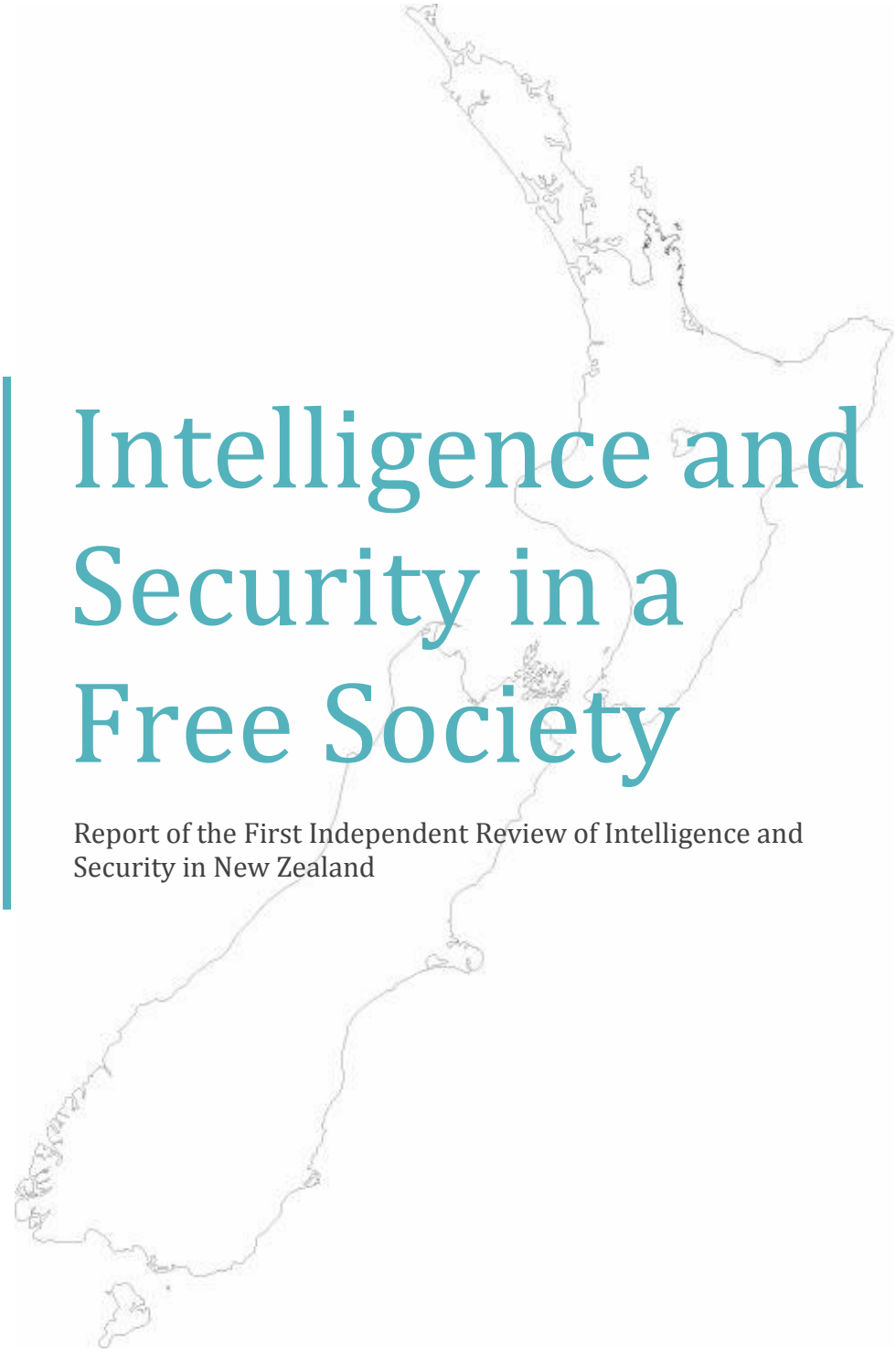


Intelligence and Security in a Free Society

Report of the First Independent Review of Intelligence and Security in New Zealand

Hon Sir Michael Cullen, KNZM and **Dame Patsy Reddy, DNZM**

29 February 2016

Foreword

The place of intelligence and security agencies in a free society arouses a wide range of responses and passions. For some, the security of the state and of the individuals within it overrides other considerations. That is especially so in times of obvious international security threats. Such a view may be summed up in the often used phrase "you have nothing to fear if you have nothing to hide".

For others, the opposite is true: freedom and liberty are so precious that any secret activity by state agencies must inevitably threaten those human rights, if only through the chilling effect of the fear of surveillance.

Most people's views probably lie somewhere between these two extremes. Ours certainly do. All that we have heard and read during this review have helped lead us to that position. Neither extreme reflects history, experience, or the realities of the modern world, especially with its borderless and rapidly multiplying forms of communication, its ease of fast international mobility and its increasingly complex security challenges.

Our review and report arises out of legislation passed in 2013 which included a requirement for periodic reviews "of the intelligence and security agencies, the legislation governing them, and their oversight legislation". In the event our terms of reference were limited to the legislative aspects. Accordingly, we have not undertaken a review of the agencies (of which there have, in fact, been a number in the last decade, including a major performance review in 2014).

We have, nevertheless, tried to develop a clear understanding of what the agencies do, how they do it, and what the rationale is for their existence. That has enabled us to develop what we hope is a clear and consistent set of recommendations for legislative change.

Our central conclusion is that there should be a single, integrated and comprehensive Act of Parliament that lays out in plain English how the agencies are constituted; what their purposes are; how all their intelligence and security activities are authorised; and how they are overseen so as to protect those freedoms and liberties that are part of what we are as a nation.

The Act should state clearly that its fundamental purpose is the protection of New Zealand as a free, open and democratic society. That then becomes the guiding principle by which the activities of the agencies must be undertaken and judged.

There should always be debate about how best to ensure that purpose is achieved. Freedom and liberty cannot be preserved either in a vacuum of apathy or in an atmosphere of tolerance of the abuse of power. But nor can they be preserved by wilfully or casually ignoring the existence of those who reject or threaten the values of freedom and liberty. Our report proposes a legislative framework designed to encompass both those enduring truths.

Hon Sir Michael Cullen KNZM

Dame Patsy Reddy DNZM

Contents

Executive summary

1. We were appointed by the Government as independent reviewers to conduct the first statutory review of New Zealand's intelligence and security agencies, the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS) (together, **the Agencies**). Amendments made to the Intelligence and Security Committee Act 1996 in 2013 require a review of the Agencies, the legislation governing them and their oversight legislation every five to seven years.

2. Our terms of reference (which are set out in full in Annex A) directed us to determine:

   - 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 Foreign Terrorist Fighters legislation, 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.

3. The primary purpose of our report is to set out a basis for comprehensive reform of the legislation relating to the Agencies. We also hope it will help to provide some clarity, so far as possible, about the purpose of intelligence and security agencies and what they do.

4. The need to maintain both security and the rights and liberties of New Zealanders has been at the forefront of our minds. Given the intrusive nature of the Agencies' activities, New Zealanders are understandably concerned about whether those activities are justifiable.

5. This concern is not helped by the fact that the Agencies' activities have been kept largely in the shadows. To secure public confidence in the modern world, the Agencies need to be able to demonstrate their value to New Zealanders. The legislation governing the Agencies also needs to include appropriate external and independent checks and balances. Because the Agencies cannot always be entirely open about their activities, the public needs to be able to count on oversight and accountability mechanisms to ensure they act lawfully and reasonably.

6. Another important part of the backdrop to our review is the need to ensure that the legislation allows for changes in the nature of threats and advances in technology. We are, after all, living in a time when change and uncertainty are ever-present. The Agencies must be able to adapt their activities to continue to meet New Zealand's needs.

Key issues identified

7. It quickly became apparent to us that there were a number of deficiencies in the Agencies' current legislative frameworks. The legislation establishing the Agencies is not comprehensive, is inconsistent between the two agencies, can be difficult to interpret and has not kept pace with the changing technological environment. This has led to some significant problems.

8. First, 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. Critical reviews in the past[1] have led the Agencies, particularly the GCSB, to take a very conservative approach to interpreting their legislation. While we understand the reason for this, and it is certainly preferable to a disregard for the law, this overly cautious approach does mean that the GCSB is not as effective or as efficient as it could be. The legislation needs to set out clearly what the Agencies can do, in what circumstances and subject to what protections for individuals.

9. Second, the inconsistencies between the Government Communications Security Bureau Act 2003 (GCSB Act) and the New Zealand Security Intelligence Service Act 1969 (NZSIS Act) – in terms of the Agencies' functions, powers and authorisation regimes – create barriers to the Agencies working together. To provide the best possible foundation for well-informed decision-making, the government needs to receive intelligence that is comprehensive and robustly tested.

10. The nature of security threats and the methods of communication used by those seeking to harm New Zealand's interests have changed drastically since the Agencies were established. We are living in an increasingly globalised world where threats do not respect geographical boundaries. In the modern technological and online environment, even internal threats to security can sometimes only be discovered or investigated using high-end electronic intelligence capabilities. The Agencies need to be able to combine their skills and knowledge to provide the information that the government requires, and the legislation should facilitate that.

11. Third, the systems for authorising the activities of the Agencies are not comprehensive. In the case of the NZSIS, in particular, many activities are carried out on the basis of the consent of the person or organisation holding the information (for example, obtaining telephone call metadata from telecommunications providers) or on the basis that the activity is not generally unlawful (for example, watching people in public places). The legislation does not provide for or require ministerial or judicial authorisation for these activities.

[1] In particular, Rebecca Kitteridge's *Review of Compliance at the Government Communications Security Bureau* (March 2013).

12. The Agencies' activities are, by their nature, intrusive. Unlike the activities of most public authorities, they are not ordinarily subject to public scrutiny or review by the courts. In that context, it is important that all of their activities are externally authorised and open to oversight to ensure they are reasonable, necessary and proportionate.

13. Fourth, it became clear to us that while intelligence can play an important role in supporting government decision-making, not all of it is useful. Intelligence collection is only of value to the extent that it focuses on the issues most important to New Zealand and is turned into a product that decision-makers can use. For this reason, we consider it is crucial 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.

Our proposals

14. Against that background, we set out in this report a range of recommendations to help ensure that the public can have confidence that the Agencies will act lawfully and appropriately, and that the legislation is fit for purpose in a modern context. We recommend that the Agencies, their oversight bodies and potentially also intelligence assessment be covered by a single piece of legislation. The legislation would include a new, comprehensive authorisation regime requiring 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. It would also make some changes to facilitate greater oversight of the Agencies and accountability for their activities.

15. These key proposals, along with the other changes we recommend, would ensure there are appropriate checks and balances on the Agencies' activities while removing unnecessary barriers to effective co-operation between them. It would also make the law easier to understand and apply. This would improve the Agencies' ability to comply with the law and allow oversight bodies to monitor compliance more effectively. By recommending increased transparency, we also hope to enable greater public involvement in the debate about how best to protect the security of New Zealand in a way that is consistent with the values of New Zealanders.

16. Our key recommendations are summarised below (paragraph 25 onward). The full recommendations are set out at the end of each relevant section of this report and listed in their entirety in Annex C.

Outline of the report

17. *Chapter 1 (Introduction)* explains the context for our review. We discuss the relationship between collective security and individual rights, and set out some key domestic and international developments relevant to the review.

18. *Chapter 2 (Intelligence)* explains what intelligence is and how the government uses it. It also explains why intelligence sometimes needs to be collected in secret, and the value of having intelligence and security functions performed by separate collection agencies (as distinct from the New Zealand Police or another public agency).

19. *Chapter 3 (New Zealand's intelligence system)* sets out the intelligence cycle and the role that each part of the intelligence community plays in it. We explain the processes for setting the government's intelligence priorities, collecting and assessing intelligence, and the various levels of oversight in place. We have tried to include in this section as much detail as possible about what the Agencies actually do and how they do it.

20. In *Chapter 4 (Transparency and accountability)*, we recommend the existing pieces of legislation be replaced with a single Act dealing with the Agencies, their oversight and potentially the assessment of intelligence. We also make recommendations to strengthen the accountability of the Agencies. Finally, we propose amendments to ensure the Inspector-General of Intelligence and Security ("Inspector-General") and Parliament's Intelligence and Security Committee are well-placed to oversee the activities of the intelligence community.

21. In *Chapter 5 (What should the Agencies do?)* we recommend the Agencies should have shared objectives and functions to allow them to work together more effectively. While recognising that the Agencies have a role in helping the government to advance New Zealand's economic and international interests, we recommend they should only be able to obtain a warrant to target New Zealanders where it is necessary to protect national security (or, in limited circumstances, if a New Zealander is acting on behalf of a foreign entity such as a government or terrorist organisation).

22. In *Chapter 6 (How should the Agencies operate?)* we set out a comprehensive authorisation framework. All of the Agencies' intelligence and security activities should require some form of authorisation at a ministerial level. Intrusive activities with a foreign focus would need to be authorised by the Attorney-General, while those relating to New Zealanders would require a warrant approved by both the Attorney-General and a judicial commissioner.

