New Zealand Intelligence and Security Bill

This document covers,

- Regulatory Impact Statement: New Zealand Intelligence and Security Bill – Agency disclosure statement

- Addendum to Regulatory Impact Statement: Intelligence and Security Legislation – Information sharing arrangements and, assisting other organisations

This page is deliberately blank.

Regulatory Impact Statement: Intelligence Services and Oversight Bill

Agency Disclosure Statement

5 April 2016

This Regulatory Impact Statement (RIS) has been prepared by the Department of the Prime Minister and Cabinet. It considers options to improve New Zealand's intelligence and security agencies (the agencies) and their oversight regime in legislation. The options presented respond to recommendations made by Sir Michael Cullen and Dame Patsy Reddy (the reviewers) in the *Report of the first Independent Review of Intelligence and Security in New Zealand* (the review), presented to the Intelligence and Security Committee (ISC) on 29 February 2016. It can be accessed by following this link to the Parliament website.

The reviewers were selected due to their significant relevant experience and skills and their high standing in the community. They conducted a thorough and wide-ranging inquiry involving extensive consultation, and gained a deep understanding of how the intelligence community operates.

Successive reviews of the agencies have identified a number of challenges facing the agencies, including significant shortcomings with their legislative arrangements. DPMC has not sought to duplicate these inquiries and will refer throughout this RIS to problems identified in the reviewers' report, in the Performance Improvement Framework 2014 review, and in the Review of Compliance at the GCSB in 2013 (also known as the 'Kitteridge Report').

The review makes 107 recommendations regarding the agencies and their oversight bodies. The scope of the changes, which traverse the agencies, their objectives, functions and powers, together with how they relate to the rest of government and their oversight mechanisms, necessitate high level analysis for this RIS. This RIS should be read alongside the reviewers' report, which provides a greater deal of background to each problem than it is practical to do in this document.

The recommendations made by the reviewers are predominately legislative, with the overarching proposal being for a single Act for the intelligence services and their oversight bodies. This RIS does not analyse the option of merging the intelligence agencies, as Ministers ruled that option out of scope through the terms of reference for the review.

Officials broadly agree with the reviewers' description of the problems and have accepted most of the recommendations, unless there is a strong reason not to. This is partly due to the special nature of these issues but also due to the robustness of the inquiry and the reviewers' intention that their recommendations work together as a coherent package.

This RIS provides more detail about officials' proposals that depart from a recommendation, and about the proposals that involve significant policy development in order to give effect to a broad recommendation.

A number of the problems faced by agencies (as well as the issues that these give rise to) are difficult to discuss publically or to quantify, because of the need to keep operational matters confidential. For this reason, it has not been possible provide significant analysis of the impacts (including of the costs and benefits) of the proposed changes; instead officials have considered matters such as transparency and building public trust and confidence in the agencies, as keystone objectives in lieu of a fully developed cost/benefit analysis.

John Beaglehole
Director - National Security Policy
Department of the Prime Minister and Cabinet

Executive summary

1. The Government Communications Security Bureau (the GCSB) and the New Zealand Security Intelligence Service (the NZSIS) play a vital role in protecting New Zealand's security and advancing New Zealand's interests in the world. However, the intrusive nature of the powers of these intelligence and security agencies (the agencies), and the possible impact of these powers on individuals, require an effective authorisation and oversight regime to maintain the trust and confidence of New Zealanders.

2. The Report of the first Independent Review of Intelligence and Security in New Zealand (the review) made 107 recommendations on how to improve the agencies' legislative framework, including arrangements for their oversight.

3. The review's recommendations can be grouped under the following headings:

    - institutional arrangements, with a view to bringing the agencies into the normal state sector arrangements, with exceptions as appropriate;
    - bringing the agencies under a single Act, including shared objectives and functions and a single warranting and authorisation regime, and enabling better cooperation between the agencies, while retaining their distinctive capabilities and focus;
    - addressing a number of issues in legislation for the first time, including bringing human intelligence within the legislative framework, and providing for certain issues relating to access to and sharing of information; and
    - enhancing oversight and safeguards through strengthening and clarifying the oversight of the agencies by the Inspector-General of Intelligence and Security (IGIS), expanding the role of the Intelligence and Security Committee of Parliament (ISC), and provision for a judicial role within the warranting and authorisation framework.

4. Officials have assessed a number of options for the overarching legislative framework, including maintaining the status quo, making targeted amendments to the current legislation, and implementing the reviewers' recommendation of a new single Act.

5. The preferred option is to develop a single Bill, which will include:

    - integrating the agencies within the public sector;
    - allowing for limited and appropriate targeting of New Zealanders communications;
    - defining national security;
    - authorisation and authorisation in urgent situations;
    - clarifying the role of the Inspector-General of Intelligence and Security;
    - re-defining the Intelligence and Security Committee;
    - providing a role for judicial commissioners, where an agency is seeking a warrant to target a New Zealander;
    - allowing the agencies to create cover for their employees;

- providing the usual immunities to agencies and their staff;
- allowing access to datasets, including case by case access to restricted information;
- creating a framework for arrangements with foreign partners;
- centralising intelligence assessments;
- allowing for the removal of passports, in very limited circumstances;
- standardising offences and protected disclosures; and
- allowing for the collection of outbound passenger information.

6. Implementing the officials' preferred package of proposals will have a range of significant impacts. While these are predominately positive, there are some negatives that will have to be mitigated and balanced. The main impacts of the package can be grouped under the following themes:

    - privacy;
    - human rights; and
    - public trust and confidence in the agencies.

Background

7. Since the enactment of the New Zealand Security Intelligence Service Act 1969 and the Government Communications Security Bureau Act 2003, roles and expectations of the agencies have changed. Shifting international dynamics and technological change have created a more complex threat environment, and there are now much greater expectations from the public for transparency and oversight.

8. Following the discovery of unlawful surveillance of Kim Dotcom in September 2012, a review of the GCSB's compliance was initiated. The Kitteridge Report identified shortcomings with the GCSB's compliance and concluded that the GCSB's legislation was not fit for purpose. The Government Communications Security Bureau and Related Legislation Amendment Bill 2013 was subsequently passed. That Bill was narrowly focused on issues of immediate concern, namely ensuring that the legislative framework governing the GCSB was clearly formulated and provided for the GCSB's activities.

9. With a view to a more systematic review being undertaken, the Intelligence and Security Committee Act 1996 was amended by the Government Communications Security Bureau and Related Legislation Amendment Act 2013. That amendment provided for periodic reviews of the agencies and their governing legislation every five to seven years. Dame Patsy Reddy and Sir Michael Cullen (the reviewers) were appointed to conduct the first review in May 2015.

10. In 2014, the Government also made changes to a number of Acts through the Countering Terrorist Fighters Legislation Act. This Bill was passed under urgency to comply with United Nations Security Council Resolution 2178, which seeks to counter the sudden rise of foreign terrorist fighters travelling from across the world to join

terrorist groups in the Middle East. A number of provisions put in place by that Bill are subject to a sunset clause and are set to expire in March 2017.

11. The terms of reference given to the reviewers asked them to determine (amongst other things):

- whether the legislative frameworks of the agencies are well placed to protect New Zealand's current and future national security, while protecting individual rights;
- whether the current oversight arrangements provide sufficient safeguards at an operational, judicial and political level to ensure the agencies act lawfully and maintain public confidence;
- whether the legislative provisions arising from the Countering Terrorist Fighters Legislation Bill, which expire on 31 March 2017, should be extended or modified; and
- whether the definition of 'private communication' in the legislation governing the GCSB is satisfactory.

12. The terms of reference explicitly required the reviewers to take into account certain matters, including that "traditionally, signals and human intelligence have been carried out separately and the government does not intend to consider merging those functions within a separate agency". The full terms of reference are included in Annex A to this RIS.

Objectives

13. The Government's objectives for the response to the review (outlined in Cabinet Paper One NSC-16-MIN-0007) are to:

- build public trust and confidence in the agencies through a full, open and unclassified policy process, with effective and informed public engagement;
- ensure the new legislative framework is adaptable to changing circumstances and is technology-neutral;
- reflect New Zealand's long standing commitment to human rights, democracy, accountability and the rule of law;
- promote effective, clear and easy to understand legislation;
- develop a framework that facilitates effective engagement and cooperation with New Zealand's international security partners; and
- promote a joined-up and efficient New Zealand Intelligence Community (NZIC) that engages effectively with domestic agencies, including law enforcement agencies.

Status quo and problem definition

14. New Zealand's core intelligence collection agencies are the NZSIS and the GCSB. The NZSIS is a security intelligence organisation and primarily uses intelligence from human sources. The GCSB is a foreign intelligence and information assurance agency, and primarily collects signals intelligence.

15. Oversight of the agencies is exercised through a number of means:

- executive oversight is exercised through Ministerial direction and authorisation;
- quasi-judicial oversight is exercised by the Commissioner of Security Warrants during the warranting process;
- Parliamentary oversight is exercised through the ISC; and
- independent oversight is exercised through the IGIS, the Privacy Commissioner, the Ombudsmen, the Human Rights Commission, the Office of the Auditor General and other like bodies.

16. The wider intelligence community also includes but is not limited to; New Zealand Defence Force, the Ministry of Defence, New Zealand Police, the New Zealand Customs Service and Immigration New Zealand. These agencies are largely not within the scope of the proposed reforms, although may be affected by some of the proposed changes.

17. The agencies and their oversight bodies are governed by both statutory and non-statutory means. The relevant Acts are:

- the New Zealand Security Intelligence Service Act 1969 (NZSIS Act);
- the Government Communications Security Bureau Act 2003 (GCSB Act);
- the Intelligence and Security Committee Act 1996 (ISC Act); and
- the Inspector-General of Intelligence and Security Act 1996 (IGIS Act).

18. There are a number of agencies and groupings of agencies that guide collection and assessment They are:

- the National Security Committee of Cabinet (NSC), which sets intelligence priorities;
- the Officials' Committee for Domestic and External Security Co-ordination (ODESC), which assists NSC by, for instance, specifying particular questions of interest within the intelligence priorities, and maintaining strategic oversight over the delivery of intelligence priorities;
- the Security and Intelligence Group (SIG) of the Department of the Prime Minister and Cabinet, which is responsible for the leadership, coordination and performance of the core NZIC (which includes the NZSIS, GCSB and National Assessments Bureau); and
- the National Assessments Bureau (NAB), which sits within SIG and leads intelligence assessment. The NAB assesses the intelligence output from agencies and external sources, and provides short situational reports and long-

term strategic assessments on overseas political, economic, environmental and security developments.

19. The reviewers identified four overarching problems with the current arrangements:

- a lack of clarity in the legislation means the agencies and their oversight bodies are at times uncertain about what the law does and does not permit, which makes it difficult to ensure compliance;
- inconsistencies between the GCSB Act and the NZSIS Act – in terms of the agencies' functions, powers, and authorisation regimes – create barriers to the agencies working together;
- the systems for authorising the activities of the agencies are not comprehensive. Oversight needs to be strengthened; and
- While intelligence can play an important role in supporting government decision-making, not all of it is useful. It is critical to ensure that the agencies' intelligence collection aligns with the government's priorities and is independently assessed to ensure as far as possible that the end product meets the needs of its users.

20. During consultation, the reviewers also identified common concerns around the need for:

- increased transparency, accountability and oversight;
- greater clarity in the legislation about what the agencies can and cannot do; and
- a strong emphasis on protecting individual rights and freedoms.

21. Officials broadly agree with the reviewers' conceptualisation of the problem and are satisfied that they conducted a thorough investigation and analysis to reach it. Further, these themes are generally consistent with those identified by earlier reviews. For instance, the 2014 Performance Improvement Framework (PIF) concluded that the agencies need to be customer focused, improve their capabilities, address public trust and confidence and to work collaboratively. The Kitteridge Report proposed to bring the agencies more into the state sector, increase legislative clarity and increase oversight. Successive inquiries by the Inspector General of Intelligence and Security have also identified shortcomings which need to be addressed in legislation.

Critical issues

22. **Public trust and confidence in the agencies:** a central problem identified in the review is a lack of public trust and confidence in the agencies. In a survey carried out in 2014 by the Privacy Commissioner, 52 per cent of respondents were concerned about surveillance by New Zealand intelligence agencies. Another 2014 poll found that 29 per cent of New Zealanders think that the New Zealand intelligence agencies are interested in their private communications. These statistics reflect both a significant distrust of the intelligence agencies and a misunderstanding of their objectives, abilities, and legal framework. The reviewers identified a lack of clarity in the agencies' governing legislation (and that of oversight bodies) as well as the agencies' secretive culture and reluctance to communicate with the public, as contributing factors.

23. **Co-operation:** a lack of co-operation between key agencies in the security sector is a barrier to lifting the sector's performance. Although this is not easily quantified, this was a common theme in both the reviewers' report and in officials' consultation with government agencies. The most important relationships are between the agencies themselves, between the agencies and Police and between the agencies and other entities such as NZDF, Customs and Immigration New Zealand. Co-operation between the agencies themselves is important because certain operations will require the NZSIS to draw upon the specialist capabilities of the GCSB and vice versa. The reviewers' report discusses case studies of when this might be important such as identifying foreign terrorist fighters. Barriers to cooperation are partly due to different cultures and methods, and are reinforced the vastly different warranting regimes contained in the respective Acts. Other agencies also need to draw upon the specialist skills of the agencies. As Ministers noted at the National Security Committee in April, the GCSB has not been able to provide assistance to Police in a timely or effective manner. Consultation has identified a lack of legislative clarity as a key barrier.

24. **Changing threat environment:** the security challenges associated with globalisation and technological change are well documented. The threat environment has been in a state of flux for some time and continuous change has become a new normal. Where there was once a strong distinction between the domestic and the international threat environment, the boundaries are now becoming blurred, and threats now reach into New Zealand from elsewhere with relative ease and speed. The National Cyber Policy Office reported in 2015 that 80% of New Zealanders now report having experienced a cyber security breach. The reviewers pointed out that 'the law needs to be framed in a way that allows the government to respond to threats as they evolve'. Specific problems in this regard include outdated conceptions of security, prohibitions on domestic intelligence collection, and impediments to cooperation between the agencies.

25. **Legislative coherence:** the statutory authority for New Zealand's intelligence agencies and their oversight bodies is spread across a range of Acts with the central acts being the NZSIS Act 1969 and the GCSB Act 2003. The different drafting styles, definitions and regimes for activities create difficulties in interpretation for the agencies, oversight bodies, and the public.

26. **Oversight:** The secret nature of the agencies' activities means that the public needs to have confidence in independent oversight mechanisms to ensure the agencies are meeting expectations of transparency, political impartiality, and accountability. Oversight of the New Zealand intelligence agencies is exercised in an array of ways and this must be reviewed periodically to ensure that the settings are correct. Officials share the reviewers' view that New Zealand has a robust system for intelligence oversight but there are a range of small changes that must be made to ensure that the system works effectively, is appropriately balanced, is easy to understand, and meets the expectations of New Zealanders.

Analysis of options

27. Four overarching policy options were assessed:

- maintaining the status quo;
- non-legislative options;
- targeted amendments to the legislative framework governing the agencies and oversight mechanisms; and

- repealing the relevant intelligence and security legislation, and replacing it with a single Act.

Maintaining the status quo

28. Officials do not consider maintaining the status quo to be a feasible option.

29. The status quo would not gain the confidence of New Zealanders, allow for the modernisation of the intelligence agencies, give effect to the reviewers' recommendations or meet the Government's objectives for the review. The agencies would continue to operate with antiquated legislation that will increasingly struggle to adapt to national security threats, and New Zealanders' security would not be as effectively protected.

30. Increasing media focus on the intelligence agencies in recent years, in New Zealand and in likeminded countries, indicates that New Zealanders' expectations of transparency, accountability and oversight from the intelligence agencies are increasing. Failing to take the opportunity to make improvements in these areas in the first review of the intelligence agencies would be a missed opportunity.

31. At the same time, New Zealand's intelligence agencies are dealing with a new set of security threats which are well documented in the review and elsewhere. This requires the agencies to have flexible, technology-neutral legislation that enables cooperation and can adapt to changing circumstances. Officials see the review as an important chance to adapt the agencies capabilities' and powers to changing circumstances.

32. Temporary provisions in the Countering Terrorist Fighters Legislation Bill that expire on 31 March also require legislative change if they are to be renewed.

Non-legislative options

33. The agencies, and their oversight bodies, are creatures of statute, and can exercise significantly intrusive powers against individuals. Giving effect to both officials' objectives and the reviewers' recommendations will require substantial legislative change. This is reflected in the form of the reviewers' recommendations, which are mostly proposals for legislative change. Non-legislative changes do not offer any ability to make substantive or real changes.

