too busy to deal with the matter".

328. The Bill expands the office of the Inspector-General with the appointment of a Deputy and the Government has made a firm commitment to provide the resources necessary to perform the functions effectively. The IGIS also has the ability to seek additional resources under the IGIS Act if there is an unexpected increase in workload or significant inquires underway.

329. Second, it seems unlikely that any Inspector-General would set aside a serious matter of concern in relation to privacy. In any case, referral of an issue to the Prime Minister would probably result in the Prime Minister referring the matter to the Inspector-General for investigation. On that basis we do not believe that it necessary to provides such a mechanism.

330. We agree that the frequency of review should be specified in the Bill. We suggest that the policy must be regularly reviewed but at least once every 3 years. The Privacy Commissioner also recommended that she or the Inspector-General should be able to trigger a review of the policy. We do not think such a provision is necessary in light of the recommendation above about the Inspector-General's role to consider matters of concern arising from the result of audits.

Recommendation 12

331. The Department recommends that the Bill be clarified to make it explicit that the Privacy Commissioner should report any issues identified from her consideration of the result of audits provided to her under new section 25A(2)(c) to the Inspector-General who will be responsible for investigating and reporting on those issues.

Recommendation 13

332. The Department recommends that the privacy policy must be reviewed regularly but it must be reviewed at least once every 3 years.

Clause 26 – Consequential amendments

333. This clause makes consequential amendments to other Acts set out in the Schedule. The Acts amended are the:

333.1. Radiocommunications Act 1989;

333.2. Search and Surveillance Act 2012;

333.3. Telecommunications (Interception Capability) Act 2004.

Comment

334. No submissions were received on this clause and no changes are recommended.

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

335. This Part amends the Inspector-General of Intelligence and Security Act 1996 to strengthen the office of the Inspector General, 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.

Comment

336. A large number of submissions supported the amendments to the IGIS Act and recommend that they be enacted. Some submitters, while supportive, felt that the amendments could go further. The Privacy Commissioner (submission 87) recommended that further consideration be given to different oversight models, and to the most appropriate method of making the Bureau accountable for how it handle personal information.

337. Careful thought was given to the appropriate oversight regime for the intelligence community, through the review of legislation and as part of the Kitteridge review. The Government's view is that the structure of the regime is appropriate however, it would benefit from some specific improvements which are set out in the Bill and further refined in this report. In addition the Government recognises that without adequate resources the regime will not be effective. Consequently, the Government has committed to providing the Inspector-General with the funding and resources necessary to carry out the role and working with the members of the ISC to improve the way it works.

338. Specific recommendations for amendments to particular provisions are discussed below in the clause by clause analysis.

Clause 29 – Section 5 and cross-heading replaced (Deputy Inspector-General of Intelligence and Security)

339. This clause replaces section 5 with new section 5, which provides for the appointment of an Inspector-General of Intelligence and Security 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.

340. The appointments will continue to be made by the Governor-General on the recommendation of the Prime Minister, but the Prime Minister will be required to consult with the ISC rather than just the Leader of the Opposition. The requirement that the Inspector-General must have held office as a Judge of the High Court of New Zealand is removed.

Submissions

341. A number of submissions support the creation of the Deputy Inspector-General role.

342. Some submitters are concerned that the appointment of the Inspector-General is made on the recommendation of the Prime Minister because the Prime Minister is

currently the responsible Minister. Those submitters believe this impacts negatively on the independence of the IGIS. They do not believe the expanded consultation requirement goes far enough. They recommend that the Inspector-General not be appointed on the recommendation of the Prime Minister, and be an officer of Parliament.

Comment

343. There are a small number of officers of Parliament. They are the Auditor-General, Ombudsmen and the Parliamentary Commissioner for the Environment. Each of them is appointed by the Governor-General on the recommendation of the House of Representatives.