23. In *Chapter 7 (Accessing and using information)* we suggest the legislation be amended to clarify what information the intelligence and security agencies can access from other government agencies. We also recommend restrictions on the circumstances in which information can be accessed and retained.

24. *Chapter 8 (Countering Foreign Terrorist Fighters)* considers whether the amendments made in December 2014 under the Countering Foreign Terrorist Fighters Legislation Bill should be extended and/or modified. We recommend that the ability to conduct visual surveillance be subject to the same authorisation framework set out in Chapter 6. The amendments to the Passports Act 1992 should continue, but with additional safeguards.

Summary of key recommendations

Single Act

25. We recommend consolidating the objectives, functions and powers of the Agencies and the arrangements for their oversight into a single Intelligence and Security Act. This would provide greater clarity about what the Agencies can and cannot do, and what the checks and balances on their activities are. Currently, the Agencies have separate governing Acts that are creatures of history and incremental reform. This has created inconsistencies and uncertainty in how to interpret the law, which hampers the Agencies' ability to perform their functions effectively.

26. The purpose of the Act should be to protect New Zealand as a free, open and democratic society. This reflects the Agencies' role in assisting the government to fulfil its obligation to ensure its citizens can go about their lawful business safely and without undue interference with their human rights.

Integrating the Agencies within the public sector

27. Currently the GCSB is a public service department but is exempt from a number of provisions in the State Sector Act 1988. The NZSIS is not subject to the State Sector Act at all. We recommend that the NZSIS should be established as a public service department subject to the State Sector Act (with any appropriate exceptions or exemptions to reflect the unique nature of some aspects of their work). The State Sector Act provisions relating to the appointment, reappointment, remuneration, performance review and removal from office of the chief executive should apply to both agencies.

Objectives and functions of the Agencies

28. We recommend that the legislation require the Agencies to perform their functions in pursuit of a shared set of objectives, reflecting the core areas where intelligence is needed to support government decision-making and operational activity. The objectives should be to contribute to:

- the protection of New Zealand's national security, including its economic security, and the maintenance of international security (which can indirectly affect domestic security)

- New Zealand's international relations and well-being, and
- New Zealand's economic well-being.

29. The Agencies should also have common functions so that they can work together more effectively toward achieving the government's priorities. These common functions should include:

Collecting intelligence

- Collecting and analysing intelligence in accordance with the government's requirements.
- Providing any intelligence collected and any analysis of the intelligence to:
  - the Minister
  - the National Assessments Bureau ("NAB")[2] for assessment; and
  - any person, office holder, entity or class of persons, office holders or entities (whether in New Zealand or overseas) authorised by the Minister to receive the intelligence.

Protective security

- Co-operating with, advising and assisting public authorities (including overseas authorities) and any other person, office holder, entity or class of persons, office holders or entities (whether in New Zealand or overseas) authorised by the Minister on protective security matters.
- "Protective security" should be defined to include the Agencies' current functions in relation to the protection of information, people and assets against security threats (for example, cyber security, information assurance and vetting government employees).

Assisting other government agencies

- Co-operating with each other, and with the New Zealand Police and New Zealand Defence Force, and assisting those agencies to carry out their functions in accordance with their governing legislation, and
- Co-operating with and assisting any other government agency or entity (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.

[2] See paragraph 3.48 below.

Protecting New Zealanders

30. The Agencies should in general only be able to obtain a warrant to target New Zealand citizens, permanent residents and organisations for the purpose of protecting national security. Their broader objectives of contributing to New Zealand's economic and international well-being should only apply in relation to foreign persons and organisations (which might include, in limited circumstances, a New Zealander acting on behalf of a foreign entity such as a government or terrorist organisation).

31. We recommend removing the current restriction on the GCSB taking any action for the purpose of intercepting New Zealanders' private communications when performing its intelligence function (section 14 of the GCSB Act). As we explain in Chapter 5, the restriction is confusing, does not protect New Zealanders to the extent it suggests, and hinders the Agencies' ability to assist the government to protect New Zealand against security threats.

32. Instead, protections for New Zealanders should be implemented through a strengthened authorisation framework. If the Agencies wish to carry out any activity for the purpose of targeting a New Zealander, a warrant approved by both the Attorney-General and a judicial commissioner should be required.

A new authorisation framework

33. The legislation should require some form of authorisation for all of the Agencies' intelligence and security activities, to ensure that appropriate safeguards apply to everything they do.

34. We recommend a three-tiered approach to authorisation of the Agencies' activities, with higher levels of scrutiny for activity that is more intrusive or that targets New Zealanders.

Tier 1 authorisation – warrant approved by the Attorney-General and a judicial commissioner

35. The highest level of authorisation should be a warrant approved by the Attorney-General and a judicial commissioner ("tier 1 authorisation"), which would be required for any activities that would otherwise be unlawful and are for the purpose of targeting a New Zealand citizen, permanent resident or organisation.

36. Both the Attorney-General and judicial commissioner would need to be satisfied that the statutory criteria for issuing an authorisation are met. The Attorney-General would also take into account broader national interest considerations and would have discretion to decline to issue a warrant even if the criteria are met. The judicial commissioner would consider the legality of the application, including consistency with human rights laws.

37. As an additional safeguard, the legislation should provide for review warrants (issued through the same process as other tier 1 authorisations). A specific review warrant would be required if the Agencies wish to analyse incidentally obtained intelligence for the purpose of an

operation or investigation targeting a New Zealander. This will ensure incidental interception cannot be used as a way around the authorisation requirements.

Tier 2 authorisation – warrant approved by the Attorney-General

38. The second tier of authorisation would be a warrant issued by the Attorney-General. A tier 2 authorisation should be required for the Agencies to carry out any activities that would otherwise be unlawful, but are not for the purpose of targeting New Zealand citizens, permanent residents or organisations.

Tier 3 authorisation – policy statement issued by the Minister responsible for the Agencies

39. The lowest level of authorisation would be a policy statement issued by the Minister responsible for the Agencies after being referred to the Inspector-General for comment ("tier 3 authorisation"). Tier 3 authorisations should cover activity that is lawful without a tier 1 or 2 authorisation (for example, collection of open source information, surveillance in public places or access to information infrastructures with consent).

40. Each tier 3 authorisation should set out what information or activity it applies to, the purposes for which that information can be collected or activity carried out, the methods that can be used and any protections that need to be put in place (for example, privacy protections).

Basis for granting tier 1 and 2 authorisations

41. Before issuing a tier 1 or tier 2 authorisation, the Attorney-General and judicial commissioner would need to be satisfied that:

- the proposed activity is necessary either:
  - for the proper performance of one of the agency's functions, or
  - to test, maintain or develop capabilities or train employees for the purpose of performing the agency's functions
- the proposed activity is proportionate to the purposes 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 authorisation 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 the single Act.

42. The Attorney-General should be required to refer applications for tier 1 and tier 2 authorisations to the Minister of Foreign Affairs for comment if the proposed activity is likely to have implications for New Zealand's foreign policy or international relations. This will ensure any relevant risks are taken into account.

Records and reporting on authorisations

43. The Agencies should be required to keep a register of all authorisations issued. The register should be made available to the Inspector-General, the Minister responsible for the Agencies, the Attorney-General and the judicial commissioners.

44. The Agencies' annual reports should include reporting on the outcome of tier 1 and tier 2 authorisations (including review warrants). This will allow the Inspector-General to monitor whether necessity and proportionality is being accurately judged at the point when authorisations are sought.

Judicial Commissioners

45. We recommend introducing a panel of at least three judicial commissioners, headed by a Chief Commissioner of Intelligence Warrants (instead of the current single Commissioner of Security Warrants). A judicial commissioner should be available at all times to ensure that applications for tier 1 authorisations can be dealt with promptly. The judicial commissioners could either be retired judges, as the current Commissioner is, or sitting judges, as the role will be part-time.

Authorisation in situations of urgency or emergency

46. Sometimes the Agencies are alerted to an imminent threat at short notice or have only a brief window of time to obtain valuable intelligence. When this happens there may be insufficient time to follow the ordinary process for obtaining an authorisation. We recommend the Agencies should be able to commence activity normally requiring a tier 1 authorisation with approval from the Attorney-General (or another minister designated to act on his or her behalf) where:

- there is an imminent threat to the life or safety of any person, or
- the delay associated with obtaining an authorisation through the ordinary process is likely to seriously prejudice national security.

47. The Chief Commissioner of Intelligence Warrants should be notified immediately and be able to direct that the activity cease at any time. The Attorney-General and Commissioner should be provided with a full application for a tier 1 authorisation within 48 hours and consider it in the ordinary way. If the application is declined, any intelligence collected under the interim authorisation would need to be destroyed unless one of the grounds for retaining and disclosing incidentally obtained intelligence is met.

48. We also recommend that the Attorney-General or the minister designated to act on his or her behalf should be able to grant a tier 1 authorisation (including interim authorisations) or a tier 2 authorisation orally (for example, over the phone) provided the director of the agency certifies the approval has been given.

49. While the interim authorisation processes above should suffice in virtually all cases, we consider it desirable to provide for the unlikely but possible event that immediate action might be required and a relevant minister cannot be contacted in the short space of time available. As a last resort, the legislation should provide for a Director authorisation if obtaining an interim authorisation or a tier 2 authorisation from the Attorney-General or the acting Attorney-General would cause delay to such an extent that the purpose of obtaining it would be defeated.

50. Where an urgent Director authorisation is granted, the Director should notify the Attorney-General (and, for activity requiring a tier 1 authorisation, the Chief Commissioner of Intelligence Warrants) without delay and provide a full application within 24 hours.

Role of the Inspector-General of Intelligence and Security

51. The Inspector-General is the main external check on the Agencies. The independence of the role is crucial to ensure a balanced and politically-neutral assessment of the Agencies' activities. In order to ensure the independence of the Inspector-General, he or she should be appointed by the Governor-General on the recommendation of the House of Representatives. In addition, the Inspector-General's Office should be funded through an appropriation that is separate from that of the Agencies.

52. We also recommend that the Inspector-General's functions and powers be enhanced in a number of respects. The category of persons who can complain to the Inspector-General should be broadened to include non-New Zealanders. The legislation should clarify that the Inspector-General's ability to review authorisations is not just in relation to procedural matters but also includes a comprehensive look behind the face of an authorisation (for example, reviewing the Agencies' case for collecting the intelligence and how the intelligence is used). The current restriction on the Inspector-General's ability to inquire into operationally sensitive matters should also be removed.

Role of the Intelligence and Security Committee

53. We recommend increasing the maximum size of the Intelligence and Security Committee of Parliament ("ISC") to allow for greater flexibility in representation. The legislation should provide for a minimum of five and a maximum of seven members. The appropriate number should be determined by the Prime Minister after consulting the Leader of the Opposition.

54. The members of the ISC should be nominated by the Prime Minister after consultation with the Leader of the Opposition and subsequently be endorsed by the House of Representatives.

The Committee should also elect its own chairperson, who would not necessarily be the Prime Minister. Currently, the legislation states that the Prime Minister (or a member of ISC appointed by the Prime Minister) is the chairperson.

55. We recommend that the ISC should be able to request (but not require) the Inspector-General to carry out an inquiry 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.

56. One of the functions of the ISC is to consider any Bill in relation to the Agencies that is referred to it by Parliament. We do not think the ISC should replace the role of a subject select committee in this respect. Select committee consideration of Bills allows the views of a broader range of political parties to be taken into account, which we think is important. The government should in general refer proposed legislation relating to intelligence and security matters to an appropriate select committee. However, the government should consider placing any related classified material before ISC, which would report its conclusions to the select committee.

Centralising intelligence assessments

57. The government should consider including the role and functions of the National Assessments Bureau in the single Act. Its function should be to assess and prepare reports relating to New Zealand's national security and economic and international interests, and to provide these reports to the relevant decision-makers.

Arrangements with foreign partners

58. The legislation should require any co-operation with and provision of intelligence to foreign jurisdictions to be consistent with the purposes of the single Act and the Agencies' obligations to act in accordance with New Zealand law, including human rights obligations. Consistent with this approach, under the new authorisation framework we propose the Agencies would require an appropriate level of authorisation to access intelligence held by foreign partners. This would ensure the legislation does not provide scope for the Agencies to use foreign partners' capabilities to collect information they could not lawfully obtain themselves.

59. We recommend the Minister responsible for the Agencies formulate standard terms on which the Agencies can co-operate or share information with foreign jurisdictions and international organisations. The terms should be consistent with the Agencies' obligations to act in accordance with New Zealand law, including human rights obligations, and include appropriate protections for New Zealanders. The terms should be provided to the Inspector-General for comment. Once finalised, they should also be referred to the ISC to be noted, along with any future bilateral or multilateral arrangements with foreign jurisdictions or international organisations.

Accessing and using information

60. Currently the Agencies have internal measures in place to ensure that information that has been collected is only accessed by analysts in appropriate circumstances. However, this is not specifically addressed in the legislation. We consider the legislation should provide that the Agencies may only examine and use information intercepted or collected for the purpose of performing one or more of their functions, or where one of the grounds for retaining and disclosing incidentally obtained intelligence is met.