Targeted amendments to the legislative framework governing the agencies and oversight mechanisms

34. The third option is to undertake a range of targeted amendments to the existing legislation governing the agencies, and their key oversight bodies the IGIS and the ISC.

35. The reviewers found that the current legislative framework for the agencies has number of deficiencies, including gaps in coverage, a lack of consistency between the two Acts, difficulties of interpretation, and a failure to keep pace with technological change. It might be possible to make targeted amendments to address a number of these issues. But given the range of legislation that would require amending, and the different legislative history and background of those Acts, it would not support the objective of establishing effective, clear and easy to understand legislation.

36. Creating a single piece of legislation will make clear the consistency of purpose and linkages across the NZIC. Targeted amendments, however, would not provide the same inherent support or clarity to this objective.

37. Additionally, while targeted amendments do not preclude the creation of a single warranting and authorisation regime for both the agencies, attempting to achieve the same outcome by amending two Acts could result in even more confusing legislation, and continue the very real difficulties the agencies now face in working together to achieve better outcomes for New Zealand.

Replacing existing intelligence and security legislation with a single Act (preferred option)

38. As the reviewers note, the NZSIS and GCSB have separate functions and different ways of operating due to their distinct histories and different legislative regimes. The threat environment faced within New Zealand and abroad is rapidly evolving. The growth of transnational violent extremism, international organised crime and hostile cyber threats from abroad suggests that there is a pressing need to ensure that the agencies can effectively coordinate their efforts to protect New Zealand and its people. Whether all of these threats pose clear and current dangers to New Zealand (and some do), new and evolving threats require new approaches and methods, if they are to be effectively detected and mitigated.

39. Accordingly, officials' preferred option is to replace the existing legislation governing the agencies and their oversight mechanisms with a single proposed Intelligence Services and Oversight Act. This approach is in line with the reviewers' recommendations.

40. With several exceptions, officials largely support the reviewers' recommendations with regard to the formulation and purpose of the proposed Act. The Act should have the following purpose: "to secure New Zealand as a free, open and democratic society".

41. As a single Act will consolidate the objectives and functions of the agencies, it will also promote easy to understand and adaptable legislation, which should in itself go some way to meeting the Government's objectives.

42. A single Act makes the legislation for the agencies and their oversight bodies more accessible to the public and enables a consistent set of principles. This is consistent with the officials' objective of developing public trust and confidence in the NZSIS and GCSB.

43. We also consider it highly desirable to support the NZSIS and GCSB working together effectively. A single Act allows for the establishment of a warranting and authorisation regime encompassing the activities of both agencies. This will ensure clarity and alignment between the agencies about what is allowed to be undertaken on specific operations.

44. Further, a new Act with consistent language and a simplified framework, this approach will make establishing an adaptable and technology-neutral legislative framework far more achievable than individually amending the existing legislation.

Analysis by issue

45. The preferred option is for a single Bill to implement the package covering the following issues:

- integrating the agencies within the public sector;

- allowing for limited and appropriate targeting of New Zealanders communications;
- defining national security
- authorisation and authorisation in urgent situations;
- clarifying the role of the Inspector-General of Intelligence and Security;
- re-defining the Intelligence and Security Committee;
- providing a role for judicial commissioners, where an agency is seeking a warrant to target a New Zealander;
- allowing the agencies to create cover for their employees;
- providing the usual immunities to agencies and their staff;
- allowing access to datasets, including case by case access to restricted information;
- creating a framework for arrangements with foreign partners;
- centralising intelligence assessments;
- allowing for the removal of passports, in very limited circumstances;
- standardising offences and protected disclosures; and
- allowing for the collection of outbound passenger information

46. This section outlines the problems, options and impacts for each of the issues. A summary of overarching impacts follows this section.

Integrating agencies within the public sector

Status quo

47. The NZSIS grew out of Police Special Branch and existed without a legislative base until the passing of the NZ Security Intelligence Service Act 1969. At the time it was considered that the terms and conditions for NZSIS employees needed to be concealed from public scrutiny. This led to the NZSIS being established outside the core public service legislation. Today the State Sector Act 1988 and the Employment Relations Act 2000 do not apply to the NZSIS. The Director of Security is a statutory officer appointed by the Governor-General on the recommendation of the Prime Minister.

48. The GCSB was originally part of the New Zealand Defence Force but became a non-public service department in 1989. In 2003 the GCSB was established as a department of state (a public service department) but was excluded from some parts of the State Sector Act 1988 regime. The Employment Relations Act 2000 does, however, apply to the GCSB. The Director of the GCSB is a statutory officer appointed by the Governor-General on the recommendation of the Prime Minister.

Problem

49. The State Sector Act 1988 sets out the appropriate standards of conduct for public agencies and employees. The NZSIS is not covered by the rules, procedures and codes of the State Sector Act 1988, with the effect that its staff are not afforded the same protections as state sector employees (for example, collective bargaining does not apply). The GCSB is only partially covered by the rules, procedures and codes of the Act. There are a range of problems with these arrangements, including fewer employment protections for NZSIS staff, and the agencies operate outside of public sector norms and are not subject to the same codes of behaviour.

50. The reviewers' findings echoed the conclusions of earlier inquiries. The 2014 Performance Improvement Framework stressed the need for the New Zealand Intelligence Community to improve in leadership and governance as well as values, behaviour and culture. The need to make changes in this area was also a significant theme of the Kitteridge Report, which found the culture of the GCSB to be a factor in its non-compliance. The report noted that 'much of the organisation is isolated and disconnected from the regular public service. This disconnection means that GCSB's responsiveness to public sector changes and adoption of new norms is often very slow'.

Reviewers' recommendations

51. The NZSIS should be established as a public service department.

52. The State Sector Act 1988 should apply to both the agencies, with appropriate exemptions agreed in consultation with the State Services Commission.

Preferred option

53. Officials support the recommendation to bring the NZSIS (in its entirety) and GCSB further under the ambit of the State Sector Act 1988. It is proposed that the NZSIS be established as a public service department, with any appropriate exemptions for both agencies.

Impacts

54. *Leadership and governance* – The State Services Commissioner will appoint and dismiss both directors.

55. *Norms and standards* - The agencies will be brought more fully into the public sector. In addition, the NZSIS will become subject to the Code of Conduct for the State Services - Standards of Integrity and Conduct (or a variation of this) for the first time. This will advance officials' objective of improving public trust and confidence in the agencies.

56. *Employment relations* - NZSIS employees will be subject to the freedom of association and collective bargaining provisions of the Employment Relations Act 2000. The GCSB is already a unionised workforce; there is no compelling reason why this cannot also be the case for the NZSIS (especially in light of the fact that the NZSIS already has an effective and respected staff association). Under the State Sector Act 1988, the State Services Commissioner is responsible for the negotiation of collective agreements, though in practice this is delegated to chief executives. We anticipate that the same arrangements will apply to the NZSIS.

57. *Access to the ERA* - NZSIS employees will also gain access to the Employment Relations Act's personal grievance provisions, which will allow them to pursue a personal grievance for a claim of unjustified dismissal. GCSB employees currently

enjoy this right. Agencies do have some concerns about giving access to the ERA where the agency is dismissing an employee because they no longer hold the required security clearance (it is a condition of employment in both the NZSIS and GCSB that employees obtain and maintain the necessary security clearance. The GCSB has indicated that it has experienced cases where the ability to hold a security clearance (where there is an existing review mechanism through the IGIS) has been conflated with procedural fairness and subsequent decision-making during the dismissal of the employee concerned. That is clearly a risk, but officials do not have a clear sense of the scale of this risk.

58. *Suitability to hold a clearance* - We consider, however, that matters relating to the Director of Security's recommendation about whether a person should maintain a national security clearance should remain within the remit of the IGIS. The Employment Relations Act 2000 should be amended so that, when such a person's suitability to hold a security clearance is raised as part of a personal grievance under the Employment Relations Act framework, the Employment Relations Authority and the Employment Court must recognise the jurisdiction and particular competence of the IGIS to inquire into complaints about a security clearance recommendation from the Director of Security. In the year to June 2015, the IGIS received eight complaints from individuals whose employment had been affected by losing their security clearance and initiated inquiries into four of those cases.

59. *Effect of a decision to dismiss an employee* - The decisions of the relevant Director as to whether to renew the employee's clearance (and to bring their employment to an end) will be able to be considered in the employment relations context. Where the IGIS has considered any complaint of the affected employee in relation to the Director of Security's recommendation, it is envisaged that the IGIS would provide advice to the Employment Relations Authority (or the Employment Court, as the case may be), which can then consider the personal grievance without needing to delve into the Director of Security's actions.

Allowing for the limited and appropriate targeting of New Zealanders

Status quo

60. The NZSIS is a domestic security focused agency and as such, can investigate New Zealanders with the appropriate authorisation. On its face, section 14 of the GCSB Act prevents the GCSB from taking any action for the purpose of intercepting the communications of New Zealanders when performing its intelligence gathering function. However, as set out in the review at length, the protection afforded by section 14 is not as comprehensive as is commonly understood, as it is subject to exceptions so that the GCSB can collect information about New Zealanders where for instance, they fall within the definition of an 'agent of a foreign power', or if the GCSB is assisting another agency.

Problem

61. The section 14 restriction does not recognise that threats can come from an individual who happens to hold a New Zealand passport. The restriction is peculiar and makes little sense. Further, the lack of clarity as to when the GCSB can target New Zealanders is also unsatisfactory. Moreover, the GCSB is also unnecessarily precluded from using its extensive capabilities to assist other agencies.

62. The "agent of a foreign power" exception has proven difficult for the GCSB to apply in practice. Furthermore, the 2013 amendments to the GCSB Act, which were intended to enable the GCSB to assist other agencies (such as the NZSIS and the Police), have

not given the GCSB the legal certainty it seeks so it can assist other agencies in some of the situations where they would be of use. In particular, the GCSB is limited by the other agency's power or authorisation. If, for example, the NZSIS does not know the actual identity of the person of interest, it cannot get a warrant and the GCSB cannot assist it.

63. There are also workability issues around the implementation of section 14. It can be very difficult to assess the nationality of a person when intercepting modern communications, especially where the person may only be identifiable by an online persona. New Zealanders, including dual nationals, are present in a great many countries across the world.

64. In short, the GCSB is not able to sufficiently contribute to the protection of New Zealanders and New Zealand's national security in important circumstances when its capabilities are required.

Reviewers' recommendations

65. Remove the prohibition on the GCSB targeting New Zealanders when performing its intelligence collection function. Protections for New Zealanders should be implemented through a strengthened authorisation framework, and in particular New Zealanders, should only be able to be targeted when they pose a risk to national security.

Preferred option

66. Officials agree with the reviewers' recommendation and propose not to include the section 14 prohibition in a new Act. Instead, protections for New Zealanders (meaning both citizens and permanent residents, but not people with temporary residency) will be implemented through the warranting system; that will impose restrictions on both agencies who wish to exercise their powers in respect of a New Zealander. The agencies will only be able to take actions for the purpose of collecting intelligence about a New Zealander if they obtain a tier one warrant (described in the authorisation section below), which will require approval from both the Attorney-General and a judicial commissioner. Further, applications for a tier one warrant in respect of a New Zealander will generally be for the objective of protecting New Zealand's national security. The agencies will only be able to obtain a warrant in respect of a New Zealander under the other two proposed objectives (New Zealand's international relations and well-being, and New Zealand's economic well-being) where they can establish the New Zealander is an "agent of a foreign power".

Impacts

67. *Role of the GCSB in protecting New Zealanders* - The primary impact of removing section 14 of the GCSB Act is to allow both agencies to counter threats regardless of whether the source of the threat happens to be a New Zealand citizen or permanent resident, or not. The current nationality distinction makes little sense. To ensure the agencies act within the scope of their powers, an application for a warrant in respect of a New Zealander will require the approval of both the Attorney-General and a judicial commissioner, and the application for the warrant will be subject to review by the Inspector-General (as is the case of all warrants).

68. *Privacy* – In some circumstances, privacy will be impacted by this change. However, due to the increased safeguards for instances where New Zealanders can be targeted, officials are confident that the changes will not amount to an overall negative impact on the privacy of New Zealanders, while allowing the agencies to collect intelligence in the range of situations where that is necessary to protect national security. Privacy and

other human rights impacts are discussed in more depth in an impact summary toward the end of this RIS.

Defining national security

Status quo

69. The NZSIS Act includes a definition of 'security' which governs the circumstances under which the NZSIS can target New Zealanders. 'Security' is defined to mean:

- The protection of New Zealand from acts of espionage, sabotage and subversion, whether or not they are directed from or intended to be committed within New Zealand:
- The identification of foreign capabilities, intentions or activities within or relating to New Zealand that impact on New Zealand's international well-being or economic well-being:
- The protection of New Zealand from activities within or relating to New Zealand that –
    - Are influenced by any foreign organisation or any foreign person; and
    - Are clandestine or deceptive, or threaten the safety of any person: and
    - Impact adversely on New Zealand's international well-being or economic well-being:
- The prevention of any terrorist act and of any activity relating to the carrying out or facilitating of any terrorist act

70. The GCSB is prohibited from targeting New Zealanders under its collection function and there is no definition of security in the GCSB Act.

Problem

71. There are a number of problems with the definition of security in the NZSIS Act which mean it is not fit for purpose in a new Act. Firstly it does not provide much clarity around what type of activities or threats activities the agencies can target New Zealanders for. This is a problem for both the general public, who have little understanding of the activities of the agencies, and also for the agencies, which do not have sufficient clarity around when they are able to carry out their functions.

72. A Curia Market Research Poll in 2014 found that 29% of randomly selected adults thought that the New Zealand intelligence agencies would be interested in their communications. This reflects a lack of understanding of the agencies' functions and the legal framework within which they operate.

73. A lack of clarity has also created a barrier to the performance of the agencies. This has been particularly problematic for the GCSB, who have been appropriately cautious about the interpretation of their legislation, particularly in light of the concerns expressed in the Kitteridge Report. This approach has created significant problems around assisting other agencies who have required the assistance of GCSB in certain circumstances.

74. The definition of security is also outdated and primarily focused on the collection of human intelligence. It would therefore not be suited to the GCSB. It also does not

account for collecting intelligence on non-traditional security threats such as cyber threats or transnational crime.

Reviewers' recommendation

75. An important part of the reviewers' package of recommendations is to include a definition of national security in a single new Act which would outline the circumstances under which the GCSB and the NZSIS could target New Zealanders. The reviewers propose that the intelligence agencies have three intelligence collection objectives: national security, economic wellbeing and international relations and wellbeing. Under their proposal, GCSB and NZSIS would not be able to target New Zealanders under the agencies' other two collection objectives of economic wellbeing and international relations and wellbeing (unless that person was an 'agent of a foreign power').

76. The reviewers propose a definition that is restricted to protecting, as opposed to advancing, New Zealand's interests. An application for a warrant would also have to demonstrate how five other criteria, including necessity and proportionality, were satisfied. These five criteria are discussed in the authorisation regime section of this RIS.

77. The proposed definition of national security forms a key part of the package of recommendations put forward by the reviewers and has impacts for the operation of the warranting system and other features such as the way that agencies are engaged to assist other agencies.

78. The reviewers' proposed definition is as follow: 'National security' means the protection against –

- *Threats or potential threats, to New Zealand's status as a free and democratic society from*
    - *Unlawful acts, or*
    - *Foreign interference;*
- *Imminent threats to the life and safety of New Zealanders overseas;*
- *Threats, or potential threats, that may cause serious harm to the safety or quality of life of the New Zealand population ;*
- *Unlawful acts, or acts of foreign interference, that may cause serious damage to New Zealand's economic security or international security or international relations;*
- *Threats, or potential threats, to the integrity of information or infrastructure of critical importance to New Zealand;*
- *Threats, or potential threats, that may cause serious harm to the safety of a population of another country as a result of unlawful acts by a New Zealander that are ideologically, religiously or politically motivated;*
- *Threats, or potential threats, to international security.*

79. This definition would be an improvement upon the status quo in that it provides more clarity to the agencies and to the general public about the types of activities they are entrusted with protecting New Zealand against. It also includes thresholds such as

‘serious harm’, ‘imminent threats’ and ‘critical infrastructure’ to assure the public that intrusive powers will only be used to investigate serious threats to New Zealand.

80. However, the proposed definition also gives rise to a series of potential problems. There is a risk that any attempt to define national security will interact with other definitions across the statute book. National security is used but not defined in statutes such as the Civil Aviation Act 1990, the International Crimes and International Court Act 2000, the Policing Act 2008, and the Immigration Act 2009; and is defined differently in the Passports Act 1992 and the Telecommunications (Interception Capability and Security) Act 2013. While it would be possible to look across and attempt to rationalise all of these definitions, doing so is outside the scope of this package of reforms.