344. There are other oversight bodies which are appointed on the recommendation of the House of Representatives but they are not officers of Parliament. The relevant examples include the Independent Police Complaints Authority and the Judicial Conduct Commissioner. Each of those bodies performs a role similar to the Inspector-General.

345. While the bodies referred to above are appointed by the Governor-General on the recommendation of the House of Representatives, in the case of the Inspector-General a more limited consultation process is appropriate. This is to allow the suitability of potential candidates to be discussed in light of the activities of the intelligence agencies, including reference to sensitive information. The Bill expands the consultation requirement from consultation with the Leader of the Opposition to consultation with the ISC.

Recommendation

346. The Department does not recommend any changes to this clause.

Clause 30 – Section 6 amended (Term of office)

347. This clause amends section 6, which provides for the Inspector-General's term of office. The amendments:

347.1. add a reference to the Deputy Inspector-General;

347.2. provide for a term of appointment of 3 years for each;

347.3. provide that each can be reappointed, but in the case of the Inspector-General only once.

Submissions

348. Many submitters welcomed these amendments, but noted that a deputy alone was not enough of an increase to the resourcing of the office to carry out its role effectively.

349. Some submissions recommended that the term of the Deputy Inspector-General also be limited to two terms. One submitter suggested that the term of the Inspector-General should be increased (submission 106).

Comment

350. The Deputy is the only one part of the package to increase the resourcing of the Office. The Government is committed to providing the office with the resources it needs to carry out its role effectively.

351. The deputy position does not have a limitation on reappointment to provide some flexibility to maintain continuity of knowledge and experience in the Office. The appointment of the deputy will be subject to consultation with the ISC, and the number of terms will be one of the matters considered. The Department does not recommend any changes to limit the reappointment of the Deputy Inspector-General.

352. The term of the IGIS is kept at 3 years and capped at two terms to provide further public assurance that the IGIS has the necessary independence.

Recommendation

353. The Department does not recommend any changes to clause 30.

Clause 31 – Section 11 amended (Functions of Inspector-General)

354. This clause amends section 11, which specifies the functions of the Inspector-General of Intelligence and Security.

Submissions

355. The LAC (submission 22) and NZLS (submission 84) note that the own motion powers of the Inspector-General to investigate whether the actions of security agencies may have adversely affected New Zealand persons requires the concurrence of the Minister. The LAC queries whether the concurrence of the Minister is necessary, given there are other mechanisms to protect sensitive information.

356. The Privileges Committee in its interim report on a *Question of privilege concerning the agreements for policing, execution of search warrants, and collection and retention of information by the NZSIS* made the following recommendations:

> *We recommend to the Intelligence and Security Committee that it considers whether there is a need to clarify the oversight of the intelligence agencies to ensure the Inspector-General of Security and Intelligence can receive complaints about, and inquire into, the actions of those agencies that affect a class of person.*
>
> *We recommend to the Intelligence and Security Committee that it considers the appropriateness of requiring the agreement of the responsible Minister before the Inspector-General can undertake an inquiry under the new section 11(1)(c) of the Inspector-General of Security and Intelligence Act 1996 that is proposed in the Government Communications Security Bureau and Related Legislation Amendment Bill.*

Comment

Concurrence of responsible Minister – new section 11(1)(c)

357. We agree with the submission of the LAC and NZLS, and the recommendation of the Privileges Committee that the concurrence of the Minister to all own motion powers should be removed.

Who can make a complaint – section 11(1)(b) of the IGIS Act

358. The Privileges Committee's recommendation regarding who can complain to the Inspector-General arises from the committee's view that the activities of the NZSIS under the agreement being examined should come clearly within the oversight of the Inspector-General.

359. The committee is concerned that "it does not appear possible under the current wording of section 11 for the Speaker to complain to the Inspector-General on behalf of the members of Parliament or about the actions or policies of the NZSIS more generally". Later in the report reference is made to the Independent Police Conduct Authority Act 1988, which provides that it may receive complaints "concerning any practice, policy or procedure of the Police affecting the person or body of persons making the complaint in a personal capacity" (see section 12(1)(a)(ii)).