61. A tier 3 authorisation should establish procedures to ensure compliance with this requirement. Compliance with the authorisation should be monitored by the Inspector-General as part of his or her existing functions.

62. Sometimes the Agencies need to access information held by other government agencies, for example to identify individuals of security concern who are seeking to enter the country or to ensure the security of staff during field operations. We recommend that the Act specifically enable the Agencies to access and retain the following electronic datasets:

- information about border-crossing craft and persons shared with the New Zealand Customs Service
- Immigration New Zealand databases, including Advanced Passenger Processing data
- information held in the Police National Intelligence Application, and
- births, deaths, marriages and relationships registers and citizenship registers.

63. Accessing and retaining datasets should be subject to a joint protocol agreed between the Minister responsible for the NZSIS or the GCSB and the Minister responsible for the agency holding the information, in consultation with the Privacy Commissioner. The Inspector-General should monitor the Agencies' compliance with each protocol.

64. The legislation should also provide for access to the following information about individuals on a case-by-case basis, to assist the Agencies in their investigations:

- 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.

65. Access should be in accordance with a tier 2 authorisation, if the information relates to a foreign person or organisation, or a tier 1 authorisation, if the information relates to a New Zealander. All authorisations would be subject to review by the Inspector-General under his or her existing functions.

Countering Foreign Terrorist Fighters legislation

66. Our terms of reference required us to consider whether the temporary provisions introduced in December 2014 under the Countering Foreign Terrorist Fighters Legislation Bill should be extended or modified.

Disruption of travel

67. We recommend that the maximum three-year cancellation period for travel documents (increased from 12 months) should continue to apply. While this maximum period should not be treated as the default position, there are cases where people make plans to travel overseas to join a terrorist organisation over a long period and a 12-month cancellation period would be insufficient.

68. We do, however, consider that an additional safeguard should be put in place to ensure that decisions to cancel or refuse to issue travel documents are appropriately made. Any decision by the Minister of Internal Affairs under the relevant provisions of the Passports Act 1992 should be reviewed by a judicial commissioner, who would have the ability to overturn the decision if one of the grounds for judicial review is made out.

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

Visual surveillance

70. Under the temporary provisions, the new visual surveillance powers introduced for NZSIS are dealt with separately from other types of surveillance and subject to different requirements. They also only apply to counter-terrorism investigations.

71. We consider that the legislation should continue to enable visual surveillance by the Agencies in appropriate circumstances. However, we recommend that visual surveillance powers should be subject to the new authorisation regime we propose and treated the same as other types of surveillance. They should not be restricted to counter-terrorism investigations.

72. This is consistent with our recommendations for a single, comprehensive authorisation framework and with the approach taken to visual surveillance powers under the Search and Surveillance Act 2012. It also recognises that visual surveillance can be an equally valuable tool outside of the counter-terrorism context (for example, in counter-intelligence investigations).

Chapter 1: Introduction

1.1 This is the first comprehensive review of the legal framework governing New Zealand's intelligence and security agencies – the GCSB and NZSIS. It provides an opportunity for independent consideration of the proper role of the Agencies and what New Zealanders should be able to expect from them.

1.2 This review comes at a time of unique challenges. In New Zealand, there is a public perception that we are relatively sheltered from the threats currently faced by many other countries. There is also increasing concern about the privacy of New Zealanders, the Agencies' compliance with the law and the prospect of widespread data collection, particularly in the wake of Edward Snowden's information leaks[3] and controversies such as the GCSB's involvement in the events leading up to Kim Dotcom's arrest.[4]

1.3 These kinds of issues have also created public concern in other democratic countries, and have triggered reviews in many of them.[5] However, those reviews, to a greater extent than ours, have been conducted against a backdrop of heightened awareness of a very real threat of terrorism. In New Zealand there remains a much greater degree of public scepticism about the need for intelligence and security agencies, and suspicion of their activities.[6] We hope this report will help to de-mystify the work of the Agencies, so far as possible, and inform the public debate in a simple and helpful way.

Collective security and individual rights

1.4 The debate about how best to balance the need for security and the privacy of individuals will continue for as long as both are seen as essential to a free society. Many countries are

[3] See paragraph 1.39 below.
[4] The USA requested the extradition of Kim Dotcom in 2012 on charges relating to a conspiracy to infringe copyright. The GCSB, acting on a request from the New Zealand Police, intercepted Mr Dotcom's communications on the basis of its mistaken belief that Mr Dotcom was a foreign person and not a permanent resident. Mr Dotcom was the holder of a residence class visa. Under the GCSB Act, the holder of a residence class visa is a permanent resident of New Zealand. The interception of Mr Dotcom's communications was therefore unlawful as the GCSB was prohibited from intercepting the private communications of New Zealand permanent residents. Subsequently, the Prime Minister apologised to Mr Dotcom for GCSB's error. The incident prompted a review of compliance at the GCSB, which is discussed at paragraph 1.35 below.
[5] For example: Parliamentary Joint Committee on Intelligence and Security *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* (AU, May 2013); The President's Review Group on Intelligence and Communications Technologies *Liberty and Security in a Changing World* (USA, 12 December 2013); Intelligence and Security Committee of Parliament *Privacy and Security: A Modern and Transparent Legal Framework* (UK, March 2015); David Anderson QC *A Question of Trust: Report of the investigatory powers review* (UK, June 2015); Royal United Services Institute *A Democratic Licence to Operate: Report of the independent surveillance review* (UK, July 2015).
[6] See paragraph 1.11 below.

grappling with how best to approach reform of their national intelligence and security laws as they respond to domestic and global events. Each country has taken a different approach, influenced by the values of its citizens, its political institutions and its recent and historical experiences.

1.5 We have approached this question from the perspective that security and privacy are complementary rather than competing rights. As Article 3 of the Universal Declaration of Human Rights states, "Every person has the right to life, liberty and security of the person." Security is a prerequisite to a free, open and democratic society in which individuals can go about their lawful activities without undue interference with their rights. Equally, the organisations responsible for protecting security should not be able to act in such a way as to undermine those basic values.

1.6 States have a fundamental obligation to protect the security of people within their territory.[7] Included in this is the duty to protect people from deprivation of life, liberty or security by third parties operating within the state's territory, such as criminals and terrorist groups.[8] At the same time, the government must ensure that steps taken to protect security are consistent with other human rights.[9] Some rights that may arise in this context are those of freedom of movement,[10] freedom of expression,[11] freedom from discrimination[12] and the right to privacy.[13]

1.7 This does not mean the government must trade security off against human rights. Security *is* a human right, and the law that protects human rights must be flexible enough to allow a balance to be struck within it.[14] Most rights are not absolute. In New Zealand, the New Zealand Bill of Rights Act 1990 provides that rights may be subject to "such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society".[15]

---

[7] International Covenant on Civil and Political Rights, art 9; Office of the United Nations High Commissioner for Human Rights *Human Rights, Terrorism and Counter-Terrorism* (Fact Sheet 32, July 2008) at 8.
[8] United Nations Human Rights Committee *General Comment No. 35 on Article 9 of the International Covenant on Civil and Political Rights* (28 October 2014) at [7].
[9] United Nations General Assembly Human Rights Council *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin: Ten areas of best practices in countering terrorism* (A/HRC/16/51, 22 December 2010) at [12]; United Nations General Assembly Resolution 63/185 *Protection of human rights and fundamental freedoms while countering terrorism* (3 March 2009).
[10] New Zealand Bill of Rights Act 1990, s 18.
[11] New Zealand Bill of Rights Act 1990, s 14.
[12] New Zealand Bill of Rights Act 1990, s 19.
[13] International Covenant on Civil and Political Rights, art 17. The New Zealand Bill of Rights Act does not expressly recognise a right to privacy. However, the right to be secure against unreasonable search and seizure (s 21) has been interpreted by the Supreme Court as providing protection against unreasonable state intrusion on an individual's reasonable expectation of privacy (see *Hamed v R* [2012] 2 NZLR 305).
[14] *Ten areas of best practices in countering terrorism* at [12]; Human Rights Commission *Briefing paper relating to human rights and the targeted review of foreign terrorist fighters* (14 November 2014) at [1.2].
[15] New Zealand Bill of Rights Act 1990, s 5.

1.8 To use the words of the New Zealand Human Rights Commission:[16]

> Central to a human rights approach is the need to balance the rights of everyone, favouring the most vulnerable where there is a conflict of rights – for example, the right to personal security of victims (Article 6 ICCPR) may take precedence over the right to privacy or freedom of assembly of those who espouse violence as a means to an end.

1.9 There is a wide range of views on the extent to which some intrusion on individuals' privacy, in particular, can be justified in the interests of security. Democratic countries generally have some restrictions on the activities of their intelligence and security agencies designed to protect their citizens, permanent residents and/or people inside their borders from undue intrusion. However, the level of protection and who it applies to varies.

1.10 The different approaches taken to protecting citizens and residents in part reflect the different values held by each country's population. The United Kingdom's legislation, for example, currently takes a less restrictive approach to surveillance of citizens and residents than many other countries.[17] Consistent with this approach, recent surveys indicate that the UK public is relatively more concerned about national security and less concerned about privacy. In a 2014 poll, 71 percent of respondents prioritised reducing the threat posed by terrorists and serious criminals, even if it eroded people's right to privacy.[18] In the same survey, 64 percent of respondents supported the British intelligence and security agencies monitoring the communications of the public at large for national security purposes.[19]

1.11 In New Zealand, there has been considerable debate in the media about whether the GCSB conducts "mass surveillance" of New Zealanders. Having spent some months learning about the Agencies' operations in detail, we have concluded that this is not the case, for reasons we discuss below.[20] However, there is a degree of scepticism among the New Zealand public about the Agencies' activities. In a survey carried out by the Privacy Commissioner in 2014,

---

[16] Human Rights Commission *Briefing paper relating to human rights and the targeted review of foreign terrorist fighters* (14 November 2014) at [1.4].

[17] Regulation of Investigatory Powers Act 2000 (UK), s 5. Any of the UK intelligence agencies can obtain warrants from the Secretary of State to target persons or premises inside the UK on national security or serious crime grounds. UK citizens and permanent residents overseas can also be targeted on those grounds or for foreign intelligence purposes. By contrast, in the USA a court order is required to target US citizens or permanent residents (50 USC §§1804, 1805, 1842, 1861, 1881b and 1881c); in Canada the signals intelligence agency, the Communications Security Establishment, is prohibited from directing its foreign intelligence or information security activities at Canadian citizens or permanent residents anywhere and any person in Canada (National Defence Act 1985, s 273.64 and s 273.61 (definition of "Canadian")); and in New Zealand the GCSB is prohibited from intercepting the private communications of New Zealand citizens or permanent residents for intelligence purposes (GCSB Act, s 14).

[18] TNS *The Public Opinion Monitor: Surveillance Special* (UK, January 2014), accessed at <http://www.tnsglobal.com/sites/default/files/whitepaper/TNSUK_POM_2014Feb03.pdf>.

[19] In an earlier poll by YouGov in 2013, 43 percent of respondents thought UK intelligence services should in some circumstances be allowed to hack into the calls, emails or text messages of UK citizens with "no questions asked": YouGov *Public Opinion and the Intelligence Services* (UK, October 2013), accessed at <https://yougov.co.uk/news/2013/10/11/british-attitudes-intelligence-services/>.

[20] See paragraphs 3.34–3.41 below.

52 percent of respondents were concerned about surveillance by New Zealand government agencies.[21] We received a number of submissions from people who did not see the need for intelligence and security agencies at all and considered there was no justification for the government intruding on individuals' privacy.[22]

1.12 These concerns may in part reflect a general lack of awareness among the public and openness by the Agencies about what they do, why we need them and the nature of the threats faced by New Zealand. In a Security Issues Poll of 1,000 randomly selected adults in October 2014, only nine percent of people could name both of New Zealand's two intelligence and security agencies.[23] 48 percent of respondents believed New Zealand faced no risk or minimal risk from security threats such as terrorism, cyber attacks and espionage.

1.13 In this sense, the relative secrecy of the Agencies to date has not helped their cause. Although both agencies have acknowledged the need for greater transparency, we consider they should do more to inform the public about the nature of the risks we face and their role in addressing them. Unlike many other countries, including our closest neighbour, New Zealand has not recently experienced terrorist attacks or serious, publicly-disclosed security threats. However, that does not mean threats do not exist or may not arise in the future. The Agencies need to be more open about their work and the reasons for their activities if they want the public to understand how they contribute to the national interest.

1.14 The legislation has a part to play as well. Currently, the two Acts governing the Agencies' activities do not provide a clear picture of what the Agencies do. We consider that creating a single Act that clearly sets out the Agencies' functions and powers and the oversight they are subject to should go a long way toward giving the public a better understanding of their purpose and activities.