81. While the reviewers’ definition provides greater clarity than the status quo, there is also significant ambiguity within the definition relating to what would be in scope, and what would meet the various thresholds such as ‘imminent’, ‘critical’, and ‘serious’. For example it is difficult to find a clear authority for the agencies to investigate transnational criminal activity such as people smuggling and drug trafficking. It is also unclear whether certain activities the agencies should appropriately be investigating, such as a small scale terrorist event, would meet the threshold of ‘serious harm’.

Alternative 1: No definition of national security

82. A different approach would be not to define national security and to leave it to the Attorney-General and judicial commissioner to make a judgement about whether activities of concern constitute a threat to New Zealand’s national security.

83. This approach would give the Minister and judicial commissioner increased flexibility in deciding what constitutes a threat to New Zealand’s national security. This would satisfy the Government’s objective of ensuring the legislation is adaptable to changing circumstances and is technology neutral. It would also reflect the longstanding constitutional convention that national security issues are the prerogative of the Executive branch of government, with the check of the judicial commissioner.

84. It would also reflect practice in other jurisdictions, notably the United Kingdom, which is current updating its intelligence legislation in the form of the Investigatory Powers Bill. That Bill does not define national security, thus enabling the legislation to respond to a changing threat environment.

85. On the other hand, were this option adopted, it would be very unclear which activities the intelligence agencies were authorised to investigate. This would be the case for both the agencies and the general public. It would therefore fail to satisfy two key Government objectives: building public confidence in the intelligence agencies and promoting effective, clear and easy to understand legislation. Further, without a definition of national security, there is arguably less protection for New Zealanders, who under the proposed regime can only be the subject of a warrant if they pose a risk to national security.

Alternative 2: An alternate provision for limiting the ability of the agencies to apply for warrants targeting New Zealanders (preferred option)

86. Another option is to create a closed list of activities and threats for which the agencies could target New Zealanders under the national security objective. This would serve a similar purpose to a definition, but sidestep the problems associated with defining national security. The list could also address some of the issues around lack of clarity in the scope and thresholds of the reviewers’ proposed definition.

87. The obvious advantage of creating a more comprehensive list would be that it would create more clarity for the general public and the agencies as to the circumstances in which the agencies could target New Zealanders.

88. A national security test (such as set out at paragraph 95) would allow for appropriate flexibility while also making it much clearer which activities the agencies are permitted to investigate.

89. The reviewers used the definition of national security as a way to constrain the agencies when the proposed to target a New Zealander. They do not appear to have considered the definition would have other uses. Creating a list of activities that would allow the agencies to apply for such a warrant offers the same restrictions, generally speaking, without the complications posed by seeking to define national security itself. The key risk associated with this would primarily be with the impact that modification would have on the overall package of proposed reforms. The definition has been calibrated to operate as a central part of the warranting system, along with the definition of 'agent of a foreign power'; and provisions relating to assistance. For this reason, any changes to the definition would need to be carefully considered and may necessitate change to those elements of the package.

90. Officials have put together a possible alternate provision which would provide that when an agency wishes to target a New Zealander the agency applying must also satisfy the judicial commissioner and the Attorney-General that:

- The proposed activity is necessary to contribute to the protection of national security; and
- The proposed activity is necessary for the collection of intelligence relating to one or more of the following activities in New Zealand or overseas.
    - Terrorism or violent extremism
    - Espionage or other foreign intelligence activity
    - Sabotage
    - Proliferation of chemical, nuclear, radiological or biological weapons
    - Activities which may be relevant to serious crime and involve:
        - The movement of money, good or people;
        - The use or transfer of intellectual property
        - The improper use of an information infrastructure
        - Damage to New Zealand's international relations or economic security
    - Threats to, or interference with, information (including communications) or information infrastructure of importance to the Government of New Zealand
    - Threats to international security
    - Threats to New Zealand Government operations in New Zealand or abroad

- Threats to New Zealand's sovereignty, including its territory or border integrity and system of government

- Threats to the life or safety of New Zealanders.

91. Officials' preferred option to ensure New Zealanders who are not agents of a foreign power are only the subject of a warrant in appropriate cases is to adopt this alternate provision or something similar based on this approach of having national security, undefined, forming an initial threshold for a list of specific things. This initial threshold is very important, as it sends a clear signal to the agencies that they ought not to become involved in matters that are not of significance at a national level, or are more properly the province of another agency, such as Police.

Impacts

92. *Workability* - Leaving "national security" undefined avoids the potential problems that a definition would bring (discussed above) and builds in flexibility to deal with change, such as changes in the threat environment.

93. *Transparency* - Coupling national security with a specific list brings an enhanced level of transparency around the types of activities and threats that the agencies can be authorised to investigate. The reviewers have identified the lack of transparency in the current legislation as a significant shortcoming and noted that many of the submissions they received from the public made comments to this effect.

94. *Legislative clarity* - Another strong benefit is clarity for the public, the agencies and other government departments about what activities and threats the agencies are able to investigate. This should improve the overall effectiveness of intelligence collection and interagency cooperation.

Authorisation

Note: Annex B provides an overview of the proposed warranting regime.

Status quo	**Reviewers' proposal**	**Officials' preferred option**
Separate warranting regimes in the GCSB Act 2003 and the NZSIS Act 1969 **Problems:** Different warranting regimes create a barrier to cooperation, the regimes are difficult to understand, regimes do not cover all of the agencies activities (eg; legal surveillance in public places)	One three tiered regime – all activities (including lawful) covered in the regime, common powers, clear description of powers, triple lock of oversight **Problems:** Common powers would expand the capacity of the warranted powers of GCSB significantly (they could conduct searches of private property for example)	Common regime as proposed by reviewers but with separate powers. Joint warrants for if GCSB and NZSIS need to conduct joint operations. This option has all the benefits of the reviewers' proposal including triple lock of oversight and more legislative clarity without expanding the powers of the GCSB into new areas. Support establishment of Ministerial Policy Statements but they will not be mandatory

Status quo

95. The NZSIS and GCSB have separate warranting frameworks. Warrants in the NZSIS Act are separated into two categories: domestic intelligence warrants and foreign intelligence warrants. If the activity targets a New Zealander or a place occupied by a New Zealander, the warrant must be issued jointly by the responsible Minister and the Commissioner of Security Warrants.

96. Authorisation in the GCSB Act comes in the form of interception warrants and access authorisations. Interception warrants allow the GCSB to use interception devices to intercept communications, while access authorisations permit access to an 'information infrastructure' (such as a communications or information technology system or network). Unlike NZSIS warrants, GCSB authorisations can be class based, meaning that they allow the GCSB to target a set of people or things as opposed to specific individuals or things

Problem

97. The existing warranting frameworks have some broad similarities, but significant differences. The lack of alignment in the existing frameworks is a significant barrier to effective cooperation, and often leads to multiple applications in respect of the same target(s).

98. The NZSIS legislation is antiquated and difficult to read, and has not kept pace with modern technology as the public would expect. This is not consistent with the goal of legislative clarity and building public confidence. The lack of clarity also means the agencies are unsure about when they can apply their powers.

99. There is currently only internal authorisation for lawful activities of the agencies (such as the NZSIS conducting surveillance in a public place, or open source collection). These activities constitute a significant part of the agencies' activities, but this is not apparent on the face of the legislation.

Reviewers' recommendation

100. The reviewers recommended an entirely new warranting regime. The reviewers did not set out a detailed proposal but their starting point is that there must 'be some form of authorisation for all the agencies' activities that involve gathering information'. The reviewers proposed therefore a three tier system:

- Tier 1: warrants (targeting New Zealanders and requiring authorisation from the Attorney General and a judicial commissioner),
- Tier 2: authorisations (the same activities as warrants but not for the purpose of targeting New Zealanders, requiring authorisation from the Attorney General); and
- Tier 3: Ministerial policy statements (a policy statement approved by a Minister, to outline the conduct of lawful activities that involve gathering information about individuals and organisations).

101. The reviewers propose that warrants and authorisations would permit the following types of activity where that activity would otherwise be unlawful under other legislation:

- interception of communications;
- acquisition of information held by third parties;

- accessing information infrastructures;
- surveillance (including using video, listening and electronic tracking devices); and
- use of human sources.

102. The reviewers propose a legal test for the warrant or authorisation with five criteria. Before issuing a warrant, the Attorney General (and the judicial commissioner in the case of tier 1 warrants) would need to be satisfied that:

- The proposed activity is necessary either:
  - for the proper performance of one of the agency's functions;
  - to test, maintain or develop capabilities: or
  - to train employees for the purpose of performing the agency's functions.
- The proposed activity is proportionate to the purpose for which the authorisation is sought;
- The outcome sought cannot reasonably be achieved by less intrusive means;
- There are satisfactory arrangements in place to ensure nothing will be done in reliance on the warrant beyond what is reasonable and necessary for the proper performance of a function of the agencies; and
- There are satisfactory arrangements in place to ensure that information is only obtained, retained, used and disclosed in accordance with legislation.

103. Implicit within the reviewers' recommendations around authorisation is that the new warranting regime would merge the powers of the agencies, meaning that they would likely have shared capabilities. This is would amount to a significant expansion of capabilities for both agencies, especially the GCSB (for instance, the proposed regime would allow GCSB staff to covertly search private properties). Officials consider any such expansion unnecessary.

104. The proposed regime provides for a broad set of powers, but does not clearly identify what the agencies would be able to do under a tier 1 or tier 2 warrant. This conflicts with the objective of creating effective, clear and easy to understand legislation. A lack of clarity may also have legal ramifications. Officials note that *Choudry v Attorney-General* held that intrusive capabilities must be clearly spelt out in legislation.

Common warranting regime with clear and distinct powers (preferred option*)*

105. The reviewers' broad strokes have needed more work to flesh out the detail of an authorisation regime that is appropriate and fit for purpose. The proposed warranting regime departs from the reviewers' recommendations in that it maintains distinctions between the powers of the NZSIS and the GCSB.

106. The particular objectives underpinning officials' preferred option with respect to the warranting regime are to:

- simplify the legislation to make it easier for the agencies and the public to understand what the agencies' powers are, and under what circumstances they can be exercised. This will enhance transparency of the activities of the agencies and strengthen oversight;

- Describe more clearly the powers available to the agencies and provide a clear legal basis for the activities of the agencies, and the protections and safeguards that apply;

- consolidate and harmonise the existing powers of both agencies under a single, framework, whereby similar activities are authorised in the same way – noting that this may lead to new labels or terminology for existing authorised activity;

- maintain appropriate distinctions between the NZSIS and GCSB powers reflect their different roles and capabilities, within the context of a unified framework that facilitates greater coordination and collaboration. Taking this approach is again likely to lead to new labels for existing powers;

- make clear that only activity that would otherwise be unlawful requires a warrant; and

- remove unnecessary barriers to effective cooperation between agencies.

107. The agencies would have a shared set of primary powers under a warrant, with the exception of measures for cyber defence which would remain a power of the GCSB only. The powers are to:

- Intercept communications;

- Search a place or thing (including information infrastructures);

- Seize physical and non-physical things (including information);

- Conduct surveillance (including visual surveillance and electronic tracking);

- Collect intelligence through human sources or intelligence officers (including online) where the officer or source may be required to undertake an unlawful act (e.g. join a terrorist group);

- Request a foreign partner to undertake activities that would require a warrant for GCSB or NZSIS to do;

- Use its powers to give effect to do anything else necessary and reasonable to maintain or obfuscate collection capabilities;

- Use its powers to give effect to do any other act that is necessary or desirable to protect the security and integrity of communications and information infrastructures of importance to the Government of New Zealand, including identifying and responding to threats or potential threats to those communications and information infrastructures. (GCSB only).

108. These are plain language descriptions of the powers of both agencies and provide transparency as to what the agencies intend to do under a warrant. Both NZSIS and GCSB have these powers (excluding the new power of intelligence collection through human sources involving unlawful activity). In GCSB's case, these largely fall under its current power to access information infrastructures. The approach would provide greater clarity and transparency about the powers of the agencies, particularly the GCSB.

109. While these powers would be shared by both agencies, the differences between the agencies would maintained in how they give effect to these powers. The NZSIS and GCSB will often effect these powers in quite different ways. For example, the NZSIS may conduct surveillance by installing a surveillance device; the GCSB may do so by remotely accessing an information infrastructure.

110. To maintain an appropriate distinction in the powers of the agencies, this option consolidates the powers to give effect available to the agencies in the GCSB Act and NZSIS Act while drawing on section 55 (regarding surveillance device warrants) and sections 110 and 112 (regarding search warrants) of the Search and Surveillance Act 2012, with appropriate modifications for intelligence and security agencies. The full suite of powers would be available to the NZSIS as this aligns with its current capabilities. The GCSB, given its different role and capabilities, will only have access to a subset of those powers.

111. Both agencies would be able to:

- access (instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of, including any audio or visual capability) an information infrastructure;
- install, use, maintain or remove an interception device;
- extract and use any electricity; and
- install, maintain, use or remove an audio or visual surveillance device to maintain the operational security of a warranted activity.

112. The NZSIS only would be able to exercise the following powers (unless the agencies were operating under a joint warrant, when they would be available to both agencies):

- install, use, maintain or remove a visual surveillance device;
- install, use, maintain or remove a tracking device;
- break open or interfere with any vehicle or other thing;
- enter any place, vehicle or other thing authorised by the warrant;
- take photographs, sound and video recordings, and drawings of a place, vehicle or other thing searched, and of anything found in or on that place vehicle or other thing;
- use any force in respect of any place vehicle or thing that is reasonable for the purposes of carrying out a search or seizure;

- to bring and use in or on the place, vehicle, or other thing search any equipment, and to use any equipment found on the place vehicle or thing; and

- to bring and use in or on the place vehicle or other thing searched, a dog;

- the specific powers would be supported by the following general ancillary powers:

- any other act that is reasonable in the circumstances and reasonably required to achieve the purposes for which the warrant was issued;

- anything reasonably necessary to conceal the fact that anything has been done under the warrant, or reasonably necessary to keep warranted activities of the agencies covert.

113. These powers would be framed in a way that more closely aligns with the Search and Surveillance Act 2012, and ensures greater coherence across both agencies.

114. Modern intelligence operations may require skills and capabilities from both agencies. Accordingly, the option also allows both agencies to access the full suite of powers if a joint warrant is approved by the Attorney-General (and judicial commissioner in the case of tier one warrants).

115. Tier one warrants (targeting a New Zealander) would be authorised by the Attorney-General, approved by a judicial commissioner, and subject to the review and audit of the Inspector-General (a “triple-lock”). Tier two warrants would be authorised by the Attorney-General alone. The Minister of Foreign Affairs would be consulted when the proposed activity is likely to have implications for New Zealand’s foreign policy or international relations.

116. Ministerial Policy Statements would not affect the lawfulness or otherwise of an activity, but would be a mechanism to enable the responsible Minister to regulate the lawful activities of the agencies. For example, physical surveillance in a public place is a lawful activity, but the Minister should set out the general parameters within which the agencies undertake that activity. The lack of a Ministerial Policy Statement would not invalidate otherwise lawful actions.

117. Ministerial Policy Statements could provide guidance for the exercise of otherwise lawful activities, including (but not limited to):

- surveillance in a public place;

- obtaining and using publicly available information;

- requests to telecommunications providers for communications data;

- provision of cyber security and information assurance services by consent;

- use of cover as a means to support intelligence collection or obfuscate activities;

- information sharing with foreign partners;

- requests for information from other any agency of the Crown and the private sector; and

- lawful human intelligence collection.

118. Ministerial Policy Statements would be an important component of the proposed new regime and would enhance oversight and compliance. They would also ensure that the agencies have clear and objective guidance about how they are to carry out their lawful activities. For example, one short-coming of the current oversight regime is a lack of clarity about what "propriety" means in the Inspector-General of Intelligence and Security Act (the Inspector-General is able to inquire into the "propriety" of the agencies' activities). Ministerial Policy Statements developed with input from the Inspector-General would give the agencies and the Inspector-General greater clarity about the standard against which propriety is judged. Accordingly, we propose the Inspector-General be required to assess compliance with applicable Ministerial Policy Statements when conducting inquiries into the propriety of the agencies' conduct.

Impacts

119. *Public confidence* - The primary impact of the proposed warranting regime is to provide a clearer and simpler regime that provides significant protections for New Zealanders. The powers will be described in plain language and align more closely with those available in other legislation (e.g. Search and Surveillance Act 2012). The impact on public confidence will be examined in more depth in the impact summary toward the end of the RIS.

120. *Oversight* - The officials' approach maintains an appropriate distinction in the powers of the agencies, reflecting their different capabilities. The preferred option will also enable, but not require, the use of Ministerial Policy Statements to provide guidance about, and set parameters around, the lawful intelligence collection activities of the agencies. This will amount to a significant increase in oversight of the agencies activities by the executive.