360. The Privileges Committee did not want to see an amendment specifically for the benefit of the House of Representatives and felt any amendment should apply more generally to all bodies of persons.

361. The IGIS Act provides in section 11(1)(b) that it is a function of the Inspector-General:

> *To inquire into any complaint by –*
>
> *(i) a New Zealand person; or*
>
> *(ii) a person who is an employee or former employee of an intelligence and security agency, -*
>
> *that that person has or may have been adversely affected by any act, omission, practice, policy, or procedure of an intelligence and security agency.*

362. "New Zealand person" is defined in section 2 of the IGIS Act as follows:

> ***New Zealand person***—
>
> *(a) means any person, being—*
>
> *(i) a New Zealand citizen; or*
>
> *(ii) a person ordinarily resident in New Zealand; or*
>
> *(iii) an unincorporated body of persons, being a body of which more than 50% of the members are New Zealand persons under subparagraph (i) or subparagraph (ii); or*
>
> *(iv) a body corporate which is incorporated in New Zealand; but*
>
> *(b) does not include—*
>
> *(i) any company within the meaning of the Companies Act 1955 or the Companies Act 1993, as the case may be, that is, for the purposes of the*

Companies Act 1955 or the Companies Act 1993, a subsidiary of any company or body corporate incorporated outside New Zealand; or

(ii) any company within the meaning of the Companies Act 1955 or the Companies Act 1993, as the case may be, or building society, in which—

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

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

(iii) any nominee of an overseas person, whether or not the nominee is also an overseas person

363. The definition of "New Zealand person" enables bodies of persons to make a complaint to the Inspector-General in the same way as the IPCA Act. However, there are limitations on the bodies that can complain under the IGIS Act, with reference to their "New Zealandness" (as determined by, for example, percentage of membership made up of New Zealand citizens and permanent residents).

364. The House of Representatives may come within the definition of "New Zealand person", by being an unincorporated body of persons or body corporate (on the basis that more than 50% of its membership is made up of New Zealand citizens or permanent residents). If that were the case, the Speaker would be able to complain on behalf of the House of Representatives.

365. The Privileges Committee report does not directly address the definition of "New Zealand person" consequently we have sought comments from the Office of the Clerk. They have made some comments in which they argue the definition of "New Zealand person" is does not capture the House of Representatives.

366. We agree that the House of Representatives should be able to make a complaint to the Inspector-General. As this is a drafting matter we recommend that the ISC agree that the Department, Parliamentary Counsel and the Office of the Clerk undertake further discussions and report any drafting changes to give effect to the policy position recommended by the Privileges Committee.

Recommendation 14

367. The Department recommends that section 11(1)(c) be amended to remove the requirement for the concurrence of the responsible Minister.

Recommendation 15

368. The Department recommends that the Department, Parliamentary Counsel and the Office of the Clerk consider any drafting changes required to give effect to the policy position (as discussed by the Privileges Committee) that the House of Representatives be able to make a complaint to the Inspector-General, and present any proposed amendments in the Revision Track version of the Bill.

Clause 32 – Section 12 amended (Consultation)

369. This clause amends section 12, which authorises the Inspector-General to consult certain public office holders. The amendment adds a reference to the Independent Police Conduct Authority (IPCA) as one of the public offices that may be consulted.

Submissions

370. The Human Rights Foundation (submission 91) supports the expanded consultation requirements and queries whether it could be extended to the Health and Disability Commissioner.

Comment

371. When reviewing the legislation, we considered whether it was necessary and appropriate to add further public office holders to the list in section 12, taking into account any overlapping jurisdiction for the security agencies or the subject matter that may require consultation between the Inspector-General and another public office holder. That review found that the IPCA should be added. The submitter has not specified why they believe the Health and Disability Commissioner should be added and we cannot find any overlap or subject matter issues that would make it necessary.