1.15 It is also important to recognise that attitudes toward privacy and security are not static. They change over time depending on a range of factors, including global events. There are some indications that New Zealanders are becoming more aware of security threats. In a Horizon Research poll in December 2015, respondents were asked to indicate how they perceived the likelihood of a terrorist attack in New Zealand on a scale of 1–10.[24] The average rating was 5.1 (neither likely nor unlikely). This may signal a small shift from the October 2014 poll

[21] Privacy Commissioner *Individual privacy & personal information: UMR Omnibus Results* (March 2014), accessed at <https://www.privacy.org.nz/news-and-publications/surveys/privacy-survey-2014/>.
[22] Although we note this appears to be the view of a relatively small minority: in an October 2014 poll only seven percent of respondents thought the GCSB was bad for New Zealand and only five percent thought the NZSIS was bad for New Zealand (versus 68 percent and 76 percent who thought the GCSB and NZSIS respectively were good or very good for New Zealand). See Curia Market Research *Security Issues Poll* (Department of Prime Minister and Cabinet, October 2014), accessed at <http://www.curia.co.nz/2015/07/security-issues-poll/>.
[23] Curia Market Research *Security Issues Poll* (Department of Prime Minister and Cabinet, October 2014), accessed at <http://www.curia.co.nz/2015/07/security-issues-poll/>.
[24] Horizon Poll "Terrorist attack: 14% of adults fear personal, family harm" (19 January 2016), accessed at <https://www.horizonpoll.co.nz/page/427/terrorist-at>.

referred to above, where around half of the respondents thought security threats posed no or minimal risk to New Zealand.

Our review

Objectives

1.16 We see this review as an opportunity to raise public awareness about what the Agencies do and to recommend a comprehensive overhaul of the existing legislation, much of which is inconsistent or outdated. Our aim has been to design a legal framework and oversight regime that will give members of the public confidence that the Agencies will act lawfully and appropriately, or will be held accountable if they do not.

1.17 Currently, the legislation governing the Agencies is inadequate in a number of respects. First, important aspects of the law are unclear to both members of the public and the Agencies themselves. This creates barriers to the Agencies carrying out their functions effectively and causes misperceptions about the nature of their activities. Second, the Agencies have separate governing Acts that are creatures of history and incremental reform. This has created inconsistencies and hampers their ability to work together effectively. Finally, the legislation is outdated and is not comprehensive. This inhibits the Agencies in adapting to change and means they must navigate complex legislative provisions to carry out their activities.

1.18 We also see the review as an opportunity to ensure that the Agencies' governing legislation allows them to operate effectively now and in the future. They have an important role to play in contributing to the protection of New Zealand's status as a free, open and democratic society.

1.19 As we explain in more detail below, the threat environment is constantly evolving, often rapidly. This has occurred even during the course of our review. There is a tendency to think that New Zealand, because of its distance from the rest of the world, is immune from serious threats to our security and well-being. Unfortunately that is not the case. In an increasingly globalised world, where the Internet is used as a tool for espionage, terrorism and harm to critical infrastructure, New Zealand is potentially as much at risk as any other country. Moreover, New Zealanders may find themselves at risk in other parts of the world. The law needs to be framed in a way that allows the government to respond to threats as they evolve in order to fulfil its obligation to protect New Zealanders' right to security, while also recognising and maintaining individuals' rights and freedoms.

Approach

1.20 In conducting our review, we gathered information from a broad range of sources. Our goal was to understand the full spectrum of perspectives before coming to a view about what the future legal framework should look like.

1.21 We called for public submissions and received responses from 100 individuals and organisations. The submissions canvassed a wide range of views from security and human rights experts, members of the public, and organisations in the public, private and not-for-profit sectors. We also met with academics, lawyers, telecommunications providers and representatives from the intelligence communities of Australia, the UK, Canada and the United States of America to gain a better understanding of the issues as they see them. A list of individuals and organisations we met with is set out in Annex B.

1.22 We were allowed access at the highest level of security clearance to the Agencies' premises, their staff and information about their activities. We spent a significant amount of time seeking to understand the Agencies' activities, the reasons for them, the processes they have in place to protect against misuse and how oversight of the Agencies works in practice. We also spoke to the ultimate users of the intelligence collected by the Agencies – primarily other government agencies and ministers – to understand its value.

1.23 We are grateful to all those who took part in the public submission process and who met with us throughout the course of the review. The submissions and discussions helped us identify areas for improvement and develop and refine our recommendations. We were particularly impressed with the willingness of the people we met with to speak freely and frankly with us about what were often sensitive issues.

1.24 We have been fortunate to have the support of a small secretariat from the Policy Group in the Ministry of Justice, who have assisted us at all stages of our review. We thank them for their assiduous attention to the issues we raised. Their work has been invaluable, particularly in enabling us to produce a single report that can be presented to Parliament and made available to the public without the need for redactions.

1.25 During the course of our review, we also considered the legislative frameworks and oversight arrangements for intelligence agencies in other countries. While our recommendations are tailored to the New Zealand context, many of the issues we face here are relevant in other countries as well. The approaches they have taken provided useful comparisons for us. We have not set out a detailed comparison of the security and intelligence frameworks in other jurisdictions in this report, as other recent reports have already done so.[25] However, we do provide specific comparisons where relevant.

[25] In particular, see David Anderson QC *A Question of Trust: Report of the investigatory powers review* (UK, June 2015) at [8.38]–[8.64] and Annex 15 ("The Law of the Five Eyes").

1.26 We have focused on designing the foundations for a clear and robust legal framework for the Agencies. We have not addressed every issue that was raised with us, as some were outside the scope of our terms of reference or were matters of minor legislative amendment that are more appropriately considered as part of the government response to our report. Where we have not commented on an existing provision in the legislation or addressed an issue that was raised with us, that should not be taken to indicate any position on it.

1.27 In particular, we have not considered the Telecommunications (Interception Capability and Security) Act 2013 ("TICSA") or related issues of mandatory data retention by telecommunications providers. Although TICSA does impose some statutory obligations on the GCSB, it is not part of the core legislation governing the Agencies.

1.28 We also have not specifically addressed the use of classified information in court and administrative proceedings, which has been reviewed separately by the Law Commission.[26] However, we took the Law Commission's work into account in carrying out our review and note that it may assist the government to address some of the issues that were raised with us. For example, the Commission recommended that a closed proceeding using a special advocate be available where a defendant wishes to challenge the grounds for a search and surveillance warrant.[27] This may go some way toward addressing the Agencies' concerns that sharing sensitive information with New Zealand Police ("Police") will lead to it being disclosed in court.

1.29 The Commission's report is broadly consistent with our recommendations, although it focuses on different areas. We note the Commission has recommended expanding the role of the Inspector-General of Intelligence and Security ("Inspector-General") to include considering any information provided by the Agencies to persons making administrative decisions affecting an individual's rights.[28] We support this move toward greater oversight of administrative decisions. In Chapter 8 we recommend that all decisions to cancel a person's travel document on national security grounds be reviewed by a judicial commissioner as a matter of course.

Common themes

1.30 We identified some common areas of concern through the public submission process and the meetings we had during our review, despite the broad range of perspectives and sometimes deeply opposed views people held about the Agencies. These common concerns included the need for:

- increased transparency, accountability and oversight

[26] Law Commission *The Crown in Court: A review of the Crown Proceedings Act and national security information in proceedings* (NZLC R135, December 2015).
[27] *The Crown in Court: A review of the Crown Proceedings Act and national security information in proceedings*, recommendation 25.
[28] *The Crown in Court: A review of the Crown Proceedings Act and national security information in proceedings*, recommendation 21.

- greater clarity in the legislation about what the Agencies can and cannot do, and
- a strong emphasis on protecting individual rights and freedoms.

1.31 These general themes have been the cornerstone of our review. Our recommendations are aimed at achieving a clearer, more comprehensive legislative framework with strong safeguards and oversight in place for all of the Agencies' intelligence and security activities. We hope this will provide the public with greater assurance that the Agencies will act in New Zealand's best interests and will be held accountable for the way in which they perform their functions.

1.32 Many members of the public who made submissions to us believed that the level of risk to New Zealand from security threats such as terrorism is very low. They therefore did not consider intrusions on individuals' privacy by the state, for example through the interception of communications and metadata, to be justified.

1.33 The information we had access to during the course of our review suggests New Zealand does face a range of threats, many of which are not disclosed to the public for a variety of reasons. While much of what we learned is classified and cannot be published in this report, we have used examples wherever possible to explain the reasons for our conclusions. Many of these examples are hypothetical, but are roughly based on actual situations that have occurred in New Zealand or overseas. We also strongly encourage the Agencies to be more open with the public about the nature of security risks, as overseas intelligence and security agencies are increasingly doing.

How did the review come about?

1.34 The Intelligence and Security Committee Act 1996 and the Inspector-General of Intelligence and Security Act 1996 were amended in 2013 to provide greater and more effective oversight of the Agencies. Among other changes, the amendments required new regular reviews of the Agencies, the legislation governing them, and their oversight legislation. Our review, which is the first, had to commence by 30 June 2015. Subsequent reviews must be held every five to seven years.

1.35 The amendments introducing the requirement for regular reviews occurred alongside significant changes to the Government Communications Security Bureau Act 2003. Those changes were prompted[29] by Rebecca Kitteridge's 2013 review into compliance mechanisms at the GCSB after it came to light that the GCSB had unlawfully intercepted the communications of Mr Kim Dotcom on the basis of a misunderstanding about his residence status.

[29] Government Communications Security Bureau and Related Legislation Bill (109–1) (explanatory note) at 2.

1.36 Ms Kitteridge published her report in early 2013, which identified systemic problems with the GCSB's compliance systems and serious deficiencies in the GCSB Act.[30] Ms Kitteridge recommended reform of the GCSB Act so that the GCSB could carry out its work with a clear understanding of the law. Ms Kitteridge also identified 88 instances where the GCSB had provided assistance to the NZSIS and Police. At the time, the GCSB Act was unclear as to whether GCSB could assist other domestic agencies in this way.

1.37 The Prime Minister asked the Inspector-General to inquire into the 88 assistance cases identified by Ms Kitteridge. The Inspector-General found that in 84 cases where telephone metadata[31] (not the content of communications) was involved, "no-one appeared to have suffered any personal detriment from the Bureau's activities".[32] The Inspector-General also recommended that the GCSB Act be redrafted to provide "precise directions" on what the GCSB can and cannot do.[33]

1.38 In response to Ms Kitteridge's report, the GCSB commenced a comprehensive change programme. As at 30 September 2014, the GCSB reported that it had implemented all of the recommendations in the report.[34]

Global context

The Snowden leaks

1.39 In 2013, during the time that the GCSB Act was being amended, The Guardian newspaper in the UK published a series of articles leaking apparently classified information about the USA's surveillance programme that had been stolen by Edward Snowden.[35] The leaked documents also revealed that New Zealand along with Australia, Canada, the UK and the USA, were members of a global intelligence-sharing alliance known as the "Five Eyes". It was alleged the Five Eyes countries all contributed to the USA' intelligence collection on a large scale.

1.40 Edward Snowden's leaks brought the powers and activities of intelligence and security agencies out of the shadows and into the public arena. Governments, including ours, were prompted to address questions of surveillance, privacy, accountability and proportionality. In the UK there have been multiple inquiries into and reviews of the intelligence and security

[30] Rebecca Kitteridge *Review of Compliance at the Government Communications Security Bureau* (March 2013).
[31] See paragraph 3.16 below for a description of metadata.
[32] Inspector-General of Intelligence and Security *Annual report of the Inspector-General – 2013* (June 2013) at 5.
[33] Inspector-General of Intelligence and Security *Annual report of the Inspector-General – 2013* (June 2013) at 5.
[34] Government Communications Security Bureau *Compliance Review – Final Report* (for the period ending 30 September 2014).
[35] Al Jazeera America provides a helpful timeline of the leaks from June 2013 to September 2014. See Al Jazeera America "Timeline of Edward Snowden's revelations", accessed at <http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html>.

agencies resulting from the Snowden leaks. The Investigatory Powers Tribunal,[36] Interception of Communications Commissioner's Office,[37] the Intelligence and Security Committee of Parliament,[38] the Independent Reviewer of Terrorism Legislation (David Anderson QC)[39] and the Royal United Services Institute[40] have all examined privacy concerns relating to the intelligence and security agencies' activities to varying degrees.