121. *Warranting* - The new warranting regime may increase the number of warrants that will be required. This would increase the workload of the agencies in applying for warrants and the judicial commissioner. The increase in workload is to be absorbed by the agencies and the Minister, however the increase on judicial commissioners will be managed by the proposal to increase the number of judicial commissioners.

Authorisation in urgent situations

Status quo

122. There is limited provision for authorisations to be obtained urgently. The two Acts are inconsistent between the agencies and between different types of warranted activity.

123. The NZSIS Act provides for the substitution of the Commissioner when he or she is unavailable but not the responsible Minister. The GCSB Act on the other hand provides for the substitution of the responsible Minister but not the Commissioner.

124. The Director of the NZSIS can authorise interception, seizure, tracking or visual surveillance for up to 24 hours in urgent situations where the delay with obtaining a warrant is likely to result in a loss of intelligence. This temporary provision to the NZSIS Act was introduced as part of the Countering Terrorist Fighters Legislation Bill

in 2014 and is temporary. GCSB has no equivalent process. This power has only been used once since granted in 2014 and is subject to strict oversight.

Problem

125. Threats may materialise quickly and require urgent action. The process of applying for a warrant might prevent the agencies carrying out appropriate intelligence collection in an extraordinary situation. Violent extremism is on the rise internationally and Western countries are increasingly being targeted in coordinated and lone-wolf style attacks. New Zealand is not immune from such risks and any such threat would require an urgent response from the intelligence agencies.

126. A number of warranting procedures currently pose a risk relating to a single point of failure (e.g. unavailability of the Commissioner or Minister).

Reviewers' recommendations

127. In urgent situations, the agencies should be able to commence activity normally requiring a tier 1 authorisation with an interim authorisation approved by the Attorney-General.

128. The Chief Commissioner of Intelligence Warrants should be notified immediately and be able to direct the activity to cease at any time. The Attorney-General and Commissioner should be provided with a full application for a tier 1 authorisation within 48 hours.

129. Only in the most serious cases, and when other measures are insufficient, would a director be able to authorise activity without a warrant. Any director authorisation is subject to stringent review and oversight and a full warrant would be required within 24 hours.

Preferred option

130. Officials propose to implement the recommendations as suggested by the reviewers.

Impacts

131. *Operational effectiveness* - The main impact is on the effectiveness of the agencies in situations of urgency. It will allow the agencies to be able to respond quickly to threats or opportunities to gain valuable intelligence.

132. *Privacy and human rights* - There may be an impact on the privacy and human rights of any individual targeted under an urgent warrant. Officials are confident that the low frequency with which this power has been used in the past (there is, and will continue to be, a requirement to report annually on use of urgent warrants), and the strict oversight being applied in the future, will ensure that the use of urgent warrants is not abused and the negative impact on individuals will be appropriately managed.

Clarifying the role of the Inspector-General of Intelligence and Security

Status quo

133. The IGIS is the main external oversight body for the agencies and plays a critical independent role in ensuring that the agencies both comply with the law and act properly.

134. In 2013, the IGIS was substantially strengthened through enhanced powers and institutional arrangements. In recent years, the office of the IGIS has undertaken a number of significant reviews and inquiries, some of which have received considerable public and media attention. These inquiries are in addition to the IGIS's regular review of warrants, access authorisations, and internal compliance systems.

Problem

135. The review provides an opportunity to strengthen the role of the IGIS, consistent with other recommended changes to improve transparency, oversight, and accountability.

Reviewers' recommendations

136. The new legislation should include a clear statutory statement about the IGIS's role, to highlight his or her independence. Arrangements relating to the IGIS's appointment, funding, advisory panel, and work programme should also be amended to highlight and reinforce the independent nature of the role.

137. The new legislation should allow the IGIS to inquire into any matter relating to the agencies' compliance with the law, including human rights law, and into the propriety of particular activities of the agencies by own motion or at the request of the ISC.

138. The new legislation should allow the IGIS to report to the ISC on any findings following an inquiry undertaken at the request of the ISC.

139. The new legislation should clarify that, in respect of his or her review of warrants, the IGIS should be able to undertake a substantive review of a warrant (including the agencies' case for a warrant and implementation of the warrant).

Preferred option

140. Officials recommend that the government accept most of the recommendations and include any relevant provisions in the Bill.

141. In particular, the reviewers recommended that the Bill should clarify that the IGIS's review of warrants is not merely in relation to procedural matters but is a comprehensive look behind the face of the warrant. This includes reviewing the agencies' case for a warrant and how the warrant was implemented. Officials support this recommendation, noting that it would clarify the IGIS's role and emphasise that the current approach (which is to undertake an end-to-end review of all warrants) represents an appropriate level of scrutiny.

142. In addition, for the avoidance of doubt, officials propose clarifying that the IGIS's review of warrants does not extend to invalidating a warrant issued by the Attorney-General (and a judicial commissioner, where applicable). This would intrude upon the independence of those decision-making roles and could serve to undermine the comity between the various 'branches of oversight'. Equally, officials propose that the Bill make it clear that, should the IGIS's review of the warrant find that, for example, the relevant agency had not provided full information to the Attorney-General (and judicial commissioner, where applicable), that would not in any way invalidate the warrant, the intelligence collected pursuant to it, or action taken by the agencies or any other body in reliance upon that warrant or that intelligence.

143. Officials propose that the recommended expansion of the category of persons who can lay a complaint to the IGIS beyond New Zealand persons is rejected. This is not an appropriate use of the IGIS's limited time and resources. There is also a risk that it may create a de facto appeal right in immigration contexts. In addition, this option risks putting the IGIS in the position of having to decide whether to reject a complaint from a foreign government or organisation (which may have foreign policy implications for New Zealand). Officials consider that there are no other feasible options to meet the recommendation.

Impacts

144. *Public confidence* - The proposed changes will emphasise the independence of the IGIS, assuring the public that the IGIS is not an 'arm of government' but rather an independent review body.

145. *Oversight* - The proposed changes will also strengthen transparency and oversight of the agencies, which in turn will improve public confidence in the agencies. The changes will have a positive impact on privacy and the protection of human rights.

146. *Administrative* - There may be some minor administrative impacts on the IGIS on accounted of the expanded role.

Re-defining the Intelligence and Security Committee

Status quo

147. The ISC is the Parliamentary oversight committee for the agencies, and examines issues of efficacy and efficiency, budgetary matters and policy settings. It is established by the ISC Act as a statutory committee of Parliament.

148. ISC is one of the main ways in which democratic oversight of the agencies is achieved. The ISC has a fairly limited public profile, although its work has attracted more attention over the past few years.

Problem

149. There are no specific problems with the status quo but the review provides an opportunity to strengthen the ISC by enabling it to request that the IGIS - with his or her significant experience and skills - investigate compliance or the propriety of certain actions undertaken by the agencies. The changes will therefore also improve democratic and independent oversight, as well as transparency.

Reviewers' recommendations

150. The membership of ISC should be increased to allow for a minimum of five and maximum of seven members. The appropriate number should be determined by the Prime Minister after consultation with the Leader of the Opposition.

151. The ISC should be authorised to request (but not require) the IGIS to inquire into any matter relating to the agencies' compliance with the law, including human rights law, and into the propriety of particular activities of the agencies. This would include operationally sensitive matters.

152. The government should consider extending ISC's examination and review to the NAB.

153. The reviewers recommended that the ISC should elect its own chairperson, as opposed to the Prime Minister being chairperson (which is the case at present).

Preferred option

154. Officials recommend that the government accept all of the recommendations except the recommendation to extend the ISC's examination and review to the NAB and for the ISC to elect their own chairperson.

155. Increasing the maximum size of the ISC may increase its representativeness, by allowing for greater diversity in political perspectives (although this depends on how many members are appointed, as well who is appointed). It would allow the ISC the opportunity to more closely reflect the multi-party nature of New Zealand's Parliament.

156. Requiring members of the ISC to be nominated by the Prime Minister after consultation with the Leader of the Opposition would give the Prime Minister (who could choose not to sit on the ISC) oversight of its membership, while ensuring that the Leader of the Opposition retains his or her influence.

157. Allowing the ISC to ask the IGIS to inquire into the agencies' compliance or the propriety of the agencies' activities will strengthen the ISC's effectiveness as a mechanism for democratic oversight, while simultaneously enhancing the IGIS's role as a provider of independent oversight.

158. Officials do not consider it necessary to extend the ISC's examination and review functions to the NAB, as recommended by the reviewers. The time and resources of the ISC are best spent focusing on the activities of the GCSB and NZSIS, as these agencies have intrusive capabilities that require democratic oversight. Moreover, the NAB is subject to the scrutiny of the Government Administrative Committee as part of DPMC's annual reporting processes. Extending another committees' examination to NAB would create unnecessary overlap and reporting requirements.

159. Officials do not consider it appropriate for the ISC to elect its own chairperson and propose to depart from the reviewers' recommendation. The Prime Minister has traditionally held a role leading the national security system. Officials therefore consider it appropriate for the Prime Minister to continue to chair the ISC.

Impacts

160. *Oversight* - Improving coordination between branches of oversight and improving Parliamentary oversight will improve accountability and transparency. This will have a positive impact on public trust and confidence in the agencies' activities.

Providing a role for judicial commissioners where an agency is seeking a warrant to target New Zealanders

Status quo

161. The Commissioner of Security Warrants jointly issues warrants for the agencies where a New Zealander may be a target for the warrant. The Commissioner of Security Warrants is appointed by the Governor-General on the recommendation of the Prime Minister following consultation with the Leader of the Opposition for a term of three years. The Commissioner is required to have previously held office as a Judge of the High Court.

Problem

162. There are two problems. The first is workload and availability. In the year to June 2015, the Commissioner of Security Warrants dealt with 29 domestic intelligence warrants from the NZSIS. While this number is not unmanageable at present, the new warranting framework is likely to see an increase in the number of warrants. A precise estimate cannot be provided as it will depend on a range of variables including the security environment. There are times when a single commissioner will be unavailable (the Commissioner might be on holiday, and the workload might increase to an extent that a single Commissioner might be stretched too thinly to carry out the functions with the appropriate rigour.

163. The second is specific to the GCSB. It must have the Commissioner's approval, even in urgent situations. If the Commissioner of Security Warrants is unavailable it may not be possible to obtain a warrant in a timely or effective manner.

Reviewers' recommendations

164. That a panel of up to three judicial commissioners should be appointed who could be sitting or retired judges, headed by a Chief Commissioner of Intelligence Warrants

Preferred option

165. Officials support the idea of increasing the capability of judicial commissioners but propose the initial appointment of at least two judicial commissioners, with further appointments to be made by the Attorney-General as the need arises.

166. In order to maintain the independence of the sitting judiciary, the preferred option is to appoint only retired judges who have held a warrant as a High Court judge.

Impacts

167. *Oversight* - The primary impact is that it will increase the level of oversight for warrants to target New Zealanders, and ensure that a judicial commissioner is always available (reducing the need for urgent warrants). Judicial commissioners, as retired judges, would bring their significant judicial experience to the warranting process without compromising the independence of the sitting judiciary.

Providing the agencies with cover for their employees

Status quo

168. The agencies rely on secrecy to protect their employees, capabilities, and lawful activities. While some specific provisions currently exist to permit assumed identity information to be established and used by the NZSIS, this is limited to the creation and use of births, deaths, marriages, and relationships registration information, drivers licences and electronic identity credentials.

Problem

169. The existing legislative provisions regarding assumed identity information do not cover all relevant identity information and do not apply to the GCSB.

170. There is no legal protection for employees who need to keep their link with the agencies secret and may commit an offence or incur civil liability in order to do so

(such as making misleading statements when misrepresenting the identity of their employer).

Reviewers' recommendations

171. The proposed new Act should explicitly provide for assumed identity information to be obtained, created and used by both the NZSIS and GCSB for the purpose of maintaining the secret nature of the agencies' authorised activities, and to keep the identity of their employees secret.

172. There should be corresponding immunities for employees (and persons assisting them) from civil and criminal liability for acts to create or maintain cover.

Preferred option

173. Officials agree that both the NZSIS and GCSB should be able to establish, maintain and use assumed identity information for the purposes of maintaining secrecy and enabling potential future operations and capabilities. This will require corresponding civil and criminal immunity.

174. Officials propose that the government should permit employees of the agencies to make misleading or false statements under their real identity in order to keep the fact of their employment with the agencies secret. This will necessitate a corresponding immunity for such misrepresentations.

Impacts

175. *Operational effectiveness* - The primary impact will be the creation of a more comprehensive cover framework that removes existing legislative gaps and protects both agencies' employees (and those assisting them), which will enable the agencies to carry out their duties and functions more effectively.

Providing the usual immunities to the agencies and their staff

Status quo

176. The agencies need immunities from civil and criminal liability when performing functions that involve carrying out an activity that would be unlawful if it was not enabled under their legislation. The agencies currently have some immunities but there are gaps and inconsistencies.

Problem

177. The existing immunities available for the NZSIS and GCSB are different in scope. NZSIS employees do not currently have broad civil immunity, as enjoyed by the rest of the public service, and do not have a criminal liability for acts carried out to obtain a warrant.

178. The lack of clarity regarding immunity from criminal liability when employees are acting under the agencies' specific assistance function has been one of several factors hindering the agencies' co-operation with other entities, notably Police.

Reviewers' recommendation

179. The reviewers recommend that the immunities should be applied consistently to both agencies.

180. The reviewers recommend that employees should be immune from criminal liability for acts carried out to obtain a tier one or two warrant and for minor offences or infringements (the reviewers suggested certain traffic offences). They also recommend that employees and persons assisting the agencies should be immune from criminal liability for acts to give effect to a warrant.

181. The reviewers recommend that when the agencies are assisting other government entities, the only criminal immunity that should apply is that available to the entity being assisted.

Preferred option

182. Officials agree with the reviewers recommendations, but propose a clarification and an appropriate extension.

183. Officials propose that the government should provide employees of the agencies with an exception (rather than immunity) to specific offences that may be committed in the course of performing an investigation, such as breaches of the Road User Rules and offences related to accepting unsolicited information. This is consistent with the exception from the Road User Rules 2004 available to Police.

184. Officials propose that there should be an additional immunity from criminal liability for acts reasonably believed necessary to give effect to the agencies' assistance function for the purpose of assisting Police or the New Zealand Defence Force. We note that this immunity extends beyond what the reviewers recommend but clarify that the agencies should still be limited to acting within the scope of the powers of Police or NZDF. The agencies should only be immune from acts carried out within that scope.

185. No immunity or exception (including the cover-related immunities discussed in the preceding section) will prevent the Crown being held directly liable for breaches of the New Zealand Bill of Rights Act 1990 by public officials.

Impacts

186. *Operational effectiveness* - The preferred approach will enable employees and those assisting the agencies to perform the agencies' functions effectively and without fear of prosecution or civil liability. The existing (and continuing) overarching requirement that the agencies comply with human rights standards recognised in New Zealand law will ensure that the agencies are not immune or excepted from breaches of human rights law.

187. *Cooperation* - The proposed new immunities will clarify an area of uncertainty that currently impedes some areas of cooperation under the agencies' assistance function.

Allowing for access to datasets

Status quo

188. Access to information held by other government departments is governed by informal

arrangements and generally occurs on a case-by-case basis under the agencies' existing powers and section 57 of the Privacy Act 1993 (which provides an exemption from most of the information privacy principles).

Problem

189. The agencies have had direct access to certain information but for the most part access takes place on a case-by-case basis. Requiring the agencies to request information on a case-by-case basis is not practical, given how often the agencies need to access this information, and does not assist the organisations to operate in a modern and efficient fashion. This is a resource intensive requirement for both the agencies and the organisations providing the requested information.

190. The current approach is also not particularly transparent since the agencies' current access to this information is generally not expressly provided for in legislation.

Reviewers' recommendations

191. The reviewers recommend that the legislation allow the agencies to access and retain certain datasets, including customs and immigration datasets. The reviewers propose that this access and retention should be subject to a joint protocol (agreed between the responsible Ministers) governing such access and retention.

Preferred option

192. Officials recommend that the government accept the reviewers' recommendation to give the agencies access to the datasets set out in the table below. As discussed in the table below, there are a number of reasons why access to these datasets is needed. In addition, giving the agencies direct access reduces the resource burden on both the agencies and the organisation holding the information in question.

193. The reviewers did not expressly address use or disclosure of this information in the context of their specific recommendations; officials consider that use and disclosure should be considered alongside access and retention.