Recommendation

372. The Department does not recommend any changes to this clause.

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

373. The amendments to section 15 are consequential on the amendments to section 12.

Comment

374. No submissions were received on clause and no changes are recommended.

Clause 34 – Section 25 amended (Reports in relation to inquiries)

375. The amendments to section 25:

375.1. 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;

375.2. permit the Minster to provide this or her response to the Intelligence and Security Committee.

Submissions

376. One submission was received on this clause, expressing surprise that the Minister was not required to provide a copy of his or her response to an inquiry conducted by the IGIS to the Committee (submission 66).

Comment

377. Officials considered the need for the ISC to have access to every response of the Responsible Minister to an inquiry by the IGIS. Whilst this might be generally desirable, there are also questions of operational security, classification of information, and timing to consider. On balance, it was determined that the Responsible Minister should have a discretion as to when he or she would provide a copy of his or her response to an inquiry by the IGIS to the ISC.

378. On a related note, the Australian Inspector-General of Intelligence and Security has suggested one of the practical matters the Bill should address is who gets the final say on what is or is not classified. The usual practice is that the author of the report has the final say on classification but it is expected that they would consult closely with those that contributed material to the preparation of the report.

379. The classification of the report is a separate matter to the final publication of the report, which will be governed by new section 25A.

Recommendation 16

380. The Department recommends that the Bill be amended to include a provision providing that the Inspector-General determines the classification of any reports they prepare, on the proviso that they must–

380.1. consult with the head of the intelligence and security agency that is the subject of the report;

380.2. retain the same security classification in respect of any material provided to the IGIS that is quoted verbatim in the report; and

380.3. otherwise respect the classification of material provided to support the inquiry before finalising the classification.

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

381. This clause inserts a new section 25A, which requires the Inspector-General, as soon as practicable after forwarding a report under section 25(1), to make a copy publicly available on an internet site maintained for the Inspector-General.

Submissions

382. Some submitters commented on the difficulty of accessing the publicly released reports of the Inspector-General and, on that basis recommend that the IGIS be made subject the Official Information Act 1982 (OIA) (see, for example, submission 11).

Comment

383. The publication requirements set out in the Bill will make the reports of the IGIS far more available than they have ever been before. A website maintained by or

on behalf of the IGIS will provide a single authoritative source for all of the past, current and future reports of the Inspector-General as well as providing background information on the role and function of the office. It will also make it easier for people to contact the office.

384. The concern expressed by the submitters about access to reports is address by this clause, which makes the recommended solution of application of the OIA to the Inspector-General unnecessary.

385. In any case it would not be appropriate, like other organisations that exercise similar functions (for example, the IPCA and Judicial Conduct Commissioner), to make the Inspector-General subject to the OIA. The Inspector-General's disclosure requirements are prescribed by the IGIS Act, and under the proposed amendments the conclusion of the Inspector-General's inquiries is more likely to be published. Any source information that informed any inquiries from the intelligence agencies is held primarily by them and it is more appropriate to seek such information from them under the OIA.

Recommendation

386. The Department does not recommend any amendments to this clause.

Clause 36 – Section 27 amended (Reports by Inspector-General)

387. This clause amends section 27, which provides for the Inspector-General's annual report. The amendments:

387.1. require the Inspector-General to certify whether each intelligence and security agency's compliance systems are sound; and

387.1. 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.

Submissions

388. No submissions were received on this clause.

Comment

389. The drafting of the amendment requiring the Inspector-General to make a public statement regarding the adequacy of each intelligence and security agency's compliance systems may need to be reconsidered. An auditor's role, on which this requirement is modelled, is to provide an opinion on the state of an entity's systems and records. That may be qualified or unqualified by the person preparing the opinion, and any qualifications are articulated in the report. The provision as drafted may be more absolute than what was intended on reflection.