1.41 In the USA, soon after the leaks, President Barack Obama ordered an independent review of the USA' surveillance capabilities and how they impact security, privacy and foreign policy.[41] In 2015 Congress passed the USA FREEDOM Act that imposed some new limits on the activities of the USA intelligence and security agencies. The European Parliament launched an in-depth inquiry into surveillance by the USA and some European Union member states and its impact on European Union citizens' rights.[42]

1.42 The leaks also challenged the trust we often place in communications providers to keep our private information secure, especially the Internet giants. The Snowden documents indicated that the USA National Security Agency was intercepting traffic inside the private networks of Google and Yahoo, and that companies like Facebook assisted with the National Security Agency's PRISM data-collection programme.[43]

1.43 Post-Snowden, the demand for encrypted communications applications is increasing. Facebook is even offering a system of alerting users when their accounts have been targeted

[36] *Liberty & Ors v the Security Service & Ors* [2014] UKIPTrib 13_77-H; *Caroline Lucas MP & Ors v the Security Service & Ors* [2015] UKIPTrib 14_79-CH.
[37] Interception of Communications Commissioner *IOCCO Annual Report for 2013* (8 April 2014).
[38] Intelligence and Security Committee of Parliament *Privacy and Security: A Modern and Transparent Legal Framework* (UK, March 2015).
[39] David Anderson QC *A Question of Trust: Report of the investigatory powers review* (UK, June 2015).
[40] Royal United Services Institute *A Democratic Licence to Operate: Report of the independent surveillance review* (UK, July 2015).
[41] The White House Office of the Press Secretary "Remarks by the President in a Press Conference" (9 August 2013), accessed at <https://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference>.
[42] European Parliament *Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs* (21 February 2014), accessed at <https://polcms.secure.europarl.europa.eu/cmsdata/upload/73108fba-bb11-4a0b-83b8-54cc99c683b5/att_20140306ATT80632-1522917198300865812.pdf>.
[43] Barton Gellman, Ashkan Soltani and Andrea Peterson "How we know the NSA had access to internal Google and Yahoo cloud data" (The Washington Post, 4 November 2013), accessed at <https://www.washingtonpost.com/news/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/>; Alexis Kleinman "NSA: Tech companies knew about PRISM the whole time" (The Huffington Post, 20 March 2014), accessed at <http://www.huffingtonpost.com/2014/03/20/nsa-prism-tech-companies_n_4999378.html>.

by a "state-sponsored actor".[44] A number of international customers, including governments, are also reported to be reappraising their reliance on major USA technology companies.[45]

1.44 In relation to New Zealand, the leaks were the basis for claims that the GCSB conducted "full-take" collection on Pacific Island states and trading partners, that New Zealand spied on some countries for economic advantage and that the GCSB used its capabilities to help the New Zealand Minister of Trade's unsuccessful bid to become the next Director-General of the World Trade Organisation.[46] This led to questions from many New Zealanders about the GCSB's activities, particularly in light of the events that gave rise to the Kitteridge Report. These questions included whether New Zealanders are in fact immune from being spied on by the GCSB and its Five Eyes partners, or whether the Five Eyes intelligence-sharing arrangement is being used as a work-around to allow the GCSB direct access to New Zealanders' communications.

1.45 The accuracy of Snowden's allegations in relation to New Zealand and the propriety of the GCSB's activities to date are not the subject of our review. However, they raised some significant public concern about what the Agencies are here for, what they should be allowed to do and what they should be prohibited from doing. These are questions we have sought to address.

The changing nature of threats in a new digital environment

1.46 The reports of David Anderson QC and the Royal United Services Institute in the UK both articulate in considerable detail how technological change is challenging the intelligence and security agencies' ability to identify and analyse current and future threats to our security.

1.47 Up until the Cold War, intelligence collection, for the most part, took place in separate communications networks from those used by the general public. This is because the communications of countries that posed a national security threat, such as the Soviet Union and its allies, were kept largely separate from other countries.[47] Direct communications between the general public and Communist nations were also a tiny fraction of all electronic

[44] Michael Pizzi "Facebook warns users of 'state sponsored' hacking" (Al Jazeera America, 21 October 2015), accessed at <http://america.aljazeera.com/articles/2015/10/21/facebook-warns-users-of-state-sponsored-hacking.html>.
[45] Claire Cain Miller "Revelations of NSA spying cost US Tech companies" (The New York Times, 21 March 2014), accessed at <http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html?_r=0>.
[46] Aimee Gulliver "Snowden documents: NZ spied on Pacific Island neighbours" (Stuff, 5 March 2015), accessed at <http://www.stuff.co.nz/national/politics/66970595/snowden-documents-nz-spied-on-pacific-island-neighbours>; Nicky Hager & Ryan Gallagher "Snowden revelations: NZ's spy reach stretches across globe" (New Zealand Herald, 11 March 2015), accessed at <http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11415172>; David Fisher "GCSB spies monitored diplomats in line for World Trade Organisation job" (New Zealand Herald, 23 March 2015), accessed at <http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11421371>.
[47] The President's Review Group on Intelligence and Communications Technologies *Liberty and Security in a Changing World* (USA, December 2013) at 180–183.

communications, as international phone calls were expensive and rare.[48] But the Internet is changing the way and the frequency with which we communicate across borders, blurring the distinction between domestic and foreign communications on which intelligence and security agencies have been built.

1.48 Voice over Internet Protocol applications such as Skype and Apple's FaceTime are replacing landline and mobile telephone calls. People are increasingly using social media platforms, chat forums, drop boxes and other messaging "apps" to communicate and can also virtually "meet" inside multiplayer role games. The way in which these communications travel over the Internet does not respect national boundaries. A single communication over the Internet is automatically split into separate "packets" (units of data) that are sent via different paths, sometimes across multiple countries, depending on which is the least congested or cheapest. For example, an email between two people in New Zealand may be routed via the USA. When these packets arrive at their destination, they are automatically reassembled into the original communication. If the communication is intercepted in transit, law enforcement and intelligence and security agencies may only be able to recover some parts of a message, making effective interception more complex.

1.49 The Internet also offers ways to anonymise communications. The "dark web", only accessible through sophisticated software, is not only used by whistleblowers and political activists, but also by illegal drug smugglers and people who produce and distribute child sexual abuse images.[49] Encryption, although not new, is on the rise. It is the process of converting information such as a text or email message into an encoded format that can only be decrypted and read by someone with access to a secret key.[50] This trend in increased encryption pre-dates Snowden's leaks and was particularly affected by the targeted attack on celebrity iCloud accounts in 2014.[51] Apple iPhones are now encrypted by default and not even Apple can unlock a user's encrypted phone.[52]

1.50 While increased encryption enhances the cyber security of the general public, both "data in transit" and "stored data" can now be difficult for law enforcement and intelligence and security agencies to access or intercept, even when they are authorised to do so by a warrant.

---

[48] The President's Review Group on Intelligence and Communications Technologies *Liberty and Security in a Changing World* (USA, December 2013) at 182.

[49] The "dark web" is a collection of websites that use anonymity software to hide the location of the servers that host them. Those who wish to access these websites must use similar anonymity software. These websites are commonly associated with the sale of illicit drugs, weapons, child pornography and counterfeit documents.
Andy Greenberg "Hacker lexicon: What is the dark web?" (Wired, 19 November 2014), accessed at <http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/>.

[50] For a simple explanation of encryption techniques see David Anderson QC *A Question of Trust: Report of the investigatory powers review* (UK, June 2015) at [4.44] to [4.46].

[51] Steve Kovach "We still don't have assurance from Apple that iCloud is safe" (Business Insider, 2 September 2014), accessed at <http://www.businessinsider.com/apple-statement-on-icloud-hack-2014-9>.

[52] Zack Whittaker "Apple doubles-down on security, shuts out law enforcement from accessing iPhones, iPads" (ZDNet, 18 September 2014), accessed at <http://www.zdnet.com/article/apple-doubles-down-on-security-shuts-out-law-enforcement-from-accessing-iphones-ipads/>.

Data volumes are rising exponentially

1.51 The volume of data we generate is already phenomenal. In 2014, the world created 4.4 zettabytes of data, enough to store all human speech ever spoken.[53] Every day we send 294 billion emails, perform over 1 billion Google searches and send over 230 million Tweets.[54] In June 2015 alone, New Zealanders used over 84,000 terabytes of broadband data.[55] And our appetite for data is only increasing. In New Zealand, one-third of all broadband internet connections (628,000) had no data cap in 2015, compared to just 155,000 in 2014.[56]

1.52 This volume of data is set to explode in the next few years with the advent of the "Internet of Things", where everyday consumables will be connected to the Internet to "speak" to each other automatically. It is not inconceivable that, in the not-too-distant future, cars could automatically provide their drivers with the best route to work meetings based on information in their calendars and inform relevant parties if they are running late.[57]

1.53 How data moves around the world has also changed in the past 40 years. New fibre-optic networks are able to send larger volumes of data over a longer distance. Google Fibre, launched in 2012 in some cities in the USA, involves data moving at about two-thirds the speed of light.[58]

1.54 Law enforcement and intelligence and security agencies are struggling to deal with this volume of data. It is becoming increasingly difficult to target the specific signal or communication that is relevant to a lawful investigation in a sea of noise.

The modern threat landscape

1.55 Developments in technology offer both opportunities and challenges for intelligence agencies. On the one hand, the quantity of potentially useful information available has increased exponentially. On the other, encryption has made it difficult to intercept the communications of sophisticated actors who wish to cover their tracks. Cyber capabilities are also increasingly

[53] Fergal Toomey "Data, the speed of light and you" (Tech Crunch, 9 November 2014), accessed at <http://techcrunch.com/2015/11/08/data-the-speed-of-light-and-you/>. A zettabyte is approximately 1 billion terabytes.
[54] IBM "Big Data & Analytics Hub", accessed at <http://www.ibmbigdatahub.com/gallery/quick-facts-and-stats-big-data>.
[55] Statistics New Zealand "Internet Service Provider Survey: 2015" (14 October 2015), accessed at <http://www.stats.govt.nz/browse_for_stats/industry_sectors/information_technology_and_communications/ISPSurvey_HOTP2015/Related%20Links.aspx>.
[56] Statistics New Zealand "Internet Service Provider Survey: 2015" (14 October 2015), accessed at <http://www.stats.govt.nz/browse_for_stats/industry_sectors/information_technology_and_communications/ISPSurvey_HOTP2015/Related%20Links.aspx>.
[57] Bonnie Cha "A Beginner's Guide to Understanding the Internet of Things" (Re/code, 15 January 2015), accessed at <http://recode.net/2015/01/15/a-beginners-guide-to-understanding-the-internet-of-things/>.
[58] Fergal Toomey "Data, the speed of light and you" (Tech Crunch, 9 November 2014), accessed at <http://techcrunch.com/2015/11/08/data-the-speed-of-light-and-you/>.

being used by state and non-state actors alike as a means of attack or to steal information of importance to individuals, businesses and governments.

1.56 The growth of technology as a vehicle for security threats is particularly significant for New Zealand. In the past, it was easy to rely on our distance from the rest of the world as our best defence. Now, our physical isolation is becoming less and less relevant.

1.57 Although New Zealand is physically removed from the turmoil in the Middle East, home-grown terrorism is a real possibility. New Zealand is not immune from the growth of a new type of violent extremism that uses the Internet to spread ideology and recruit supporters. The Islamic State of Iraq and the Levant (ISIL) has used this form of communication to spread its message very effectively on a global scale and a number of New Zealanders are already known to be fighting with or otherwise supporting ISIL.[59] There is also a risk that New Zealanders radicalised by ISIL here or returning from Syria or Iraq will be inspired to carry out attacks on home soil, as has occurred in other Western countries.[60]

1.58 While our intelligence and security agencies are now working on new areas of concern such as terrorist groups and criminal organisations, there has also been a resurgence in state-based threats. Intense inter-state strategic competition is giving rise to regional instability, which could impact directly on New Zealand's national interests and require a response from New Zealand in one form or another. Foreign state espionage is still a real threat to New Zealand but the form it takes and what it targets has changed. While Cold War espionage was focused on uncovering the military and weapons capabilities of other states, espionage against New Zealand today includes attempts to influence government policy and target certain sectors of the economy to steal intellectual property. To do this, states are supplementing their traditional arsenal of human-based operations with cyber capabilities, which allow them to engage in espionage remotely.

Cyber threats

1.59 The volume of business conducted online and the amount of personal information users readily share presents a range of opportunities to potential attackers. Terrorist organisations, foreign governments and even ordinary criminals can target the New Zealand government, New Zealand companies and New Zealanders from around the globe using cyber capabilities.

1.60 Cyber tools are low cost and carry relatively little risk, as attributing activity to a specific foreign organisation or group is often a very difficult process. New Zealand's world-leading skills in niche areas such as biotechnology and agribusiness could be the target of foreign states or organisations that want to sidestep years of research and development that would

[59] New Zealand Security Intelligence Service *Annual Report for the year ended 30 June 2015* at 10; Director of Security *Opening remarks to the Intelligence and Security Committee* (8 December 2015).
[60] For example, the Sydney Lindt Café siege in December 2014, the Charlie Hebdo shootings in January 2015, the Paris attacks in November 2015 and the San Bernardino mass shooting in December 2015 were all apparently carried out by groups or individuals who were motivated by ISIL propaganda.

allow them to be equally competitive. Theft of intellectual property and economic information in this way can cost the New Zealand economy in the form of lost revenue and increased spending on protection mechanisms.

1.61 The nature of cyber threats has evolved over the past decade from cyber crime to espionage, sabotage and even cyber warfare. Most attacks are designed to steal information such as intellectual property and trade secrets, and to disrupt businesses. Attackers realise that people are often the weakest link in an organisation's defences. They exploit this weakness through both targeted and untargeted attacks.