Dataset	Examples of why access may be needed
Information about border-crossing craft and persons held by the New Zealand Customs Service and Advanced Passenger Processing and Passenger Name record data collected by Immigration New Zealand (MBIE)	To cross-check agencies' information against Customs information about arrivals and departures at the border, to detect the movements of foreign intelligence officers or other persons of interest (such as suspected terrorists).
Immigration New Zealand databases	To allow the GCSB or NZSIS to ascertain if a person is a New Zealander, to determine whether to apply for a tier one or tier two warrant.
Births, deaths, marriages and relationships, and citizenship registers	To allow the agencies to cross-check information to certify identity or associations between persons of interest, or to ascertain nationality.

194. Further discussions with New Zealand Police have led officials to believe that there is not a strong case for access to New Zealand Police's National Intelligence Application (NIA) at this time. Rather, issues of physical security are best handled through the agencies continuing to work closely with the Police as issues arise. For this reason, officials do not propose to provide the agencies with access to NIA.

195. The reviewers did not expressly address allowing the agencies to access Customs information about border-crossing goods. However, Customs has clarified that it would be difficult for the agencies to access information about border-crossing craft and persons without simultaneously accessing information about border-crossing goods. Having regard to the scope of the National Intelligence Priorities, officials consider that there is a compelling case for allowing the agencies to access this information (as well as information about border-crossing craft and persons).

Dataset	Examples of why access may be needed
Information held in New Zealand Police's National Intelligence Application	To allow the agencies to determine the physical safety risk to its field officers posed by certain individuals (who might be under investigation or might be on the periphery of an investigation).

196. Officials consider 'access' should mean a type of access that is as direct as possible and that meets the agencies' operational needs while minimising resourcing demands on the disclosing agency. There may be different ways to facilitate such access, which may vary depending on the dataset in question. For example, one option may be for the agencies to regularly receive a copy of a dataset, which is then isolated from the original and securely stored by the agencies.

197. The agencies and each organisation holding the information above will therefore work closely together to ascertain how best to provide for such access. In the meantime, officials propose to work with Parliamentary Counsel Office to ensure that the drafting of the Bill enables the full range of possibilities.

198. Officials agree with the reviewers' recommendation that the agencies should only be able to access and retain (as well as use and disclose) information stored on these systems in accordance with joint protocols agreed between responsible Ministers. The reviewers recommended that the joint protocols be developed in consultation with the Privacy Commissioner, which officials propose to accept. Officials also consider that the IGIS should be consulted during a joint protocol's development, and that both the Privacy Commissioner and the IGIS should be consulted when the responsible Ministers review joint protocols every three years.

199. The reviewers recommended that the IGIS should monitor the agencies' compliance with each protocol, which officials also propose to accept.

200. Supplementary to the reviewers' recommendations, officials also propose that the Bill require the parties to a joint protocol to each publish a summary of the joint protocol on their websites once it is agreed and following the completion of each three yearly review (ensuring that publication occurs in a manner compliant with requirements of security). Officials note that the Official Information Act 1982 would apply to joint protocols in the usual manner.

Impacts

201. Privacy - In addition to reducing the burden on the agencies and disclosing organisations, direct access minimises adverse privacy impacts on individuals in appropriate cases. It ensures other organisations are not unnecessarily alerted to the interest of an intelligence agency in a particular individual, which - given the nature of intelligence investigations - could lead to that organisation taking action against that individual.

202. Transparency - Officials consider that expressly allowing the agencies direct access to the specified datasets in primary legislation builds transparency, by making their powers in this area clear.

203. Ministerial oversight - Requiring joint protocols, executed by Ministers, is appropriate as it will ensure the agencies' ability to access, use, disclose and retain information from these datasets is limited, justified, and transparent.

Case by case access to restricted information

Status quo

204. Some information collected by other organisations cannot be shared despite the agencies' general powers and the section 57 exemption. This occurs where legislation that gives public sector agencies the authority to collect personal information restricts the disclosure of that information to specific purposes or entities (for example, personal tax information). Where this is the case, the organisation holding the information cannot share it unless expressly authorised to do so by legislation or directed under warrant to do so.

Problem

205. The agencies need occasional access to this information, but cannot access it due to a statutory prohibition. Due to operational sensitivities, it is not possible to provide specific data on how often the agencies require access to this information.

Reviewers' recommendations

206. The legislation should provide for access to the following information about individuals on a case-by-case basis, pursuant to a tier one or two warrant:

- Tax information held by the Inland Revenue Department;
- Driver licence photographs held by the New Zealand Transport Agency; and
- National Student Identification Numbers held by the Ministry of Education.

Preferred option

207. Officials propose that the government accept the reviewers' recommendation to give agencies the ability to access the information above pursuant to a warrant. This type of information is needed by the agencies on a fairly infrequent basis and only in specific investigations. Therefore, direct access to relevant datasets is unnecessary and unlikely to be a proportionate response. Officials agree with the reviewers that allowing the agencies to obtain this information on a case-by-case basis is more appropriate in these situations. Requiring a warrant provides a high level of protection

for the individual concerned, and ensures that the information is not inappropriately accessed. In relation to tax information this may require an amendment to the Tax Administration Act 1994 to override tax secrecy and require the Commissioner of Inland Revenue to comply with the warrant.

208. Officials also propose that access to National Student Number (NSN) linked information should only be available for adults and young people in relation to tertiary education, not for children in the early education, primary or secondary schooling systems. Unless it could be shown that schools may be delivering education that creates a security risk, the benefits of access to this information would be unlikely to outweigh its intrusive nature (particularly given the tight statutory controls around the use of NSNs).

Impacts

209. *Intelligence* - The proposed change would give agencies access to information that they legitimately need to see, with potentially significant consequences for the quality of intelligence gathered.

210. *Privacy* - There would be a consequential impact on the privacy of the person to whom the information applies but, given the requirement of a warrant, this impact can be considered justifiable.

Creating a framework for arrangements with foreign partners

Status quo

211. The agencies have both formal and 'ad hoc' relationships with their counterparts in different countries. Through these relationships, New Zealand draws upon a larger pool of information, skills, and technology than would otherwise be available to it.

212. New Zealand's most important partnership is that with the United States, United Kingdom, Australia and Canada (the Five Eyes). However, New Zealand also has bilateral relationships with a number of other countries.

Problem

213. The current legislation does not explicitly acknowledge or provide for New Zealand's arrangements with foreign partners.

214. There is room to improve the oversight and transparency of New Zealand's intelligence relationships to improve public confidence in the intelligence agencies.

Reviewers' recommendations

215. The legislation should explicitly enable the agencies to co-operate and share intelligence, in accordance with the Act and with New Zealand's human rights legislation, with foreign jurisdictions and international organisations.

216. New bilateral and multilateral relationships should be referred to the ISC for noting.

217. The government should consider including restrictions on the circumstances in which information collected by the agencies about New Zealanders can be shared with foreign jurisdictions and international organisations.

218. The Act should set out standard terms for 'ad hoc' intelligence sharing with the draft terms being forwarded to the IGIS for comment and the final version provided to the ISC for noting.

Preferred option

219. Officials recommend that the government agree with the thrust of the recommendations and include relevant provisions in the Bill.

Impacts

220. *Transparency* - New Zealand's existing ability to enter into intelligence relationships with other jurisdictions will be placed on a statutory footing. This will enhance transparency and oversight of New Zealand's cooperation with other countries. This will help to improve public confidence in the intelligence agencies.

221. *Oversight* - Requiring new arrangements to be forwarded to ISC will improve transparency, thereby increasing accountability and democratic oversight (which in turn builds public confidence in the agencies).

222. *Human rights* – The agencies will develop standard terms for intelligence sharing on an 'ad hoc' basis. Those standard terms will recognise New Zealand's human rights obligations, as set out in domestic law. Officials agree with the reviewers that there will be some circumstances in which intelligence – regardless of the nationality of the person to whom it relates – should not be shared. A strong example is where there are legitimate concerns that information may be used to punish someone in a manner inconsistent with human rights standards.

Incidentally obtained intelligence

Status quo

223. In the course of intelligence collection, the agencies sometimes incidentally obtain other intelligence that is not relevant to their objectives and/or functions. In certain circumstances that information should be shared with other organisations. For example, if through the course of their intelligence collecting activities the agencies learnt of an individual planning an armed robbery, it would be in the public interest to share that intelligence with the New Zealand Police in as timely a fashion as possible, even where restrictions on the retention or sharing of that information would normally apply.

224. Section 25 of the GCSB Act 2003 regulates the retention and communication of incidentally obtained intelligence. There is no equivalent section in the NZSIS Act.

Problem

225. The agencies' ability to retain and communicate incidentally obtained intelligence should be clearly spelt out in legislation, to provide legal certainty to the agencies and to ensure their powers are transparent.

Reviewers' recommendations

226. The reviewers recommend retaining section 25 of the GCSB Act 2003, with any necessary modifications.

Preferred option

227. Officials recommend carrying over and extending section 25 of the GCSB Act 2003 so that it applies to both agencies. That is, the relevant Director should only be able to retain incidentally obtained intelligence where that intelligence is relevant to:

- preventing or detecting a serious crime
- preventing or avoiding the loss of human life on the high seas
- preventing or responding to threats to human life in New Zealand or any other country; or
- identifying, preventing or responding to threats or potential threats to the security or defence of New Zealand or any other country.

228. In accordance with section 25 of the GCSB Act 2003, officials also recommend that the relevant Director should only be able to communicate that intelligence to:

- any employee of the New Zealand Police;
- any member of the New Zealand Defence Force;
- the Director of the GCSB or the NZSIS, whichever is relevant; or
- any public authority (whether in New Zealand or overseas) that the Director thinks fit to receive the information.

Impacts

229. *Transparency* - The preferred option makes the agencies' powers in this area clear and accessible, further building transparency.

Centralising intelligence assessments

Status quo

230. Assessment is an important part of the intelligence cycle. The reviewers identified NAB, a business unit of the Department of the Prime Minister and Cabinet, as New Zealand's dedicated intelligence assessment centre. Cabinet has established NAB as the lead assessment body but NAB is not recognised in legislation. NAB produces assessments based on both open source and secret intelligence for customers such as the Ministry of Foreign Affairs and Trade. The Combined Threat Assessment Group (CTAG) also has an independent assessment mandate and operates from within the NZSIS. Other parts of the intelligence community that produce assessments include Customs, Police and NZDF.

Problem

231. There is not sufficiently clear independence of the assessment function from the collection function. The importance of assessment in the intelligence cycle is not recognised in legislation.

232. The reviewers have identified some overlap between CTAG and NAB. In particular, the reviewers considered CTAG's independence may be impacted by being located within the NZSIS.

Reviewers' recommendations

233. The government should consider including the role and functions of NAB in the single Act.

234. The government should review the current placement of CTAG within the NZSIS and consider whether it might more appropriately be situated within the NAB.

Preferred option

235. Officials support the inclusion of the role and functions of NAB in the proposed new Act. Officials propose to confer the functions of NAB on the chief executive of DPMC in the proposed new Act, with the chief executive being able to delegate these functions under section 41 of the State Sector Act 1988 as he or she sees fit.

236. Officials agree that the current placement of CTAG should be reviewed, and will do so through the NZIC four-year plan.

Impacts

237. Oversight - The role of independent assessment in the intelligence cycle will be emphasised and strengthened. The separation of collection and assessment is an important check on the agencies and improves the integrity of the assessments the intelligence community generates.

Disruption of travel

Status quo

238. Amendments to the Passports Act 1992 were made by the Countering Terrorist Fighters Legislation Bill. Those amendments allow the Minister of Internal Affairs to cancel or refuse to issue a travel document. The grounds for cancelling or refusing to issue documents refer to the definition of 'terrorist act' in the Terrorism Suppression Act. There is a maximum three-year cancellation period (the previous maximum period was 12 months), and travel documents can be suspended for ten working days to prevent a person from travelling while a cancellation is processed.

Problem

239. These provisions are required to respond to the threat of individuals attempting to travel to the Middle East to fight in terrorist groups. Specific information on the number of people attempting to travel from New Zealand cannot be provided, as it is operationally sensitive.

240. These provisions were enacted in 2014 in response to the United Nations Security Council Resolution 2178. Security Council resolutions are legally binding upon member States.

241. These provisions in the Passports Act are subject to a sunset clause (expiring at the end of March 2017).

Reviewers' recommendations

242. The maximum three-year cancellation period for travel documents and the 10 working day suspension period to allow for processing of a cancellation should continue to apply.

243. Any decision by the Minister of Internal Affairs to cancel or refuse to issue a travel document on security grounds should be referred to the Chief Commissioner of Intelligence Warrants for review by a judicial commissioner on grounds of judicial review, with the judicial commissioner having the ability to overturn the decision if one of the grounds for judicial review is made out.

244. The ability to suspend a travel document for a maximum of 10 working days should be retained, to prevent a person from leaving the country while the process for cancelling their travel document is progressed.

Preferred option

245. Officials accept the reviewers' recommendation to retain the maximum three-year cancellation period and the 10 working day suspension period to allow for processing of a cancellation. The recommendation for a judicial commissioner to review the Minister of Internal Affairs' decisions to cancel or refuse a travel document is accepted except with respect to a judicial commissioner being able to overturn the Minister's decision. Officials consider that if a decision is to be reviewed on judicial review grounds, the process should follow judicial review in terms of outcome also, with the judicial commissioner being able to refer a decision back to the Minister for reconsideration rather than overturning it.

Impacts

246. *Human rights* - The cancellation of, or refusal to issue, a travel document impinges on a person's right to leave New Zealand and can have a significant impact on the individual concerned. To improve public confidence that this capability is not being abused, the reviewers have recommended that decisions made by the Minister would be subject to judicial review. Officials agree that this is an appropriate safeguard in light of the potential impact on an affected individual's right to freedom of movement.

Visual surveillance

Status quo

247. Visual surveillance powers for the NZSIS are provided through a temporary amendment to the NZSIS Act via the Countering Terrorist Fighters Legislation Bill which expires in March 2017 unless renewed. The temporary provisions allow the NZSIS to obtain visual surveillance warrants and undertaken warrantless surveillance (authorised by the Director of Security) for a period of up to 24 hours in situations of emergency or urgency. These powers only apply for the detection, investigation or prevention of an actual, potential or suspected terrorist act. Since its introduction, the power has only been used twice.

Problem

248. Prior to December 2014, the NZSIS lacked clear statutory authority to carry out visual surveillance on private property where an individual had an expectation of privacy.

249. Visual surveillance currently operates under a separate regime to other forms of surveillance that are covered in the NZSIS Act. There is no compelling reason for this distinction.

Reviewers' recommendations

250. The legislation should continue to enable visual surveillance by the agencies but it should not be restricted to counter terrorism. It should be treated the same way as other forms of surveillance.

Preferred option

251. Officials support the inclusion of visual surveillance in the agencies powers under the new authorisation regime.

Impacts

252. *Privacy* - The primary impact is on individuals' privacy. The power will be subject to the warranting and oversight regimes in the same way as the other powers of the agencies.

Offences and protected disclosures

Status quo

253. Offences for disclosing national security information are currently located across a number of statutes with varying levels of penalty applying. These Acts include the NZSIS Act, the GCSB Act, the Crimes Act and the Summary Offences Act. There are offences under the IGIS Act and the ISC Act that protect the processes of the oversight mechanisms and information that is disclosed to them in the course of those processes.

254. There is also an offence in the NZSIS Act to publish or broadcast the identity of a NZSIS employee other than the Director of Security (section 13A), and an offence of personation as an employee of the NZSIS (section 13).

255. There is also an offence under section 23(8) of the IGIS Act that relates to the exercise of powers under the Act by the Inspector-General which covers actions such as obstruction, non-compliance with a lawful requirement, and making a false statement.

256. The Protected Disclosures Act 2000 provides a procedural pathway for "whistle blowing". It provides protection in respect of disclosures that follow the prescribed pathway, including from criminal liability for disclosures that would otherwise be in breach of the various offences protecting national security information. The Act contains provisions applying to the intelligence and security agencies, which include requirements in relation to internal procedures of the agencies and for IGIS to be the only "appropriate authority" to whom disclosures may be made by employees of the agencies. The Act also contains a provision that applies to employees of certain other agencies who are likely to encounter issues relating to international relations and intelligence and security. That provision is inconsistent in its terms with the provision applying to the agencies and raises questions about the disclosure pathway for such employees, and more broadly for employees in other agencies that are not listed in it in respect of disclosures involving national security issues.

Problem

257. Unauthorised use or disclosure of information with national security implications could have serious ramifications for New Zealand's national security and international relations. This might include undermining New Zealand's reputation as an intelligence partner with the capabilities to protect classified information.