Recommendation 17

390. The Department recommends that the ISC agree that new section 27(2)(b) be amended to say "…whether and, if not, to what extent…" or similar.

Part 3 – Amendments to Intelligence and Security Committee Act 1996

391. This Part contains amendments to the Intelligence and Security Committee Act 1996 (ISC Act).

Clause 38 – Section 6 amended (Functions of Committee)

392. This clause amends section 6, which specifies the functions of the Committee. 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 section 6(1)(e), which requires the Committee to present an annual report to the House and to make an annual report publicly available on the Internet site of the New Zealand Parliament.

Submissions

393. A number of submitters (see for example submissions 5, 6, 7, 9, 12, 13, 95) recommend that the ISC Act be amended to provide the ISC with the same functions as the Inspector-General under section 11 of the IGIS Act.

Comment

394. The ISC and IGIS have distinct and separate roles to play in the oversight regime for the New Zealand Intelligence Community. The primary purpose of the ISC is to provide parliamentary oversight and undertake the role otherwise undertaken by a parliamentary select committee. It provides political oversight to the community.

395. The ISC's functions mirror those of a select committee. Its functions, in relation to an intelligence agency, are set out in section 6. They are:

395.1. to examine the policy, administration, and expenditure of each intelligence agency, and to receive and consider the annual reports of the agencies;

395.2. to consider any bill, petition, or other matter in relation to an intelligence agency referred to it by the House of Representatives;

395.3. to consider any matter referred to it by the Prime Minister.

396. The ISC has the power to call witnesses and require the production of documents (see section 14 of the ISC Act).

397. These functions are, however, limited in section 6(2). The limitations are that the functions of the ISC do not include:

397.1. inquiring into any matter within the jurisdiction of the Inspector-General of Intelligence and Security appointed under section 5 of the Inspector-General of Intelligence and Security Act 1996;

397.2. inquiring into any matter that is operationally sensitive, including any matter that relates to intelligence collection and production methods or sources of information;

397.3. originating or conducting inquiries into complaints by individuals concerning the activities of an intelligence and security agency that are capable of being resolved under any other enactment.

398. A specific inquiry into operational matters involves looking at on the ground activities, and is the province of the Inspector-General. Looking at such matters involves delving into sensitive information that could put the officers and employees of the intelligence agencies in mortal danger.

399. The IGIS has a role in looking more closely at specific matters, policies and procedures. In simple terms the IGIS provides an oversight mechanism similar to the Ombudsmen, Office of the Auditor General and other statutory officers, in a manner that accommodates the nature of the intelligence community. It is a role delivered by an independent statutory officer that operates free from political influence.

400. A duplication of functions while superficially attractive unduly confuses the two different types of oversight and could create an unhelpful tension between the two bodies. It would also duplicate the resources required to carry out the functions in section 11 of the IGIS Act.

401. The ISC is not a body suited to receive individual complaints. It operates by majority and would bring an unduly political nature to matters that should instead be investigated by an independent statutory officer.

Recommendation

402. The Department does not recommend any change to clause 38.

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

403. This clause inserts new section 7A, which contains further provisions about the chairperson of the Committee. The new section provides:

403.1. 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;

403.1. 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.

Submissions

404. No submissions were received on this clause.

Comment

405. Existing section 13(6) of the Intelligence and Security Committee Act 1996 prohibits members of the Intelligence and Security Committee from being

represented by anyone else. Officials note that this provision is at odds with new section 7A (found in clause 39 of the Bill) and needs fine-tuning to enable the new provision creating some flexibility in respect of the chair of the Committee to work as intended.

Recommendation 18

406. The Department recommends that existing section 13(6) of the Intelligence and Security Act is expressed to be subject to new section 7A(3) of the Intelligence and Security Act.

Recommendation 19

407. The Department recommends that new section 7A(3) of the Intelligence and Security Act:

407.1. be moved closer to existing section 13(6) of the Intelligence and Security Act; and

407.2. be amended to also give the Leader of the Opposition the same right to nominate an alternate, albeit limited to the deputy leader of his or her party.