1.62 Untargeted attacks include, for example, sending emails to a large number of people encouraging them to respond with sensitive information such as credit card details or internet banking log-in details. A targeted attack could involve, for example, compromising a legitimate website frequented by staff in a particular business sector so that the visitors' browsers automatically download malware that allows the attacker direct access to the device. Typically, these devices are connected to a wider organisational network and the attacker will use this device as a "staging area" to attack the victim organisation's wider network and secure a foothold. They will look for valuable information to steal or critical points of failure to exploit.[61]

1.63 Attackers can range from cyber criminals to well-resourced state actors, "hackers for hire" and "hacktivists". One of the most crippling and lesser-known attacks by a "hacktivist" group happened in 2012. A group calling itself the "Cutting Sword of Justice" infiltrated the networks of Saudi Arabia's state oil company, Saudi Aramco, which supplies 10 percent of the world's oil. The company had most of its computer systems and critical files destroyed by the virus. The entire business operation was forced offline and employees moved to using typewriters and faxes. It took Saudi Aramco five months to bring its newly secured computer network back online.[62]

1.64 In December 2015, it was reported that cyber attackers launched a multi-pronged attack on electricity suppliers in some regions of Ukraine. The attacks cut electricity to over 80,000 customers and flooded the companies' help lines to prevent legitimate callers from getting through.[63] As recently as February 2016, the Hollywood Presbyterian Medical Centre was the subject of a "ransomware" attack by cyber criminals. It was reported the hackers demanded

[61] See UK Parliamentary Office of Science & Technology *Cyber Security in the UK* (September 2011), accessed at <http://www.parliament.uk/documents/post/postpn389_cyber-security-in-the-UK.pdf>.
[62] Jose Pagliery "The inside story of the biggest hack in history" (CNN, 5 August 2015), accessed at <http://money.cnn.com/2015/08/05/technology/aramco-hack/>.
[63] Kim Zetter "Everything we know about Ukraine's power plan hack" (Wired, 20 January 2016), accessed at <http://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/>.

over US$3.6 million to unlock patient files. As a result, computer networks essential for CT scans, documentation, laboratory work and pharmacy needs had to be taken offline.[64]

1.65 Businesses may also find themselves the target of foreign governments and business rivals in a campaign of industrial espionage. The Chinese military is widely believed to conduct extensive cyber espionage against commercial targets to obtain intellectual property for commercial advantage.[65] "Hidden Lynx" is an alleged China-based professional organisation of between 50 and 100 people that can be hired to run cyber espionage operations. Symantec Corp has claimed that Hidden Lynx might have been involved in attacks on Google, Adobe Systems and other companies in 2009 to access and change source code.[66]

1.66 Cyber threats are becoming more sophisticated and it is becoming increasingly difficult to differentiate between state and criminal actors. While New Zealand is yet to suffer a serious attack affecting public confidence, we are seeing attacks overseas that are more high-profile and more destructive. These include the attack on Sony Pictures and subsequent leak of sensitive personnel information and unreleased versions of films, the breach of the USA Department of Personnel Management's servers with fingerprints of 5.6 million individuals stolen, and the attack on the German Parliament's computer systems.[67]

1.67 The government estimates that more than 80 percent of New Zealanders have experienced a cyber security breach (such as having your email hacked) and that 56 percent of businesses have been attacked at least once a year.[68] It has been reported that Spark's network operations centre in Auckland, for example, is the target of about 3,800 cyber attacks a day.[69]

1.68 In September 2014, Spark's network was apparently disrupted for about 36 hours because foreign cyber criminals staged a Distributed Denial of Service (DDOS) attack on websites in

---

[64] Steve Ragan "Ransomware takes Hollywood hospital offline, $3.6m demanded by attackers" (CSO Online, 14 February 2016), accessed at <http://www.csoonline.com/article/3033160/security/ransomware-takes-hollywood-hospital-offline-36m-demanded-by-attackers.html>.

[65] James R Clapper, Director of National Intelligence *Statement for the Record to the Senate Armed Services Committee: Worldwide Threat Assessment of the US Intelligence Community* (26 February 2015); Larry M Wortzel *The Chinese People's Liberation Army and Information Warfare* (US Army War College Press and Strategic Studies Institute, March 2014) at 24.

[66] Jim Finkle "Hacker group in China linked to big cyber attacks: Symantec" (Reuters, 17 September 2013), accessed at <http://www.reuters.com/article/us-cyberattacks-china-idUSBRE98G0M720130917>.

[67] BBC News "The Interview: A guide to the cyber attack on Hollywood" (29 December 2014), accessed at <http://www.bbc.com/news/entertainment-arts-30512032>; Andy Greenberg "OPM now admits 5.6m Feds' fingerprints were stolen by hackers" (Wired, 23 September 2015), accessed at <http://www.wired.com/2015/09/opm-now-admits-5-6m-feds-fingerprints-stolen-hackers/>; Anton Troianovski "German parliament struggles to purge hackers from computer network" (The Wall Street Journal, 12 June 2015), accessed at <http://www.wsj.com/articles/german-parliament-struggles-to-purge-hackers-from-computer-network-1434127532>.

[68] New Zealand Government "New Zealand's Cyber Security Strategy" (December 2015), accessed at <https://www.dpmc.govt.nz/dpmc/publications/nzcss> at 3.

[69] Juliet Speedy "Cyber attacks biggest threat to NZ businesses" (3 News, 21 June 2015), accessed at <http://www.3news.co.nz/nznews/cyber-attacks-biggest-threat-to-nz-businesses-2015062116#axzz3xqpdWrBk>.

Eastern Europe using Spark's customer connections as a launching pad.[70] A DDOS attack makes an online service unavailable by flooding it with traffic from multiple sources.[71]

1.69 We expect that other large commercial organisations in New Zealand experience similar levels of attempted cyber attacks on a daily basis. In particular, we expect companies offering financial services and organisations holding significant amounts of personal information are targeted by organised cyber criminals.

1.70 The GCSB is one of a number of organisations involved in improving New Zealand's cyber security, particularly through its CORTEX project. CORTEX offers organisations of national significance, including some government departments and operators of critical national infrastructure, protection against sophisticated malicious software or "malware".[72] Each month, the GCSB and its international cyber security partners identify around 900 new fingerprints associated with some form of cyber threat. They use these fingerprints to try and identify the source of the threat and to help organisations avoid the threat.[73]

1.71 There is no requirement to report cyber security incidents in New Zealand. In fact, victims often do not report harm because they are embarrassed or, in the case of businesses, are unaware that their systems have been compromised or are afraid it could undermine customer confidence in their business. The information we do have on the number and cost of cyber security incidents are almost certainly just the tip of the iceberg. This suggests that both government and private sector organisations may need to increase their focus on achieving more consistent and public reporting on cyber security incidents.

[70] Nicky Ryan "Nude celebrity photos might not be to blame for New Zealand internet crash" (Business ETC, 8 September 2014), accessed at <http://businessetc.thejournal.ie/spark-hack-internet-photos-cyber-attack-1660366-Sep2014/>.
[71] For more information on DDOS attacks worldwide visit <www.digitalattackmap.com>.
[72] Government Communications Security Bureau "CORTEX Frequently Asked Questions" (7 December 2015), accessed at <http://www.gcsb.govt.nz/our-work/information-assurance/cortex-faqs/>.
[73] Una Jagose "Speaking Notes: Speech to the Technology and Privacy Forum" (29 September 2015), accessed at <http://www.gcsb.govt.nz/publications/news/speaking-notes-for-speech-to-the-technology-and-privacy-forum-by-una-jagose-acting-director-government-communications-security-bureau/>.

Chapter 2: Intelligence

2.1 In this chapter we explain what intelligence is and how the government uses it. We also explain why intelligence sometimes needs to be collected in secret, and the value of having intelligence and security functions performed by separate collection agencies (as distinct from Police or another public agency).

What is intelligence?

2.2 Intelligence is, in essence, useful information that can help decision-makers achieve desired outcomes. As individuals we usually make the assumption that the more we know, the better informed our decisions will be and the better off we will end up being. Most information we rely on is publicly available. This is referred to as open source information. Much of this information is published in newspapers, books, journals and on the Internet, and some we consciously pick up through interactions with individuals and groups. A great deal of this information may be accurate but some of it can be inaccurate or deliberately intended to mislead us.

2.3 Governments face similar issues when looking for information that will enable them to make good decisions. But unlike most individuals, governments have access to additional information obtained in secret. This includes information that others are seeking to prevent governments from knowing and will go to considerable lengths to ensure it is not acquired. For example, groups that organise and profit from people smuggling ventures across borders often do not use open channels of communication and generally code or encrypt their messages to prevent detection.

2.4 As a starting point, open source information can show what data is still missing and therefore what needs to be obtained through secret methods. Secret information in turn helps to validate, qualify or discount open source information or diplomatic and military reporting. Together with material from open sources, this secret information is evaluated for its accuracy, assessed for relevancy and distributed to government decision-makers as "intelligence".

2.5 Intelligence is used for a range of purposes in New Zealand: from assisting Police to uncover child sexual exploitation networks to supporting the government to detect and monitor illegal fishing activity.

Open source information

2.6 The volume of open source information (sometimes referred to as OSINT), especially in the Internet age, has dwarfed the information available through secret sources. It is estimated

that between 90 and 95 percent of intelligence reports today are comprised of open source information.[74] It is not only governments that use it. The private sector also uses open source information to identify risk and new opportunities to grow. For example, the Economist's Intelligence Unit provides a comprehensive service for businesses that need to understand how industry developments intersect with economic, political and socio-demographic trends.[75]

2.7 A new and growing category of open source information is the information we share in exchange for free digital products such as social media, e-mail and "apps". There are numerous companies interested in what we search for and in what we click, "like" and share online. Our smart phones provide another layer of personal information, acting as mini tracking devices by sharing the locations we visit most often and when. An entire business sector has developed around collecting, analysing and packaging these datasets to sell as a commodity to credit card issuers, retail banks, telecommunications companies and insurers.[76]

2.8 We consider there is scope for the government to make greater use of such open source information. As a general principle, intelligence should be collected using the least intrusive means possible in the circumstances. Where information can be collected through open sources, that should always be the preferred option. Any use of intrusive collection methods must be justified in that context.

The value of intelligence to decision makers

2.9 The role of government is to protect the interests and values of its citizens. This includes providing conditions that enable people to carry out their lawful business and take advantage of opportunities to improve their prosperity and well-being without undue interference with their rights – that is, to maintain a free, open and democratic society. To achieve this, the government needs to protect against threats to those interests and values, including through maintaining laws and institutions. The government's role also extends to taking advantage of opportunities to advance the country's interests internationally and, as a result, increase opportunities for New Zealanders.

2.10 In performing this role, the government relies on having accurate and relevant intelligence on which to base its decisions. Intelligence informs both strategic policy decisions that influence New Zealand's future position in the world and more immediate decisions relating to specific situations. For example, the government needs to be sufficiently informed about other

[74] Loch K. Johnson (ed) *The Oxford Handbook of National Security Intelligence* (Oxford University Press, New York, 2012) at 16.
[75] For more information on the Economist Intelligence Unit see <http://www.eiu.com/home.aspx>.
[76] One data broker allegedly holds, on average, 1,500 pieces of information on over 200 million Americans. This can include everything from age, gender, race, height, weight, marital status to education level, number of children, type of car driven, political affiliations, income and medical history. See 60 Minutes "The Data Brokers: Selling your personal information" (24 August 2014), accessed at <http://www.cbsnews.com/news/data-brokers-selling-personal-information-60-minutes/>.

countries' activities and intentions in order to make decisions on foreign policy. Intelligence can assist the government in deciding how to vote for positions on key international bodies, or to assess how other nations might respond if New Zealand takes a particular stance on an issue of international significance. It is also important to have reliable information about emerging political instability in other countries, so that the government can prepare or respond appropriately. These issues are not only important because they might affect New Zealand's interests; they are also relevant to regional and even global security and well-being.

2.11 Intelligence also helps to inform more immediate decisions, such as decisions about how to prevent a possible terrorist attack or administrative decisions that affect individuals (for example, whether to approve an immigration application where a potential risk to national security has been identified).

2.12 Intelligence can also assist frontline agencies – such as Police in its role of preventing crime and enforcing the law, and the New Zealand Customs Service ("Customs") and Immigration New Zealand ("Immigration") in protecting New Zealand's borders.

Why does some intelligence need to be collected in secret?

2.13 Many government agencies collect information in the course of carrying out their functions, providing services to the public and providing policy advice to the government.

2.14 In most cases, government agencies can collect the information they need openly and transparently, such as by seeking consent. However, there are some aspects of society that are not so open. Activities that threaten New Zealand's national security, such as transnational crime, espionage and terrorism, are often carefully orchestrated in order to avoid the attention of the state. For example, people involved in production and distribution of child sexual abuse images go to great lengths to conceal their online activities.

2.15 The nature of these activities is such that, to be effective in countering them, collection of intelligence to detect them also needs to be done in secret. If perpetrators become aware of what the authorities are doing to discover their activities, they have the opportunity to change the way they do things and avoid detection. Because of this, in many instances countering covert behaviour by people or states by collecting information in secret is unavoidable.

Why do we need special intelligence and security agencies?

2.16 As in most democracies, New Zealand's intelligence and security agencies operate separately from other government agencies and are governed by their own specific legislative regimes.