258. The current offences applying to the intelligence and security sector are inconsistent in terms of their formulation and penalties. There are gaps in the current law and some of the penalties applying to the current offences are out of date and arguably no longer provide a realistic deterrent. Also, given the intended aligning of the NZSIS and GCSB, having the offences of publication of an identity and personation of an employee applying to one agency but not the other is inconsistent with the intent of the review and officials' objectives for the response to the review.

259. Protected disclosures and offences to protect information with national security implications should be seen as closely related in the sense that the protected disclosure pathway is provided to enable a person with good faith concerns to seek to have those investigated and addressed if necessary. Where a person does not take the appropriate pathway, the individual should be held accountable for the harmful disclosure.

Reviewers' recommendations

260. The reviewers propose carrying over and amalgamating offences in the existing four Acts in the proposed single new Act.

Preferred option

261. Officials have considered the full suite of relevant offences beyond just those in the four Acts with a view to ensuring that there is appropriate protection of information with national security implications, and in relation to the agencies and their oversight mechanisms. The offences in the current Acts that apply to employees of the agencies will be carried over, rationalised and applied to both agencies. The offences from the IGIS Act and the ISC Act will also be carried over.

262. A new offence in the Crimes Act is proposed. The new offence will be based on section 78A Crimes Act but will be aimed specifically at persons owing a specific obligation of confidence in relation to classified information. It will also create a warrantless search power, similar to that which applies to espionage under section 78 of the Crimes Act.

263. The penalties applying to all the offences have been reviewed to ensure relativity and consistency with other relevant provisions on the statute book, as well as providing a realistic deterrent.

264. The Protected Disclosures Act should be amended to ensure that for individuals working with classified information or who have access to information relating to the activities of the agencies, there is a clear and easily accessible pathway for protected disclosures.

Impacts

265. *Legislative clarity* - As the proposed new offences regime will largely rationalise offences already on the statute book, the impact will be limited. Having the offences in a single Act will provide more clarity to employees of the intelligence and security agencies, and to the broader public, about what is and is not permitted. This, coupled with an updated penalties regime, will provide a more effective deterrent to committing an offence related to the intelligence and security sector.

266. *Protected disclosures* - This should be understood along with the proposed improvements to the protected disclosures pathway. Any employee of another agency who has good faith concerns has a clear and accessible pathway to seek to have those concerns investigated. If that person chooses to bring the issue to light in another way, there is a more serious criminal sanction than is currently available.

267. *Cover* - The new regime will allow for the protection of identities of GCSB staff. This, along with a similar broadening of the personation offence, does impact freedom of expression. Given the sensitive nature of the work the agencies carry out, and the very real dangers their covert employees face, this extension is justified. It is also appropriate for the new regime to go beyond staff currently involved in covert activities, for a variety of reasons, including the risks for them in being seen to associate with someone known to be an employee of the agencies.

Proposed changes to the Immigration Act

Advance Passenger Processing for outbound travellers

Status quo

268. Currently the Immigration Act 2009 requires carriers to provide Immigration New Zealand (in the Ministry of Business, Innovation and Employment) with information for the purpose of Advance Passenger Processing (APP) for inbound travellers (that is, every person who intends to board the craft for the purposes of travelling to New Zealand) but not for outbound travellers. The Immigration (Carriers' Information) Regulations require elements such as the person's name, date of birth, nationality, gender, and the number of the passport or certificate of identity and its expiry date and issuer. Outbound APP is also provided by airlines, on an entirely voluntary basis.

Problem

269. Currently, border agencies only know that a person intends to depart New Zealand when he or she arrives at the outward immigration processing point (the departure passport control). Border agencies may have insufficient time to identify high risk travellers intending to depart New Zealand, assess their intentions, and where indicated, plan an intervention. High risk individuals may include:

- foreign fighters and other people who pose a security threat;
- criminals sought for arrest, or prisoners who have escaped or are on parole;
- persons using lost, stolen, invalidated or fraudulent travel documents;
- travellers who pose a risk to the safety of passengers, crew, or craft; or

- potential perpetrators or victims of people trafficking.

270. Delayed notification that a high risk person is intending to depart means carriers may be forced into a last minute search and off-load of the individual's hold-stored baggage. This is costly and inconvenient for the carrier and can cause delays for other travellers.

271. Further, APP transactions drive SmartGate processing on departure. Currently, airlines provide APP information on outbound travellers voluntarily so that passengers can use SmartGate – but it is important to remove legislative doubt to assure passengers' ability into the future be processed via Customs through automated means, that is, via SmartGate. The voluntary nature of the provision means that the government cannot, for example, infringe carriers who do not provide APP data.

272. withheld consistent with s6(a) of the Official Information Act 1982

withheld consistent with s6(b)(i) of the Official Information Act 1982

Reviewers' recommendation

273. The reviewers did not consider APP for outbound travellers.

274. Officials have addressed this issue in consultation with relevant agencies, and the preferred option below has the support of Border Sector Governance Group senior officials (which includes the New Zealand Customs Service, the Department of Internal Affairs, the Ministries of Business, Innovation and Employment, Foreign Affairs and Trade, Primary Industries and Transport) as well as the Police, Avsec and the NZSIS.

275. Although cruise ships are within the scope of these legislative changes (they are included in the definition of a 'carrier'), regulations will need to be developed to give effect to the law. Unlike aviation, the systems are not currently in place. However, officials are planning to undertake the necessary policy and operational work to manage the risks and a detailed regulatory impact statement will accompany regulatory proposals, which will be on a slower than regulation changes for air carriers.

Preferred option

276. Amendments should be made to the Immigration Act 2009 in relation to APP for outbound travellers that:

- allow for both the collection of information and for boarding directives;
- make it mandatory and apply an infringement and offence regime (in the same way as it does for inbound APP information) so that the provision of information is assured and boarding directives are followed; and
- allow Immigration New Zealand to share outbound APP information with Police, Customs, the Department of Corrections and the Aviation Security Service or allow

them direct access to the information (the agencies will have access to outbound APP through the information-sharing provisions described above).

Impacts

277. *Privacy* – Carriers are already required to provide APP information on inbound travellers and the information required is the same as that provided in a traveller's passport, which the traveller has to present at the departure passport control. The presence of a carrier infringement regime means the information collected is more likely to be accurate as carriers have incentives to comply.

278. *Public trust and confidence in the agencies* – Public trust and confidence in the NZSIS, border agencies and the Police are likely to be enhanced if the public believes that these agencies are better able to identify high risk travellers before those travellers board a carrier leaving New Zealand (and so better ensure the safety of other travellers for example).

279. *National security* - Outbound APP would provide border and security agencies and the Police with greater warning of a person's intention to travel than those agencies have at present. This could be several days prior, if the traveller is checking in online, or several hours if departing from a domestic port or directly from an international port. The extra warning time would allow agencies to better identify high risk travellers, assess their intentions and, if indicated, plan an intervention.

280. *Compliance costs:* Requiring carriers to provide outbound APP would not pose any further compliance burden on airlines as they are already doing it on a voluntary basis. They are already required to provide APP for inbound flights to New Zealand (under New Zealand law), and outbound flights from New Zealand to Australia (under Australian law). Costs incurred under the infringement regime would only apply if the carrier failed to provide the required information.

Clear legislative authority for Immigration New Zealand to use Passenger Name Record information for outbound travellers

Status quo

281. Currently, Immigration New Zealand has no clear legislative authority to use Passenger Name Record (PNR) information for outbound travellers. Travellers booking inbound travel often book their outbound travel at the same time so Immigration New Zealand is in practice already provided with outbound PNR information.

282. Customs has authority under its legislation to require airlines to submit PNR for passengers departing New Zealand and is working with airlines to obtain departure PNR for profiling persons departing New Zealand, and specifically to identify potential foreign fighters who are not on existing watch lists. However, there is no provision under either Immigration or Customs legislation for a carrier infringement offence regime regarding outbound travellers as there is for inbound travellers under the Immigration Act. Under the Border Sector Policy Statement on Airline PNR data, Immigration New Zealand's carrier infringement regime is the agreed means to manage non-compliance with PNR data provision.

Problem

283. Not having clear legislative authority for Immigration New Zealand to use outbound PNR information hampers its ability to effectively screen travellers, as important information to identify risk may be in the traveller's outbound travel records. It also hampers Immigration New Zealand's ability to support government's collective efforts to profile and interdict foreign terrorist fighters.

Reviewers' recommendation

284. The reviewers did not consider this matter.

Preferred option

285. Amendments should be made to the Immigration Act 2009 in relation to PNR information for outbound travellers to:

- provide clear legislative authority for Immigration New Zealand to use PNR information for outbound travellers, as is the case for inbound travellers, and
- make the provision of PNR information on outbound travellers mandatory and include an infringement office, as is the case for inbound travellers.

Impacts

286. *Privacy* – PNR is a record in an airline's computer reservation system that contains a range of information including the itinerary of a passenger, ticket information, contact details and means of payment. Customs has legislative authority to use this information on outbound passengers for profiling purposes. This proposal would remove legal doubt about Immigration New Zealand's ability to use this information concerning outbound passengers.

287. *National security* – PNR is a rich source of data used in many countries to detect possible criminal or terrorist threats. The proposal to clarify Immigration New Zealand's ability to use departure PNR and to apply the carrier infringement regime to non-provision of departure PNR will support government's collective efforts to profile and interdict foreign terrorist fighters.

Compliance costs

288. Carriers are already required to provide PNR information to Immigration New Zealand on inbound travellers and to Customs on outbound travellers. Costs incurred under the infringement regime would only apply if the carrier failed to provide the required information.

Express powers for Immigration New Zealand to direct a carrier not to carry a person out of New Zealand on stolen or otherwise invalid travel documents

Status quo

289. There is a general international expectation, found in Annex nine of the International Civil Aviation Organisation Convention on Civil Aviation, that member states will remove fraudulent travel documents from circulation rather than allow people to travel on them. Customs has an existing power to seize lost, stolen, invalidated or

fraudulent travel documents (using information supplied by the Department of Internal Affairs to intercept New Zealand passports when indicated). Immigration New Zealand, however, has no express power to direct a carrier not to carry a person out of New Zealand on lost, stolen, invalidated or fraudulent documents to effectively manage identity risks on departure.

Problem

290. Under existing arrangements, Immigration New Zealand's checks could identify that a person is using a lost, stolen, invalidated or fraudulent travel document but, by the time either Customs or the Police has been advised and is able to intervene, the person could have already left New Zealand.

Reviewers' recommendation

291. The reviewers did not consider this matter.

Preferred option

292. Amendments should be made to the Immigration Act 2009 to grant Immigration New Zealand an express power to direct a carrier not to carry a person out of New Zealand on a lost, stolen, invalidated or fraudulent travel document.

Impacts

293. *National security* – knowing a person's identity is fundamental to assessing a person's national security risk. Directing a carrier not to carry a person out of New Zealand on fraudulent travel documents supports international as well as national security.

Summary of Impacts

294. This section sets out the overarching impacts of the package of proposed changes.

Impact on the privacy of New Zealanders

295. Privacy is an important end in and of itself. A person's right to vote and freedom of expression is predicated on the opportunity that privacy provides a person to think for themselves and to act (within the bounds of the law) without the fear of scrutiny from others. Parliament's recognition of the importance of this value can be seen in the enactment of the Privacy Act 1993, which provides a regime that both protects personal information and allows for it to be shared appropriately.

296. To some extent, officials' proposals in response to the review represent an extension of the ability of the agencies to investigate New Zealanders. The proposals also broaden and expressly confirm the ability of government agencies to share certain sets of personal information with the agencies. Importantly, the proposals make it easier for the NZSIS and GCSB to work collaboratively. This represents a broadening of the type of security issues that the GCSB can investigate and a growth of the capabilities that the NZSIS can bring to bear during a domestic investigation.

297. However, under the proposed new arrangements, there will be increased oversight, accountability and transparency around the exercise of these powers. Officials propose to implement the reviewers' recommendation that 'there should be some level of authorisation for all of the agencies intelligence and security activities that involve gathering information about individuals or organisations, proportionate to the level of intrusion involved'.

298. Officials are confident that the safeguards are stringent enough to prevent unnecessary intrusion into the privacy of New Zealanders. For the agencies to investigate a New Zealander, a warrant application will need to be judged to meet five specific legal criteria by the Attorney General and a retired High Court judge. These are detailed in the warranting framework at paragraph 102 of this RIS.

299. How the warrant is implemented will then be subject to independent review by the IGIS. These changes will constitute a 'triple lock' of protection for New Zealanders that will ensure that intrusive powers are not abused.

300. The IGIS is able to inquire, not only into matters of legality in relation to the agencies, but also into issues of propriety. Procedural requirements have been included in certain proposals that ensure the expertise of the Privacy Commissioner forms an important part of the oversight arrangements.

Impact on human rights

301. Of particular note in this regard are provisions within the Bill that may impact upon the right to be free from unreasonable search and seizure. Shared powers between the agencies that might impinge upon the right include the ability to seize physical and non-physical things (including information) and the ability to search a place or thing (including information infrastructures). In New Zealand, this right requires both that powers of search, and the exercise of those powers, are reasonable and that there are appropriate safeguards to ensure that reasonableness. Officials are confident that the authorisation process is sufficiently robust to meet these requirements. Inherent in

this process is the need for the decision-maker(s) to be satisfied that any search or seizure is a necessary and proportionate activity. The exercise of the power is in turn subject to external oversight from the IGIS.

302. Certain aspects of the Bill infringe upon the right of individuals to be free from discrimination. Non-discrimination is a core value in New Zealand society and the right to be free from unfair discrimination is protected by the Human Rights Act 1993 and the Bill of Rights Act 1990. This Bill will discriminate on the basis of nationality, in that New Zealand citizens and permanent residents are afforded added protections in the warranting and oversight regime compared to foreign nationals. Officials are confident that national security and the national interest provide sufficient grounds for a limitation on the right, and that drawing such a distinction in this sphere reflects established practice in New Zealand and comparable jurisdictions.

303. The Bill will also impact upon the right of citizens to enter New Zealand and the right of everyone to leave. These rights are protected by the Bill of Rights Act. The Bill proposes to extend amendments made to the Passports Act, which were passed in 2014 as part of the Countering Terrorist Fighters Legislation Amendment Bill. The provisions allow the Minister of Internal Affairs to refuse to issue or to cancel a passport or refugee travel document, to cancel a certificate of identity, or to cancel emergency travel documents on grounds of national security.

304. Officials are of the view that the need to be able to prevent the movement of people for national security purposes is a justifiable limit on this right and the need is particularly acute in light of the rise of foreign terrorist fighters attempting to travel from our region to the Middle East. While the scale of the foreign terrorist fighter problem is lower in New Zealand than in some other countries, these changes amount to a proportionate response because of the significance of any New Zealander traveling to join a terrorist group, our responsibilities as a good international citizen and the checks placed on the power to prevent it being abused. The reviewers' have recommended adding an additional safeguard to this power, that any decision to cancel travel documents on the grounds of national security be reviewed by a judicial commissioner on the basis of judicial review. Officials agree that this is an appropriate constraint.

305. Surveillance, or the perception of surveillance, can also impact upon the right to freedom of expression. Studies have demonstrated that a person's behaviour can change when they are given reason to believe that they are being watched. These concerns are compounded by recent technological advances that increase the ability of governments and the private sector to monitor individuals and further still by the fact that the intelligence agencies are careful to ensure that their methods are kept secret. The reviewers note in their report that the need for 'greater clarity in the legislation about what the agencies can and cannot do' was a significant theme amongst public submissions. The Government agrees that there is room for enhancing transparency and has made it an overarching objective of the new legislation. A single Act, with a clear explanation of powers and the circumstances in which they can be used against New Zealanders, will be a significant step forward in this respect.

Impact on public confidence in the agencies

306. The covert nature of intelligence activities means that special authorisations and oversight processes are required to ensure robust control of the activities of the

agencies. The details around the authorisation of covert activities, or the undertaking of activities that do not require authorisation must, by necessity, remain secret. This secrecy is required to protect sensitive operational activities and capabilities, and partnerships with other agencies. However, secrecy will always result in a level of anxiety and suspicion for some, particularly where there is the potential to impact the rights and freedoms that the public enjoy.

307. While the proposed reformulation of the authorising regime and oversight mechanism could, potentially, go some way to assuring the public that the agencies are subject to an appropriate level of control and oversight, it is likely that concerns will remain. Additionally, the expansion of the powers that the agencies can draw upon will also reinforce these concerns.

308. Aside from the expansion of the authorising regime and oversight mechanism, mitigation of these concerns will be achieved by the greater clarity as to the role and powers of agencies, and their oversight mechanisms, provided by the creation of a single Act. The agencies are also engaging more with the public, and this is an important development.

Financial impact

309. The financial impacts of the proposed package of reforms are yet to be fully determined but expected to be minor. Minor financial impacts may come in the form of increased staffing, training and administrative costs.