Clause 40 – Section 18 amended (Restrictions on report to House of Representatives)

408. This clause makes amendments to section 18 that are consequential on the amendment made by clause 38.

Comment

409. No submissions were received on this clause and no changes are recommended.

Summary of Recommendations

This section of the Report contains the recommendations to the Committee.

Part 1

The Department recommends that:

1. Officials work with PCO to reconsider new section 8A(c) in light of new section 8B(1)(c) and develop any necessary amendments to better align these provisions.

2. In relation to new section 8C that:

    2.1. the opening words of subsection (2) be tightened by inserting "only" before "perform";

    2.2. paragraph (2)(b) begin with the words "in accordance with" instead of "subject to";

    2.3. PCO be asked to include a separate provision to the effect that any advice or assistance provided under section 8C(1) to another entity is subject to 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 co-operation with Police); and

    2.4. PCO be asked to include a provision clarifying that it is intended that the IGIS would continue to have an oversight role in respect of activities undertaken by the Bureau under new section 8C.

3. A new provision be inserted here (either in new section 15A itself a standalone provision immediately following), listing the information to be captured in each warrant / authorisation. The provision will need to–

    3.1. capture the items described as needing to be specified in section15A(1), i.e. the authorised interception device or devices, the persons or classes of persons whose communications may be intercepted, the places or classes of places where communications made or received may be intercepted;

    3.2. also capture the items listed in section 15A(2) that could usefully be included in a warrant / authorisation, e.g. the function under which the Bureau is proposing to act;

    3.3. capture the items currently listed at new section 19(2), i.e. the date of issue, the term of the warrant, any relevant information infrastructure or information infrastructures or classes thereof;

4. A new provision be inserted to apply when a warrant or authorisation must be issued jointly by the Minister and the CSW. As an added safeguard for New Zealanders an additional criteria to be satisfied before the warrant or authorisation is granted is that the communication to be intercepted is not privileged. The provision would be modelled on section 4A(3) of the NZSIS Act.

5. Subject to the agreement of the Committee to recommendation 3, section 18 be repealed and the requirements regarding the specification of persons assisting be incorporated into the new proposed section.

6. New section 19(2) be amended:

   6.1. subject to the agreement of the Committee to recommendation 3, to refer to the need to capture the same information on the Register as is recommended in this Report for inclusion in a warrant/authorisation (i.e. by reference to the section number); and

   6.2. to ensure that paragraph (e) also applies to warrants.

7. New section 19A be amended to require that the Responsible Minister be informed as soon as reasonably practicable after an urgent warrant or authorisation had been issued.

8. Subject to the agreement to recommendation 3 that section 22 be repealed and the requirements regarding the term of warrants and authorisations be incorporated in the new proposed section.

9. New section 25(2) be amended to allow the communication of incidentally obtained intelligence for the purpose of avoiding the loss of life at sea in international waters.

10. New section 25(2)(c) be amended to replace the term “national security” with the term “security or defence”.

11. New section 25(3)(d) be amended to remove references to “any other person” and replace it with “any other public authority in New Zealand and any other country”.

12. The Bill be clarified to make it explicit that the Privacy Commissioner should report any issues identified from her consideration of the result of audits provided to her under new section 25A(2)(c) to the Inspector-General who will be responsible for investigating and reporting on those issues.

13. The privacy policy must be reviewed regularly but it must be reviewed at least once every 3 years.

Part 2

The Department recommends that:

14. Section 11(1)(c) be amended to remove the requirement for the concurrence of the responsible Minister.

15. The Department, Parliamentary Counsel and the Office of the Clerk consider any drafting changes required to give effect to the policy position (as discussed by the Privileges Committee) that the House of Representatives be able to make a complaint to the Inspector-General, and present any proposed amendments in the Revision Track version of the Bill.