2.17 Intelligence and security agencies employ their specialist skills to collect and analyse information in accordance with the government's intelligence priorities. They cannot and should not make decisions about how the intelligence they collect should be acted upon – this

is the role of Ministers or agencies with specific decision-making or enforcement functions, such as the Minister of Foreign Affairs or Police, who receive the intelligence.

2.18 We received a number of submissions from individuals and organisations presenting the view that there should be no intelligence and security agencies because intelligence gathering is better carried out by fully accountable government agencies. Many of these submitters were also of the view that individuals should only be investigated if they are suspected of having committed a crime, which is the responsibility of Police.

2.19 To be effective in the modern world, law enforcement and intelligence agencies need to collect a broader range of information than just in relation to specific individuals who may have committed an offence. For example, Police are responsible for crime prevention and need to collect and receive intelligence in order to make informed decisions on where and how to target their activities. Similarly, intelligence agencies have a responsibility to identify potential threats before they become events of security concern.

2.20 While many government agencies collect intelligence in order to carry out their functions, we consider there are significant benefits to having separate secret intelligence collection agencies, for the following reasons:

- separating collection from enforcement acts as a check on decision-making
- intelligence and security agencies are well placed to provide a cross-government perspective, and
- intelligence collection requires specialist skills and capability.

Separating collection from enforcement acts as a check on decision-making

2.21 While government agencies such as the Police, Customs, New Zealand Defence Force ("Defence Force") and Immigration sometimes need to collect information in secret in order to carry out their role effectively, it is for the purpose of exercising their frontline activities, which often have a direct impact on individuals.

2.22 In contrast, intelligence and security agencies exist to collect information in accordance with the government's broader priorities or when tasked by another agency. Intelligence and security agencies do not have enforcement or decision-making powers over individuals. While their activities can sometimes be intrusive, their primary role is to collect information in accordance with the government's priorities. They therefore do not have the same performance incentives as agencies with responsibility for achieving certain outcomes.

2.23 Separating intelligence collection from enforcement ensures that information collected about individuals where there is no evidence of wrongdoing is independently assessed before it is used to make a decision that affects them – for example, by Police before deciding to apply for

a search warrant. This acts as an important constitutional check on the power of the state over individuals, and guards against the risk of a single agency becoming the "secret police".

Intelligence and security agencies provide a cross-government perspective

2.24 Unlike agencies with specific frontline and policy responsibilities that drive their decision-making, intelligence and security agencies exist to inform decisions across the whole of government, with regard to the broader security context and New Zealand's international and economic interests.

2.25 As noted above, the Agencies do not collect information for the purpose of achieving specific policy outcomes. Their cross-government perspective enables the government to receive comprehensive, balanced assessments of risks and opportunities in order to make policy decisions.

Intelligence collection requires specialist skills and capability

2.26 Specialist skills and capabilities are required to collect, piece together and analyse the information needed to advise the government about threats to security or developments affecting New Zealand's interests. For example, the GCSB consists of staff from a wide range of disciplines including foreign language experts, communications and cryptography specialists, engineers and technicians. Some of the Agencies' specialist capabilities are discussed further in Chapter 3.

2.27 The information, and the methods used to collect it, are often highly sensitive or classified and need to be protected accordingly. In some instances, highly specialised technical skills are required to collect or analyse information, for example, encrypted communications.

2.28 While there are some overlaps in intelligence collection with other government agencies, there are efficiencies to be gained in centralising expertise where possible.

Chapter 3: New Zealand's intelligence system

3.1 Intelligence collection is part of a continuous cycle of developing unrefined data into assessed intelligence products. On either side of collection, the government sets priorities and analysts assess the material collected for eventual distribution to decision-makers. In this chapter we explain this cycle and the role that each part of the intelligence community plays in it. Our aim is to provide as much detail as possible on how the government sets national security priorities, how the Agencies collect intelligence, how intelligence is assessed and the various levels of oversight and scrutiny in place. See Annex D for an overview of the intelligence system, including the agencies involved in it.

Setting priorities

3.2 New Zealand takes an "all-hazards" approach to national security. This means all national security risks, whether internal or external, human or natural, are included within the ambit of the national security system.[77] These risks include a broad spectrum of threats from terrorism, espionage and cyber security to earthquakes, floods and major biohazard events.

3.3 The Agencies do not set their own priorities. The National Security Committee (NSC) of Cabinet is responsible for determining national security intelligence priorities. These priorities serve to focus the efforts of relevant government agencies on those issues that are most important to New Zealand. They are based on seven key objectives:

- protecting the physical security of citizens and exercising control over territory consistent with national sovereignty
- protecting both physical and virtual lines of communication that allow New Zealand to communicate, trade and engage globally
- contributing to the development of a rules-based international system and engaging in targeted interventions offshore to protect New Zealand's interests
- maintaining and advancing the economic well-being of individuals, families, businesses and communities
- preventing activities aimed at undermining or overturning government institutions, principles and values that underpin New Zealand society
- providing for and mitigating natural or man-made risks to the safety of citizens and communities, and

[77] Department of the Prime Minister and Cabinet *New Zealand's National Security System* (May 2011).

- contributing to the preservation and stewardship of New Zealand's natural and physical environment.[78]

3.4 At the heart of any discussion about intelligence priorities is an assessment of how much risk a country is willing to take about its future, and therefore how much "information insurance" it needs.[79] This assessment depends in part on the nature of a country's international interests, and on the contribution that secret intelligence is expected to make to an understanding of national security threats and opportunities.[80]

3.5 New Zealand's intelligence priorities are focused on both geographic and thematic threats and opportunities. While the actual list of priorities is secret, the key threats identified by the recently declassified Briefing to Incoming Ministers provide an indication of some of the priorities. These include:

- a rise in violent extremism in New Zealand and by New Zealanders
- loss of information and data through compromises of major New Zealand companies and government departments
- hostile intelligence operations in and against New Zealand
- illicit drug trafficking
- money laundering
- mass arrivals of illegal immigrants
- illegal fishing in New Zealand's maritime domain, and
- instability in the South Pacific.

3.6 Once Ministers agree on priorities, the Officials' Committee for Domestic and External Security Co-ordination ("ODESC") and its subordinate governance boards and working committees assist the NSC by producing detailed requirements of what information is needed for each topic, and what is practical and achievable given the capabilities and resources of the New Zealand Intelligence Community ("NZIC").[81] The Chief Executive of the Department of the

[78] Department of the Prime Minister and Cabinet *New Zealand's National Security System* (May 2011).
[79] Loch K. Johnson (ed) *The Oxford Handbook of National Security Intelligence* (Oxford University Press, New York, 2012) at 14.
[80] Loch K. Johnson (ed) *The Oxford Handbook of National Security Intelligence* (Oxford University Press, New York, 2012) at 14.
[81] The NZIC is made up of government agencies representing a broad spectrum of intelligence providers within New Zealand's national security system. The core NZIC is the GCSB, the NZSIS and the NAB. Defence Intelligence, Police, Customs, Immigration, the Ministry of Primary Industries and the Ministry of Foreign Affairs and Trade are all part of the wider NZIC. Key users of intelligence such as Maritime New Zealand, The Treasury and the Ministry of Health may also be involved with the ODESC system and/or intelligence requirement-setting where relevant.

Prime Minister and Cabinet ("DPMC") serves as the chair of ODESC and the Security and Intelligence Group within the Department provides the ODESC secretariat. The Security and Intelligence Group is also responsible for the leadership, co-ordination and performance of the core NZIC, that is, the GCSB, NZSIS and the National Assessments Bureau ("NAB").

Collection

3.7 New Zealand adopts an "all-source" approach to intelligence collection. Multiple government agencies collect information that is processed into intelligence. Some of these collection agencies are operational agencies that collect intelligence on particular topics relevant to their areas of expertise. For example, Defence Intelligence collects intelligence to support military operations and provides geospatial intelligence (geographic imagery and mapping data). Police, Customs, Immigration, and the Ministry of Primary Industries all have intelligence capabilities. The Ministry of Foreign Affairs and Trade also collects information that would not otherwise be available to New Zealand through its network of diplomatic missions overseas.

3.8 The NZSIS and GCSB form the core of the secret intelligence collection community in New Zealand. They are different from the other agencies referred to above in that they do not have specific decision-making or enforcement functions. They collect information for other people and agencies to use, rather than for their own purposes. The NZSIS does this primarily by using human, rather than electronic, sources of information. This is called human intelligence or "HUMINT". The GCSB, by contrast, uses highly technical methods to obtain electronic communications and signals. This is called signals intelligence or "SIGINT". We set out our understanding of the collection methods used by NZSIS and GCSB in more detail below.

The New Zealand Security Intelligence Service

3.9 The NZSIS was established in 1956 as the New Zealand Security Service. It grew out of the Police Special Branch, which was established in 1949, and its predecessor, the Security Intelligence Bureau of 1941. In 1969, Parliament passed legislation to govern NZSIS operations. The NZSIS's main function is to collect intelligence relevant to security and advise government ministers on matters of security.[82]

3.10 The NZSIS is not a public service department and was established outside the public service sector legislation in force at that time. The State Sector Act 1988 and all other legislation dealing with employment relationships do not apply to the NZSIS. But the NZSIS is a part of the wider state services, which includes the NZDF and Police. It is required by legislation to be apolitical when discharging its statutory functions.[83] The NZSIS does not have a chief

[82] The NZSIS also advises government on protective security measures, conducts inquiries into whether certain individuals should be granted a security clearance and makes recommendations relevant to security under the Citizenship Act 1977 and Immigration Act 2009.
[83] New Zealand Security Intelligence Act 1969 (NZSIS Act), s 4AA.

executive (an administrative head), but it is controlled by a Director of Security. The Director is appointed by the Governor-General.[84]

3.11 In its early days during the Cold War, the NZSIS focused its intelligence-gathering activities on countering the perceived threat of foreign espionage and subversive activities in New Zealand. Initially, this included monitoring domestic organisations that were either overtly communist or pro-Soviet and were suspected of seeking to establish in New Zealand a Soviet-style government. Groups such as the Communist Party of New Zealand and the Society for Closer Relations with Russia were watched closely for any signs that their members included hostile agents or that they were disseminating subversive materials in New Zealand. Later in the Cold War, the NZSIS collected intelligence on anti-war, anti-nuclear and Māori protest movements as it suspected they had been infiltrated by radical and subversive elements.[85]

3.12 Today, the NZSIS is focused mainly on protecting New Zealand against threats from violent extremists, preventing the proliferation of weapons of mass destruction, identifying and investigating foreign intelligence agents whose work is directed against New Zealand interests, and providing protective security advice to New Zealand government agencies. Detecting and preventing sabotage and subversive activities is still a part of the NZSIS's legislative mandate, but the NZSIS Act explicitly states that the exercise of the right to engage in lawful advocacy, protest, or dissent does not, of itself, justify the NZSIS instituting surveillance of any person in New Zealand.[86]

3.13 In the 2014/15 year, the NZSIS had approximately 240 staff members and its total expenditure was NZ$44,770,000.[87]

What does an NZSIS investigation involve?

3.14 NZSIS investigations begin with a "lead", or information suggesting a possible security threat. The NZSIS receives leads from a variety of sources, including foreign partners, members of the public, government agencies and information gathered in the course of other NZSIS intelligence work. An example of a lead might be a foreign partner alerting the NZSIS that an individual training in combat with a terrorist organisation in Syria has a New Zealand phone number.

3.15 Once an intelligence officer receives the lead, they decide what initial steps to take to determine whether the lead requires further investigation. These steps may include checking the NZSIS's own files or requesting information from government agencies or private businesses, such as telecommunications companies or banks. Any initial steps must be lawful and proportionate. In the example given above, information from a telecommunications

[84] NZSIS Act, s 5(2).
[85] Graeme Hunt *Spies and revolutionaries: A history of New Zealand subversion* (Reed, Auckland, 2007) at 257–264.
[86] NZSIS Act, s 2(2).
[87] New Zealand Security Intelligence Service *Annual Report for the year ended 30 June 2015* at 8 and 29.

company may reveal the identity of the person using the phone, while a government agency may be able to confirm the person is a New Zealand citizen.

3.16 Metadata is an important tool, particularly at the initial stage where NZSIS is seeking to determine whether a lead requires further investigation. Metadata is data about data, such as the time, date and sender of an email or text message. Metadata associated with phone calls might disclose the frequency and type of contact between individuals and the broad location from which messages and calls are sent and received. This type of information might enable the NZSIS to establish, for example, that a person of interest is in contact with a known foreign intelligence officer or ISIL recruiter.

3.17 On many occasions, the information obtained during these initial enquiries will allow the NZSIS to determine that there is no credible threat. The investigation is then discontinued. In other cases, further investigation is required and the intelligence officer will consider what next steps are appropriate.

3.18 The NZSIS has a range of collection methods that are used in combination to build a picture of the possible threat, corroborate information from different sources and determine whether any further investigation is necessary. NZSIS case officers speak confidentially to members of the public who may be able to provide relevant information. Some of these individuals may provide confidential information on an ongoing basis or assist the NZSIS in other ways, such as by facilitating access to certain people or places.