310. Remuneration for the directors of the NZSIS and GCSB is currently set by the Remuneration Authority. There may be funding implications from moving this to the State Services Commissioner as different frameworks are used for each. The SSC is working with the Remuneration Authority to smooth the transition to the State Services Commissioner acting as the employer of the chief executives of the NZSIS and GCSB. Any financial implications arising from this will be looked at during the development of the implementation work programme.

311. Any changes made to the roles and functions of the two directors may affect the total package for either role. This has yet to be determined but in either case will be a cost to the agencies.

312. An increase in the number of judicial commissioners will also have financial implications. This is unlikely to be significant as the costs are driven by the time the commissioners spend.

313. The proposal to shift the setting of remuneration for the IGIS and the Deputy Inspector General to the Remuneration Authority may have financial implications. However, at this stage it is not clear if that is the case.

314. In some circumstances, there may be some increased costs on government entities associated with providing access to data sets. In others, costs will be decreased with through allowing direct access. These details are yet to be resolved as the specific mechanisms for sharing information have not been identified.

315. As was set out in Cabinet Paper One (NSC-16-MIN-0007) of the proposed package of reforms, any fiscal implications of the proposals will be covered from within the agencies' baselines.

Consultation

316. There are two main phases of consultation – the review and the Government's response to the review. The passage of the legislation will also be subject to a full legislative process allowing for public consultation during the select committee phase.

317. The reviewers underwent a thorough consultation process. They first called for public submissions and received responses from more than 100 individuals and organisations. They also met with academics, lawyers, telecommunications providers, and representatives from the intelligence communities of Australia, the UK, Canada and the United States. Annex B of the reviewers' report lists their consultation activities in full.

318. The reviewers note that when engaging with the public there were a broad range of perspectives however a number of common themes emerged about the need for:

- Increased transparency, accountability and oversight
- Greater clarity in the legislation about what the agencies can and cannot do and,
- A strong emphasis on protecting individual rights and freedoms

319. The reviewers explain that these general themes form the overarching recommendation for a clearer, more comprehensive legislative framework with strong safeguards and oversight in place for all of the agencies activities.

320. The second stage of consultation occurred during the government's response to the reviewers' recommendations. Officials in the Department of the Prime Minister and Cabinet ran an in-depth consultation process with relevant government agencies. This has involved circulating each Cabinet paper for comment and hosting interagency meetings on key issues. Agencies engaged have included the NZSIS, the GCSB, the Ministry of Foreign Affairs and Trade (MFAT), New Zealand Defence Force (NZDF), Ministry of Defence (MoD), Ministry of Justice (MoJ), Department of Internal Affairs(DIA), the New Zealand Customs Service, Ministry of Business, Innovation and Employment (MBIE), New Zealand Police, the Treasury and the State Services Commission (SSC).

321. On specific issues, such as information sharing, officials have also consulted with other agencies such as the Ministry of Education, the Ministry of Transport and the Inland Revenue Department (IRD).

322. Officials have also met with other relevant entities such as the Ombudsman, the office of the Privacy Commissioner, the Commissioner of Security Warrants, the IGIS and the Human Rights Commission in relation to the overall Government response and specific issues of relevance to those bodies.

323. Officials have focused their attention on consulting with government agencies on the workability of policy proposals and have not consulted the public, non-governmental organisations or business sector groups such as the airline or cruise ship industry. These groups can express their views at the select committee stage.

324. Officials have considered material provided during agency consultation on proposals in the Cabinet papers. While officials consulted on all proposals, this RIS focusses

instead on specific themes that emerged from the consultation process. For ease of reference, this is grouped by type of agency below.

325. Overarching themes from consultation with security sector agencies

- The work and capabilities of the agencies were highly sought after by agencies in the security sector who seek to leverage their skills and expertise;
- Security agencies hope to see a regime developed that would see intelligence helping to inform their decision making to a greater extent;
- Need for clear legislation and clarity around what will be within the scope of the agencies, what will be covered by the national security provision;
- Need for clear roles amongst different agencies; and
- Need for flexibility in the legislation so that it can respond to the a fluid security environment.

326. Overarching themes from consultation with oversight agencies, the State Services Commission and the Ministry of Justice were:

- Would like to see the agencies brought into the state sector through the State Sector Act 1988;
- Need for clear legislation;
- Need for robust oversight of access to personal information; and
- Need to align the agencies' activities more with the Privacy Principles contained in the Privacy Act 1993.

There were a number of specific issues that were also consulted on in greater depth. The following are a number of examples of how DPMC approached consultation on different types of issues:

327. *The definition of national security:* DPMC hosted an interagency workshop with approximately fifteen Government departments including the agencies, NZ Police, Customs, NZDF, MFAT and Justice to discuss the reviewers' proposed definition. There were a range of views on the reviewers' proposed definition but a consensus emerged that there was a lack of clarity within the definition about the activities that would or be covered under the definition. Various scenarios were discussed as well as alternate approaches to the reviewers' proposed concept. DPMC took these comments and formulated alternate definitions which were circulated amongst the agencies and other entities such as Crown Law. The alternate preferred approach (set out earlier in the RIS) represents the wider agencies' desire for more clarity in the definition.

328. *Information sharing:* the reviewers recommended that the agencies have direct access to certain datasets and access to restricted information on a case-by-case basis. This has required consultation with agencies holding such information (including Customs, DIA, MBIE, Education, Police and IRD), as well as with agencies with a general interest (such as Justice and the Office of the Privacy Commissioner). The agencies requested access to the Police's National Intelligence Application, primarily for the purposes of ensuring the safety of their staff while on operations.

After consultation with Police it was decided that this would not be appropriate and issues of physical security are best handled through the agencies continuing to work closely with the Police as issues arise.

329. *Judicial commissioners:* The reviewers recommended that the Government appoint a panel of judicial commissioners to be overseen by a Chief Commissioner of Intelligence Warrants. The Government consulted with a number of different parties including the Chief Justice and the Commissioner of Security Warrants, Sir Bruce Robertson. These discussions influenced the decision not to provide for the immediate appointment of three judicial commissioners, and to not include sitting judges as judicial commissioners.

Monitoring, evaluation and review

330. Section 21 of the ISC Act requires 'a review of the intelligence and security agenices, the legislation governing them, and their oversight legislation' to be 'held at intervals not shorter than 5 years and not longer than 7 years'. Officials have recommended that this section to be reproduced in a new Act.

331. In a changing threat environment, this is an appropriate timeframe for the government to review whether the settings are appropriate for New Zealand's security and for the public's confidence in the agencies.

332. Officials consider that the enhanced oversight of the IGIS and the ISC will enable close monitoring of the implementation and workability of the new legislation. Monitoring and evaluation through these mechanisms is appropriate as safeguards apply to ensure classified information and details of sensitive operations and capabilities are protected.

Implementation Plan

333. The changes proposed will have significant operational impacts and will require an extensive programme of work to ensure that they are implemented fully by the date that the Bill commences (the majority of the Bill will commence six months after the date on which the Bill receives the Royal assent) and to manage risks associated with the changes.

334. The NZSIS and GCSB have begun to develop an implementation workplan. That work plan will be developed in consultation with the Department of the Prime Minister and Cabinet, the State Services Commission, and the Treasury. The Minister in Charge of the NZSIS and Responsible for the GCSB will be briefed by 1 August 2016 on the workplan and implications.

335. The workplan will set out the workstreams and resourcing necessary to implement the following matters:

- the agencies being subject to the State Sector Act 1988 (including the associated application of the Employment Relations Act 2000), such as the development of a code of conduct and comprehensive employment relations policies;

- Ministerial Policy Statements, which will set the parameters for lawful activities carried out by the agencies in pursuit of their security and intelligence functions (as detailed in Paper two of this suite of papers);

- development of internal warranting and authorisation processes to ensure compliance with the new statutory regime;

- development of policies and processes to support better coordination and cooperation between the agencies, with particular reference to the authorisation regime;

- procedures for accessing, understanding and protecting other agencies' information; and

- any other matters that might appropriately be brought into this implementation work stream.

Transitional arrangements

336. The provisions of the Bill that will continue the amendments to the Passports Act 1992 put in place by the Countering Terrorist Fighters Legislation Bill will commence immediately after the Bill receives Royal assent. Certain provisions giving the agencies access to datasets held by other government agencies will commence the day after the Bill receives Royal Assent. It is proposed that the rest of the Bill come into force six months after the Bill receives Royal Assent.

337. Warrants and authorisations under both the New Zealand Security Intelligence Service Act and the Government Communications Security Bureau Act should be "grandfathered" consistent with the approach that was taken in the Search and Surveillance Act 2012. That Act provided that applications made prior to commencement but not determined were to be determined under and governed by the old provisions and warrants that were in force at the date of commencement were to continue in force with the old provisions applying to them. We note that this will enable the existing warrants and authorisations to be transitioned to the new legislative regime in a progressive fashion rather than requiring them all to be renewed in a short period, which would put pressure on the agencies and on the relevant Ministers and the judicial commissioners.

338. Cancellations and refusals to issue travel documents made under the temporary provisions in the Schedule to the Passports Amendment Act 2014 should be treated as if they had been made under the re-enacted provisions in the new Act so that timeframes are unaffected by the transition to the new provisions.

339. The Directors of the agencies in office at the time the legislation commences will continue in office, subject to certain conditions being met.

340. In the event of these conditions not being met, no compensation will be payable to either (which is consistent with the Directors' current terms of appointment).

341. The appointments of the IGIS and the Deputy IGIS should be treated as if they were made under the new Act meaning that the terms of both appointments continue as originally intended at the time of appointment.

342. The ability of the responsible Minister or the Prime Minister to agree to the findings of the IGIS being referred to the ISC should apply to any own-motion inquiry or an inquiry requested by one of those Ministers, regardless of whether the inquiry commenced prior to the commencement of the new Act.

343. The appointment of the Commissioner of Security Warrants will not be continued under the new legislation. A Chief Commissioner will be appointed at the appropriate time. Officials consider that the new role of the Chief Commissioner is sufficiently distinct from the role undertaken by the Commissioner of Security Warrants at present to mean a fresh appointment is required.

ANNEX A: Terms of Reference for the First Independent Review of the Intelligence Agencies

The purpose of the review, taking into account that subsequent reviews must occur every 5 – 7 years, is to determine:

- whether the legislative frameworks of the intelligence and security agencies (GCSB and NZSIS) are well placed to protect New Zealand's current and future national security, while protecting individual rights;

- whether the current oversight arrangements provide sufficient safeguards at an operational, judicial and political level to ensure the GCSB and NZSIS act lawfully and maintain public confidence.

The review will have particular regard to the following matters:

- whether the legislative provisions arising from the Countering Foreign Terrorist Fighters legislation, which expire on 31 March 2017, should be extended or modified;

- whether the definition of "private communication" in the legislation governing the GCSB is satisfactory;

- any additional matters that arise during the review as agreed by the Acting Attorney General and notified in writing in the NZ Gazette.

When determining how to conduct the review, the reviewers will take into account:

- the need to ensure that a wide range of members of the public have the opportunity to express their views on issues relating to the review;

- the need for the law to provide clear and easily understandable parameters of operation;

- the Law Commission's work on whether current court processes are sufficient for dealing with classified and security sensitive information;

- previous relevant reviews and progress towards implementing their recommendations;

- relevant overseas reviews to identify best practice in areas relevant to this review, including oversight arrangements;

- that traditionally, signals and human intelligence have been carried out separately and the Government does not intend to consider merging those functions within a single agency.

ANNEX B: SHARED WARRANTING FRAMEWORK FOR NZSIS & GCSB

WARRANT FOR THE PURPOSE OF

- The proper performance of one of the agencies' functions
- To test, maintain or develop capabilities
- To train employees for the purpose of performing the agencies' functions

Functions

- Collect intelligence in accordance with government requirements
- Protective security, including vetting and cybersecurity
- Assisting other government agencies: (a) within the authorities of NZDF or Police and (b) any other government agencies where imminent threat to life of New Zealander in New Zealand or overseas, or any person in New Zealand or on the high seas

SHARED WARRANTABLE POWERS (para 39)

- Interception of communications
- Search a place or a thing (including information infrastructures)
- Seize physical & non-physical things (including information)
- Conduct surveillance (including visual surveillance & electronic tracking)
- Collect intelligence through human sources or intelligence officers (including online) where source or officer may be required to undertake an unlawful act
- Request a foreign partner to undertake activities that would require a warrant for GCSB or NZSIS to do
- Use powers to give effect to do anything else necessary and reasonable to maintain or obfuscate collection capabilities
- Any other act necessary or desirable to protect communications or information infrastructures of importance to govt of NZ

GCSB only

SEPARATE POWERS TO GIVE EFFECT

GCSB = green only, unless joint warrant then all
NZSIS = green and red

- Access to information infrastructure

  Access = instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of, including any audio or visual capability that is part of the information infrastructure being accessed.
- Extract and use any electricity
- Install, use, maintain or remove interception device
- Install, maintain, use or remove an audio or visual surveillance device to maintain the operational security of a warranted activity
- Install, use, maintain or remove a visual surveillance device
- Install, use maintain or remove a tracking device
- Break open or interfere with any vehicle or other thing
- Enter any place, vehicle or other thing authorised by the warrant
- Take photographs, sound and video recordings, and drawings of a place, vehicle or other thing searched, and of any thing found in or on that place, vehicle or other thing of thing searched
- Use any force in respect of any place, vehicle or thing that is reasonable for the purposes of carrying out a search or seizure
- To bring and use in or on the place, vehicle or other thing searched, and to use any equipment found on the place, vehicle or thing
- To bring and use in or on the place vehicle or other thing searched, a dog

SHARED, GENERAL ANCILLARY POWERS

- Any other act that is reasonable in the circumstances and reasonably required to achieve the purposes for which the warrant was issued
- Anything reasonably necessary to conceal the fact that anything has been done under the warrant, or reasonably necessary to keep warranted activities of the agencies covert

Addendum to Regulatory Impact Statement: Intelligence and Security Legislation

11 August 2016

Information sharing arrangements and, assisting other organisations

Executive summary

1. This addendum to the Regulatory Impact Statement (RIS) covers two matters:

   - proposals to improve information sharing arrangements for the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS); and

   - explicitly providing for the GCSB and NZSIS to be able to assist other organisations, primarily the New Zealand Police and the New Zealand Defence Force, to perform their functions in a timely and effective manner.

2. The primary RIS (which is entitled *"Intelligence Services and Oversight Bill"*) covered access to certain government datasets, such as births deaths and marriages registers. However, it did not cover case by case information sharing arrangements between the GCSB and NZSIS (the agencies) and other organisations such as other government agencies, telecommunications providers, and banks. It also did not cover the issue raised in the review of whether the current legislation is too restrictive with respect to assistance to other organisations such as the New Zealand Police and New Zealand Defence Force.

3. Cabinet authorised the Minister for National Security and Intelligence and the Minister Responsible for the GCSB and in Charge of the NZSIS/the Attorney-General to take decisions following further officials' advice on these matters, with the Minister of Justice included for decisions on information sharing arrangements.

4. On information sharing, it is recommended the Bill include provisions that recognise the agencies' existing ability to ask for information, as well as individuals' and other organisations' existing abilities to disclose information to them where disclosure is not otherwise constrained. Those requests and disclosures would only be permitted where necessary for the performance of the agencies' functions.

5. It is also recommended that more Privacy Act 1993 information privacy principles are applied to the agencies, as only very few currently apply. It is possible to apply a broader range of principles to the agencies without undermining their ability to protect New Zealand and its interests, and without overly complicating the scheme of the Privacy Act 1993. Some privacy principles would need in-built exemptions. These in-built exemptions would allow the use and disclosure of personal information where it is necessary for the performance of the agencies' functions.

6. On assistance, it is recommended that the Bill provide for cooperation and assistance (whether in New Zealand or abroad), where it is necessary to respond to an imminent threat to the life or security of a New Zealander or anyone in New Zealand or in international waters or air space. Such a provision would need appropriate restrictions and involve oversight by the Inspector General of Intelligence and Security. This is in

addition to retaining the current assistance function in the Government Communications Security Bureau Act 2003 and extending it to the NZSIS.

7. The advice summarised in this addendum includes information provided by the Ministry of Justice, New Zealand Police, the GCSB and the NZSIS. The Inspector-General of Intelligence and Security and the Privacy Commissioner were also consulted on some matters and their comments reflected.

Objectives

8. The Government's objectives are set out in paragraph 13 of the primary RIS. Relevant to matters in this addendum, effective engagement and cooperation is a theme alongside building public trust and confidence in the agencies.