16. The Bill be amended to include a provision providing that the Inspector-General determines the classification of any reports they prepare, on the proviso that they must–

    16.1. consult with the head of the intelligence and security agency that is the subject of the report;

    16.2. retain the same security classification in respect of any material provided to the IGIS that is quoted verbatim in the report; and

    16.3. otherwise respect the classification of material provided to support the inquiry before finalising the classification.

17. The ISC agree that new section 27(2)(b) be amended to say "…whether and, if not, to what extent…" or similar.

Part 3

The Department recommends that:

18. Existing section 13(6) of the Intelligence and Security Act is expressed to be subject to new section 7A(3) of the Intelligence and Security Act.

19. New section 7A(3) of the Intelligence and Security Act:

    19.1. be moved closer to existing section 13(6) of the Intelligence and Security Act; and

    19.2. be amended to also give the Leader of the Opposition the same right to nominate an alternate, albeit limited to the deputy leader of his or her party.

Appendix 1: Submissions

No.	Submitter	Supports policy intent, Oppose or Neutral	Oral submission
1.	Gregory Warren	Oppose	
2.	Gavin Miller	Oppose	
3.	Adams and Huatau Marae	Support in principle but need effective oversight	
4.	Paul Stitchbury	Oppose	
5.	Dianne Sharma Winter	Support only for the stated purpose of the Bill	
6.	Margaret Harris	Oppose	
7.	Vikram Kumar	Support only for the stated purpose of the Bill	✓
8.	Di Hickman	Oppose	
9.	Ben Simpson	Support only for the stated purpose of the Bill	
10.	Matthew Wilson	Oppose	
11.	Joshua Grainger	Neutral	
12.	Cameron McAlpine	Support only for the stated purpose of the Bill	
13.	David ten Have	Support only for the stated purpose of the Bill	
14.	Ian Mackenzie	Oppose	
15.	Barry Phease	Oppose	
16.	Pakeeza Rasheed	Oppose	
17.	Bevan McCabe	Oppose	
18.	Bart Ludbrook	Oppose	
19.	Reihana Robinson	Oppose	
20.	Maria Sagarzazu	Oppose	
21.	Brendon Grant	Oppose	
22.	Legislation Advisory Committee	Neutral	✓
23.	Garth Williamson	Oppose	
24.	Robert Tobias	Oppose	
25.	Jason Potter	Oppose	
26.	Michael Fincham and Erin Salmon	Oppose	
27.	Valerie Morse	Oppose	✓
28.	Nathan Bregman	Oppose	

29.	Peter Bulmer	Oppose	
30.	Keith Locke	Oppose	✓
31.	Andrew Riddell	Oppose	
32.	Elaine Hampton	Oppose	
33.	Chris Russell	Oppose	
34.	Terry Baucher	Support only for the changes made to oversight legislation	
35.	Stephen Judd	Oppose	✓
36.	Michael Koziarski	Oppose	✓
37.	Francis Devine	Oppose	
38.	Cheryl Lewis	Oppose	
39.	Allan Murray	Support only for the stated purpose of the Bill	
40.	Daniel Richards	Oppose	
41.	Jan Zawadzki	Oppose	
42.	Jonathan Mandeno	Oppose	
43.	Michael Langton	Oppose	
44.	Annemarie Thorby	Oppose	✓
45.	Dr Joel Pitt	Oppose	✓
46.	Robert Anderson	Oppose	
47.	Byron Andrews	Oppose	
48.	Elliot Olsen	Oppose	
49.	David Robb	Support only for the changes made to oversight legislation	
50.	Kit Withers	Oppose	
51.	Clive Teare	Oppose	
52.	Fergus Wheeler	Oppose	
53.	Leslie Margaret Barrett	Oppose	
54.	Brent Jackson	Oppose	
55.	Marianne Macdonald	Oppose	
56.	Glibert van Reenen	Oppose	
57.	Bera MacClement	Support only for the changes made to oversight legislation	
58.	New Zealand Council of Trade Unions	Support only for the changes made to oversight legislation (though the Bill could go further)	✓
59.	Daniel Wright	Oppose	
60.	Malcolm Harbrow	Oppose	
61.	Nicol MacArthur	Oppose	
62.	Jay Queenin	Oppose	

63.	Ryan Wolstenholme	Oppose	
64.	New Zealand Council for Civil Liberties	Oppose	✓
65.	Georgina Preston	Oppose	
66.	James Cone	Oppose	
67.	Anita Evans	Oppose	
68.	Claire Breen	Oppose	
69.	Iona Woodward	Support only for the changes made to oversight legislation	
70.	Simon Terry	Oppose	✓
71.	Jacquelyne Taylor	Oppose	
72.	Shaun McLaughlin	Oppose	
73.	Merryn Bayliss	Oppose	
74.	Mike Scott	Oppose	
75.	Matt Browning	Oppose	
76.	John Oldridge	Oppose	
77.	Rebecca Herald	Oppose	
78.	Kaelan Bhate	Oppose	
79.	Don Carson	Oppose	
80.	Reon Hogg	Oppose	
81.	Rebekah Wilson	Oppose	
82.	Nicolaas Francken	Oppose	
83.	Dr Jacob Edmond	Oppose	
84.	New Zealand Law Society	Support only for the changes made to oversight legislation	✓
85.	Claire Breen	Oppose	
86.	Kate Dewes And Rob Green	Support only for the changes made to oversight legislation	✓
87.	Privacy Commissioner	Oppose	
88.	Father Gerard Burns	Oppose	✓
89.	John Laurence Boomert	Oppose	✓
90.	James Veitch	Oppose	✓
91.	Human Rights Foundation	Oppose	✓
92.	Michael Shallcrass	Support only for the stated purpose of the Bill	
93.	P David J Corke	Oppose	
94.	B A Olsen	Oppose	
95.	Cherie Hereora	Support only for the stated purpose of the Bill	
96.	Richard Keller	Oppose	

97.	Ian Fish	Oppose	
98.	D E Ryan Sheridan	Oppose	
99.	Martin Roberts	Support only for the stated purpose of the Bill	
100.	Alexander Armstrong	Oppose	
101.	Hamish Harding	Oppose	
102.	Andrew Mcpherson	Oppose	
103.	Dr Rhys Jones	Support only for the changes made to oversight legislation (though the Bill could go further)	
104.	Sharyn Black	Oppose	
105.	Frank Macskasy	Oppose	✓
106.	Professor Kevin Broughan	Oppose	✓
106A			
107.	Joyce Campbell	Oppose	
108.	Tech Liberty	Oppose	✓
109.	Greenpeace New Zealand	Oppose	
110.	Helen Crawford	Support only for the stated purpose of the Bill and the changes made to oversight legislation	
111.	Joe Russell	Oppose	✓
112.	Kim Dotcom and Bram van der Kolk	Support only for the changes made to oversight legislation (though the Bill could go further)	✓
113.	John Miller Crawford	Support only for the stated purpose of the Bill and the changes made to oversight legislation	
114.	Sheldon Te Kare	Oppose	
115.	Corey Hulbert	Support only for the changes made to oversight legislation	
116.	Jan Rivers	Oppose	
117.	D'Hondt Michel	Support only for the changes made to oversight legislation	
118.	Environment and Conservation Organisations of New Zealand	Support only for the changes made to oversight legislation	✓
119.	Susan Miller	Support only for the changes made to oversight legislation	✓
120.	InternetNZ	Oppose	✓
121.	Penelope Bright	Oppose	✓

122.	Denis Tegg	Support only for the changes made to oversight legislation	
123.	Reece Robinson	Support only for the stated purpose of the Bill	
124.	John McElhiney	Oppose	