Analysis by issue

Information sharing arrangements

Status quo and problem definition

9. To perform their statutory functions, the GCSB and the NZSIS often need data and information, including personal information, lawfully collected and held by individuals or organisations in New Zealand, as well as intelligence or other material generated (collectively, "information") by those individuals or organisations. And reciprocally, other government organisations seek information from the agencies. Those government organisations may need to disclose information to the GCSB and/or the NZSIS to identify their intelligence needs, for example.

10. The problem with the current system is that the governing statutes do not specifically state that both agencies are able to request the disclosure of information. Nor do the statutes clearly provide for individuals other organisations to disclose information to the GCSB or the NZSIS, creating uncertainty in respect of their general ability to disclose information to the agencies.

11. In addition, the Privacy Act 1993 contains 12 information privacy principles that apply to the collection, storage and security, access to and correction of, retention, use, and disclosure of personal information. By virtue of an exception that is contained in section 57 of the Privacy Act, the agencies are currently only subject to a limited set of the principles. The agencies are covered by principles 6, 7, and 12. (An appendix to this addendum sets out all of the information privacy principles, together with a description of the proposed changes in relation to the GCSB and the NZSIS.)

Reviewers' recommendations

12. Broadly, the reviewers recommended that the shared functions of the agencies should include collecting intelligence and assisting other government organisations. Also, any collected information should be examined and used only for the purpose of performing one or more of their functions. The reviewers did not provide specific recommendations on information sharing, beyond recommending access to specific datasets and some information that cannot be disclosed to the agencies because of a statutory restriction on its disclosure.

13. The reviewers' report proceeded on the basis that personal information can be disclosed to the agencies on a case-by-case basis given section 57 of the Privacy Act 1993, which provides that disclosure of personal information to and by the agencies is not subject to the relevant information privacy principle. It did not, therefore, include recommendations about case-by-case disclosures. Nor did it address the application of further information privacy principles to the agencies.

Preferred Option

14. It is proposed that the Bill also recognise that the GCSB and the NZSIS may request disclosure of information from other organisations, and that the Bill describe the ability of other organisations to disclose information to the GCSB and the NZSIS in certain circumstances.

15. It is also proposed that the Bill amend the Privacy Act 1993 so that information privacy principles 1, 4(a), 5, 8, 9, 10, and 11 apply to the GCSB and the NZSIS. These principles do not currently apply.

16. In considering the suite of information privacy principles, some remain incompatible with the functions of the agencies – specifically principles 2, 3 and 4(b).

    - Principles 2 and 3 provide for, respectively, collecting information directly from the individual as the default means of collection, and making the individual aware of the collection of information. The nature of intelligence collection means that the presumed starting point for collection is usually a source other than the individual concerned. As such, applying either of these principles to the GCSB and the NZSIS is fundamentally at odds with the nature of their work.

    - Principle 4(b) restricts collection of information by unfair means or by means that intrude, to an unreasonable extent, upon the personal affairs of the individual. The nature of intelligence collection, however, can lend itself to an element – and sometimes a significant element – of deception, covertness, or intrusion. It is difficult to maintain an argument that these means of collection can ever be said to be 'fair'.

17. Applying principles 10 and 11 to the NZSIS and the GCSB requires an additional in-built exception to avoid any possibility of the principles constraining the agencies' ability to protect New Zealand and its interests.

    - Principles 10 and 11 respectively limit the use and disclosure of personal information unless certain grounds for exception are met. Some of the intelligence collection scenarios do not fit within the exceptions listed. For example, a person planning to travel overseas to participate in terrorism may not have committed an offence and would therefore be unlikely to fall within the listed exception of 'maintenance of the law'. Information use or disclosure necessary for the prevention of offences outside of New Zealand is also not covered well by the Privacy Act 1993. And information used by the agencies to assess threats to public health or safety may not meet the condition of being 'necessary to prevent or lessen a serious threat' because the threat may not yet have crystallised.

18. For principles 10 and 11 it is recommended that bespoke exemptions be added to the Privacy Act based around the GCSB's and the NZSIS's statutory functions. Specifically, the particular use/disclosure of certain information should be provided for, where it is necessary, to enable the performance of all or any of the GCSB's and the NZSIS's statutory functions..

19. Another option to increased application of the Privacy Act principles is to make the GCSB and the NZSIS subject to bespoke privacy principles set out in the Bill. However, officials consider that there is considerable benefit in being able to point to the GCSB and the NZSIS being made subject to the more of the information privacy principles. This is consistent with the theme underlying the reviewers' report to make both agencies more fully subject to the requirements usually applying to public sector organisations.

20. The organisations referred to here include individuals, as well as body corporates and unincorporated entities, departments and departmental agencies. In practice, the agencies frequently seek and receive information from organisations such as other government agencies, telecommunications providers, and banks in order to carry out their functions.

21. The range of organisations involved means that amendments will be required to certain Codes of Practice issued under the Privacy Act in order to give effect to the decision to insert bespoke exemptions for the GCSB and the NZSIS in the information privacy principles. In particular, it is likely that urgent amendments to the Credit Reporting Code, Telecommunications Information Code, and Health Information Privacy Code will be made so that the rules from those Codes that substitute in place of information privacy principles 10 and 11 will include the same bespoke exception that is included in the principles in the body of the Privacy Act. Urgent amendments to Codes of Practice under the Privacy Act dispense with public consultation, and are as a result, temporary. It is proposed therefore that wider consultation will be carried out before making permanent amendments after a year.

Impacts

22. *Intelligence* – the proposed changes would give the agencies legal clarity about their ability to request disclosure of information. The changes will also give individuals and other organisations in New Zealand more legal clarity and certainty about their ability to disclose information to the agencies, thereby improving the agencies' ability to carry out their statutory functions.

23. *Privacy* – the application of additional information privacy principles to the agencies would have an impact on the privacy of the people to whom personal information held by the agencies relates. Individuals may complain to the Privacy Commissioner if they consider that the GCSB or the NZSIS has interfered with their privacy, but this right only applies to actions that engage information privacy principles that apply to the GCSB and the NZSIS. Increased application of the principles gives individuals an avenue of complaint in respect of certain actions taken by the NZSIS and GCSB where none has existed previously. Increased clarity about the legal position in this area will make information sharing easier, leading to the possibility of greater information sharing and therefore privacy impacts on a greater number of people. However, this is counter-balanced by the greater scope for complaint to the Privacy Commissioner brought about by the application of further information privacy principles.

24. *Transparency* – the proposed provisions for request and disclosure would increase transparency in respect of the agencies' activities, since it will be clear on the face of their legislation that they regularly request disclosure of information and that other organisations regularly disclose information to them. Increased application of the Privacy Act 1993 will also increase transparency about information handling practices.

25. *Administrative clarity* - there is a risk that the provision acknowledging individuals' and organisations' abilities to disclose information may create confusion about the basis for disclosure of personal information (which will be in the Privacy Act 1993 or any relevant Code of Practice issued under that Act). There is also an argument that the lack of equivalent disclosure provisions in statutes governing other organisations may lead to those statutes being read restrictively, thereby precluding other organisations' abilities to disclose information in the absence of an equivalent provision to that proposed for the NZSIS and the GCSB. Careful drafting will be required to minimise these impacts.

GCSB and NZSIS assisting other government organisations

Status quo and problem definition

26. GCSB has a statutory function of assisting specified organisations – the policy, Defence Force and SIS. There is no legislated provision to help other organisations such as Maritime New Zealand or the Royal New Zealand Coastguard where the specialist capabilities of the agencies might assist with a search and rescue. SIS does not have any legislated function of assistance.

27. The GCSB have not always been able to provide assistance in a timely or effective manner to the Police, New Zealand Defence Force, or the NZSIS. This includes being able to support in search and rescue situations, assistance for drug investigations or helping the New Zealand Defence Force when they are deployed overseas. Examples include the Police or Maritime New Zealand looking for a missing tramper or lost yacht. Searchers would benefit from information obtained from intercepting communications. The NZSIS, in particular, does not have a specific statutory function of assisting other entities carry out their functions. Deployment with the NZ Defence Force was a scenario referenced in the review where there would be benefit in explicit provision for assistance.

Reviewers' recommendations

28. The Reviewers recommended that the GCSB and the NZSIS be able to:

- co-operate with each other and with the Police and the Defence Force, and assist those agencies to carry out their functions in accordance with their governing legislation, and

- co-operate with and assist other government organisations (whether in New Zealand or overseas), where it is necessary to respond to an imminent threat to the life or security of a New Zealander overseas or any person in New Zealand or on the high seas. This might include, for example, New Zealand Police, Maritime New Zealand, or overseas search and rescue authorities.

Preferred option

29. Officials recommend that the Bill include a provision based on current section 8C of the GCSB Act 2003 to clearly provide for both the GCSB and the NZSIS to be able to cooperate with each other and with the New Zealand Police and New Zealand Defence Force.

30. The Government Communications Security Bureau Act (section 8C) sets out as a function of the GCSB cooperation with, and the provision of advice and assistance to, the Police,

the New Zealand Defence Force and the NZSIS. This section also contains limitations on the performance of that function, and sets out the oversight provisions, including being subject to the Independent Police Conduct Authority and Inspector-General of Intelligence and Security, as relevant. Officials recommended retaining these provisions in respect of the GCSB and extending them the NZSIS to give the NZSIS a clear basis to assist the Police and the New Zealand Defence Force. A new provision is also proposed that enables the GCSB and the NZSIS to do anything necessary and desirable in order to cooperate with others (for example, agencies that have search and rescue responsibilities), where it is necessary to respond to an imminent threat to the life or security of a New Zealander or anyone in New Zealand or in international waters or airspace. The reviewers' reference to `high seas' should be expanded so it clearly covers international waters and airspace, and the area for which New Zealand has search and rescue responsibilities.

31. The scope of the proposed provision is broad. However, officials consider that this is necessarily so given the wide range of situations in which this function might be engaged and use of the NZSIS's and/or the GCSB's capabilities justified. Officials also propose a number of significant limitations be incorporated through supporting provisions that preclude the potential for circumventing the warranting process, including:

    - if the activity falls within the intelligence gathering and analysis or protective security functions of the agencies, then they should be required to obtain a warrant and cannot rely on the assistance function;

    - a restriction on the use of any information obtained through the assistance function for any other purpose (except to the extent that it is otherwise permitted by a warrant); and

    - oversight by the Inspector-General of Intelligence and Security.

Impacts

32. *Intelligence* – the proposed change would give the agencies, NZ Police, the Defence Force, and other organisations (for example those doing maritime search and rescue) more certainty in regard to having necessary information and assistance to legitimately carry out their functions.

33. *Privacy* – there would potentially be an impact on the privacy of the person to whom the information relates. However, any privacy impacts for a person who is subject to an imminent threat to life can be justified by the increased chances of rescue of that person in the search and rescue context. With respect to assistance to the New Zealand Police and New Zealand Defence Force, the NZSIS and the GCSB will only be able to act within the scope of the powers of the agency they are providing assistance to. Arguably, this means that any privacy impacts are ones that exist already.

Consultation

34. In addition to consultation set out in the principle RIS, the Inspector-General of Intelligence and Security and the Privacy Commissioner were specifically consulted on the information sharing proposals. On the application of the information privacy principles, both consider that all the principles can be applied.

35. The Privacy Commissioner supports provisions that recognise that the agencies may request disclosure of information and that other organisations may disclose information to the agencies, as they will enhance clarity about the legal situation. The Inspector-General of Intelligence and Security does not support these provisions on the basis they are legally unnecessary.

36. The NZ Police and the Defence Force support the proposed assistance provisions.

Implementation plan

37. The proposals will be implemented through the Intelligence Services and Oversight Bill. The GCSB and the NZSIS have already begun to develop an implementation work plan. Formal protocols will be developed (particularly with the Police) in relation to the carrying out of the agencies' assistance function to the NZ Police and the New Zealand Defence Force. These will ensure a clear understanding on the part of all agencies as to how the assistance function will work in any given situation, and provide for relationship management protocols and related procedures.

Monitoring, evaluation and review

38. In the primary RIS it is recommended that the existing requirement for a review of the governing legislation, at intervals not shorter than 5 years and not longer than 7 years, be included in the Bill.

Appendix 1: Table of proposed application of the IPPs to the GCSB and NZSIS

Summary of IPP	Applies now?	Proposed application
1: Purpose of collection of personal information Personal information shall not be collected by any agency unless (a) it is collected for a lawful purpose connected with a function or activity of the agency; and (b) the collection of that information is necessary for that purpose	No	Apply
2: Source of personal information Where an agency collects personal information, it shall collect the information directly from the individual concerned, unless it believes, on reasonable grounds, that certain circumstances, which are listed within the IPP, apply. These circumstances include, for example, where the agency believes on reasonable grounds that: • the information is publicly available; • non-compliance is necessary to avoid prejudice to the maintenance of the law; • compliance would prejudice the purposes of the collection; or • compliance is not reasonably practicable in the circumstances of the particular case.	No	Do not apply
3: Collection of information from subject Where an agency collects personal information directly from the individual concerned, it shall take such any steps reasonable in the circumstances to ensure, for example, the individual is aware of: • the fact that the information is being collected; • the purpose for which it is being collected; • the intended recipients of the information; • any relevant law that authorises or requires the information to be collected; and • their rights of access to, and correction of, personal information. It is not necessary for an agency to comply with these requirements if the agency believes on reasonable grounds, for example, that:	No	Do not apply

Summary of IPP	Applies now?	Proposed application
• non-compliance is authorised by the individual concerned; • non-compliance is necessary to avoid prejudice to the maintenance of the law; • compliance would prejudice the purposes of collection; or • compliance is not reasonably practicable in the circumstances of the particular case.		
<u>4: Manner of collection of personal information</u> Personal information shall not be collected by an agency - (a) by unlawful means; or (b) by means that, in the circumstances of the case,- (i) are unfair; or (ii) intrude to an unreasonable extent upon the personal affairs of the individual concerned.	No	Apply 4(a) Do not apply 4(b).
<u>5: Storage and security of personal information</u> An agency holding personal information must ensure that: • it is protected, by such safeguards as it is reasonable in the circumstances to take, against loss, unauthorised access, use, modification or disclosure; and • if it is necessary for the agency to give the information to a person in connection with the provision of a service to the agency, everything reasonably necessary within the power of the agency is done to prevent unauthorised use or unauthorised disclosure.	No	Apply.
<u>6: Access to personal information</u> Individuals are entitled to: • obtain confirmation of whether or not the agency holds such personal information; and • have access to that information. *Note the application of this principle is subject to section 27, which permits refusal to disclose information if disclosure would be likely to, for example, prejudice the security or*	Yes	Continue to apply.

Summary of IPP	Applies now?	Proposed application
defence of New Zealand or endanger the safety of an individual.		
7: Correction of personal information Individuals are entitled to request correction of their personal information. If information is incorrect, the relevant agency must take any reasonable steps to correct it.	Yes	Continue to apply.
8: Accuracy, etc, of personal information to be checked before use An agency holding personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading.	No	Apply.
9: Agency not to keep personal information for longer than necessary. An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.	No	Apply.
10: Limits on use of personal information. An agency that holds personal information that was obtained in connection with one purpose shall not use that information for any other purpose unless it believes on reasonable grounds that certain circumstances, which are listed within the IPP, apply. These circumstances include, for example, where the agency believes on reasonable grounds that: • non-compliance is necessary to avoid prejudice to the maintenance of the law or for the conduct of court proceedings (IPP 10(c)(i) and (iv)); or • that the use of information for that other purpose is necessary to prevent or lessen a serious threat to public health or public safety; or the life or health of the individual concerned or another individual (IPP 10(d)).	No	Apply with new in-built exception permitting use of personal information for a purpose other than that for which the information was collected where use is believed on reasonable grounds to be necessary to enable the performance of the GCSB's/NZSIS's functions.
11: Limits on disclosure of personal information An agency that holds personal information shall not disclose the information to a person or body or agency unless the	No	Apply with new in-built exception permitting disclosure of personal information for a

Summary of IPP	Applies now?	Proposed application
agency believes on reasonable grounds that certain circumstances, which are listed within the IPP, apply. These circumstances include, for example, where the agency believes on reasonable grounds that: • non-compliance is necessary to avoid prejudice to the maintenance of the law or for the conduct of court proceedings (IPP 11(e)(i) and (iv)); or • that the disclosure of the information is necessary to prevent or lessen a serious threat to public health or public safety; or the life or health of the individual concerned or another individual (IPP 11(f)).		purpose other than that for which the information was collected where disclosure is believed on reasonable grounds to be necessary to enable the performance of the GCSB's/NZSIS's functions.
<u>12: Unique identifiers</u> This principle places limits around the use of unique identifiers. In particular, agencies shall not assign unique identifiers unless they are necessary to enable the agency to carry out one or more of its functions efficiently.	Yes	Continue to apply.