3.19 Another way the NZSIS collects intelligence is through surveillance. This may include physically observing individuals to track their movements and who they are meeting with, or using listening devices or electronic tracking devices (if an applicable warrant is obtained).

3.20 Once all necessary collection is completed, NZSIS intelligence officers bring together all the relevant information and assess the level of risk posed by an individual or group. If they decide the person or group poses no credible threat, the investigation is concluded. If the information suggests there is a credible threat, the NZSIS may make a report to that effect to political decision-makers and/or an enforcement agency such as Police.

The Government Communications Security Bureau

3.21 In a pre-electronic age, gathering communications intelligence was a labour-intensive activity, which involved physically acquiring, opening and reading communications exchanged within or across borders (for example, letters). Signals intelligence came into being during the First World War with the interception of radio messages and telegrams. The widespread use of machine-enabled encryption during the Second World War spurred the development of ways to speed-up the decryption process through, for example, the development of the massive decryption facility at Bletchley Park and Alan Turing's "Bombe" machine to decipher German Enigma-machine encrypted messages.

3.22 New Zealand has had the capability to decipher foreign coded messages since the Second World War. This function was performed by the Armed Forces and the New Zealand Post Office until the formation of the Combined Signals Organisation in 1955, a unit within the NZDF. The Combined Signals Organisation was replaced by the GCSB, a civilian organisation within the NZDF, in 1977.

3.23 In 1989 the GCSB was made a separate entity, with its chief executive reporting directly to the Prime Minister. In 2003, the GCSB was given a statutory footing and made a public service department. The GCSB's objective is to contribute to the national security, international relations and well-being, and economic well-being of New Zealand. The Act also specifies the GCSB's functions, which are to:[88]

- provide information assurance and cyber security services to protect information and infrastructure of importance to New Zealand
- gather and analyse intelligence about the capabilities, intentions and activities of foreign persons and organisations, and
- co-operate with and assist the NZSIS, Police and NZDF to carry out their lawful functions subject to any restrictions that apply to those agencies.

3.24 Today, the GCSB employs around 330 staff across a wide range of disciplines (including foreign language experts, communications and cryptography specialists, engineers, technicians and corporate staff). Its total expenditure for the 2014/15 year was NZ$86,834,000.[89]

What does a GCSB intelligence operation involve?

3.25 The GCSB undertakes collection in response to requests for information from intelligence users within the New Zealand government, such as government agencies or ministers. Requests usually take the form of an intelligence question – for example, the GCSB might be asked to monitor illegal fishing activity within New Zealand's area of responsibility.

3.26 Before collecting any information, the GCSB checks that the request is in line with the intelligence priorities and requirements agreed by the NSC (as discussed above). It also makes sure that the methods it needs to use to get the information are lawful, proportionate to the information sought and authorised under an appropriate warrant or authorisation.

3.27 If these initial thresholds are met, a GCSB analyst researches who or what is likely to be a source of information and which intelligence methods are likely to be most productive. Sources are generally foreign persons or organisations, as there is a statutory restriction on

[88] Government Communications Security Bureau Act 20013 (GCSB Act), ss 8A, 8B and 8C.
[89] Government Communications Security Bureau *Annual Report for the year ended 30 June 2015* at 8 and 31.

the GCSB's ability to intercept the private communications of New Zealand citizens or permanent residents.[90]

3.28 As a signals intelligence agency, the GCSB gets information by intercepting and potentially deciphering electronic communications. "Communication" is understood in a broad sense, including all kinds of electronic signals sent by people and machines.[91] For example, the GCSB might intercept radar signals or internet browsing history, phone calls, text messages, emails or radio transmissions. This interception could include metadata, which we have discussed above in relation to the NZSIS, and/or the content of messages.

3.29 Communications can be intercepted in a number of ways, depending on how they are transmitted. The GCSB has two interception stations: a high frequency radio interception and direction finding station at Tangimoana, near Palmerston North, and a satellite communications interception station at Waihopai, near Blenheim. The GCSB can also obtain information by accessing an information infrastructure.[92]

3.30 The GCSB can also request the assistance of telecommunications service providers and network operators with interception and access. Network operators are legally required to ensure their services or networks have interception capability.[93] Network operators and service providers are required to assist a surveillance agency, which includes the GCSB, to collect communications in accordance with a warrant or authorisation.[94]

3.31 In addition to these methods of primary intelligence collection, the GCSB can also access information through its foreign partners (as discussed further below). This is particularly useful where the intelligence sought relates to areas of the globe that the GCSB may not itself have the capacity or capability to collect information about.

3.32 Once a GCSB analyst has identified a target and the best way to access the information requested, the GCSB will again check that there is an appropriate warrant or authorisation in place allowing it to proceed, or apply for a new one if required.[95] The analyst then issues instructions to the part of the GCSB responsible for carrying out the intelligence collection method selected (for example, a request may be sent to Waihopai if satellite communications are required). These instructions will provide specific details about the information to be collected.

---

[90] GCSB Act, s 14. There are exceptions to this general restriction, as discussed in Chapter 5.
[91] GCSB Act, s 4: **communication** includes signs, signals, impulses, writing, images, sounds, information or data that a person or machine produces, sends, receives, processes, or holds in any medium.
[92] GCSB Act, s 4: **information infrastructure** includes electromagnetic emissions, communications systems and networks, information technology systems and networks, and any communications carried on, contained in, or relating to those emissions, systems, or networks.
[93] Telecommunications (Interception Capability and Security) Act 2013, Part 2.
[94] Telecommunications (Interception Capability and Security) Act 2013, s 24.
[95] The warrant and authorisation requirements applying to GCSB are set out in Chapter 6.

3.33 A digital copy of the information collected is taken for GCSB analysts to examine. The information needs to be processed into a useable format, which might involve, for example, decrypting or translating it. Once this is done, an analyst assesses the information for its intelligence value. If the information helps to answer the user's intelligence question, the analyst will prepare an intelligence report conveying the key facts. If the information is irrelevant, the analyst assesses whether there are other ways to obtain the required information.

Does the GCSB conduct "mass surveillance"?

3.34 As we discussed in Chapter 1, there has been some debate in the public arena about whether the GCSB conducts "mass surveillance". In light of this, we considered it important to describe what the GCSB does and does not do. While we cannot go into as much detail as we would have liked given the classified nature of the GCSB's operational activities, we hope what we can say will inform this debate in a useful way.

3.35 "Mass surveillance" is a term that can be understood in a number of different ways. In this context it is important to distinguish between communications that are collected by GCSB systems – for example, its satellite interception station at Waihopai – and those that are actually selected and examined by an analyst.

3.36 The reality of modern communications is that it is often not possible to identify and copy a specific communication of interest in isolation. If a particular satellite might carry a relevant communication, the GCSB cannot search for that communication before interception occurs. First it needs to intercept a set of communications, most of which will be of no relevance and will be discarded without ever being examined by an analyst. This is the haystack in which the needle must be found.

3.37 Even this "haystack" represents only a tiny proportion of global communications. The GCSB conservatively estimates that there are over 1 billion communications events every day on the commercial satellites that are visible from Waihopai station. These represent approximately 25 percent of commercial satellites that match the Earth's rotation[96] (although signals cannot always be secured even from those satellites that are visible). We were told the proportion of those 1 billion communications that are actually intercepted equates to roughly one half of a bucket of water out of an Olympic-sized swimming pool.

3.38 To find the "needle" (or the communications that are of intelligence value), the GCSB filters intercepted material for relevance using search terms. Only those communications that meet the selection criteria are ever seen by an analyst. The GCSB has internal processes in place to

[96] This is referred to as "geosynchronous orbit". Satellites in geosynchronous orbit stay roughly in the same position relative to the Earth. Satellites that are in low or medium-Earth orbit rather than geosynchronous orbit move at a different rate to the Earth's rotation and are therefore positioned over different regions on different days.

ensure analysts justify their use of each search term and record all searches for the purpose of internal audits and review by the Inspector-General of Intelligence and Security.

3.39 Given these controls on what information can actually be examined by analysts, in our view the GCSB's ability to intercept sets of communications does not amount to mass surveillance. That term suggests a kind of active monitoring of the general population that does not occur. It would neither be lawful nor even possible given the GCSB's resourcing constraints.

3.40 Capacity acts as a check on all signals intelligence agencies, although it is particularly pronounced for the GCSB given its comparatively small size. It is simply not possible to monitor communications (or other data) indiscriminately. Professor Michael Clarke, the (now retired) Director-General of the UK's Royal United Services Institute who convened the 2015 Independent Surveillance Review, referred to this when giving evidence before the Joint Committee on the Draft Investigatory Powers Bill:[97]

> The other great safeguard is the sheer physical capacity. One will be astonished at how little [intelligence agencies] can do, because it takes so much human energy to go down one track. The idea that the state somehow has a huge control centre where it is watching what we do is a complete fantasy. The state and GCHQ [the UK's signal's intelligence agency] have astonishingly good abilities, but it is as if they can shine a rather narrow beam into many areas of cyberspace and absorb what is revealed in that little, narrow beam. If they shine it there, they cannot shine it elsewhere. The human limitation on how many cases they can look at once is probably the biggest safeguard.

3.41 We also observe that there are currently restrictions on the GCSB's ability to intercept the private communications of New Zealand citizens and permanent residents.[98] These restrictions apply to New Zealanders anywhere in the world, not just those in New Zealand. It was clear to us from our discussions with GCSB staff and from the GCSB's own internal policy documents that these restrictions are interpreted and applied conservatively.[99] Far from carrying out "mass surveillance" of New Zealanders, the GCSB is unable to intercept New Zealanders' communications even where it is for their own safety.[100] For example, the GCSB would be unable to analyse the communications of a New Zealander taken hostage in a foreign country unless it was assisting the NZSIS, NZDF or Police under their legislation.

---

[97] Joint Committee on the Draft Investigatory Powers Bill "Oral Evidence: Draft Investigatory Powers Bill" (HC 651, 2 December 2015), accessed at <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/oral/25685.html>.

[98] GCSB Act, s 14. This restriction is discussed in detail in Chapter 5.

[99] Government Communications Security Bureau *Nationality Policy* at [13], accessed at <http://www.gcsb.govt.nz/assets/GCSB-Documents/GCSB-Nationality-Policy.pdf>.

[100] As we discuss in Chapter 5, there are a number of problems with the current restriction on GCSB intercepting New Zealanders' private communications that lead us to recommend its removal. However, we propose GCSB would only be able to target New Zealanders for limited national security reasons and in accordance with a strict authorisation regime. This would leave no room for large-scale surveillance of New Zealanders.

Foreign partners

3.42 As national security threats are becoming more complex and transnational, it would be extremely expensive for New Zealand to create a wholly self-reliant intelligence community.[101] This is particularly so given our small size when compared to some of our partners. Through foreign intelligence partnerships, New Zealand draws on a much greater pool of information, skills and technology than would otherwise be available to it. For example, a foreign partner may have greater access to intelligence that requires the right mix of ethnic, cultural and language backgrounds to collect and analyse.[102] Intelligence partnerships also help New Zealand prioritise and focus intelligence collection and assessment resources on the areas most important to us, while avoiding intelligence gaps.

3.43 We obtained some statistics from the Agencies that give a sense of how significant our international partnerships are. Of all security leads the NZSIS investigates, around half are received from foreign partners. These represent possible threats to the security of New Zealand, most of which we would not be able to discover on our own (for instance, because they have a foreign source). New Zealand also gains considerably more from its international partnerships than we provide in return. For every intelligence report the NZSIS provides to a foreign partner, it receives 170 international reports. Similarly, for every report the GCSB makes available to its partners, it receives access to 99 in return.

3.44 New Zealand's most publicised partnership is that with the USA, UK, Australia and Canada (the Five Eyes). Defence and intelligence co-operation between the USA and the UK during the Second World War resulted in the UKUSA agreement of 1946.[103] The agreement governed co-operation between the USA, UK and all other British Empire SIGINT authorities. All parties agreed to exchange intelligence products relating to "foreign communications". In 1955 the agreement was updated to explicitly include Canada, Australia and New Zealand as "UKUSA-collaborating Commonwealth countries", elevating and distinguishing them from other Commonwealth countries.

3.45 Collaboration between the Five Eyes has moved beyond just intelligence over the past 70 years. It also extends to border security, defence and police activities (for example, the Five Country Conference on Immigration). Ministers with responsibility for domestic security also meet regularly as the "Five Country Ministerial".[104]

---

[101] Even after the suspension of some forms of defence co-operation following the introduction of New Zealand's anti-nuclear policy in the 1980s, New Zealand did not face the costs of a self-reliant intelligence capability because of continued co-operation between Five Eyes signals intelligence agencies.

[102] Loch K. Johnson (ed) *The Oxford Handbook of National Security Intelligence* (Oxford University Press, New York, 2012) at 215.

[103] National Security Agency Central Security Service "UKUSA Agreement Release 1940-1956", accessed at <https://www.nsa.gov/public_info/declass/ukusa.shtml>.

[104] The Ministers released a communiqué following their meeting in London on 6 February 2015: see <https://www.gov.uk/government/news/five-country-ministerial-communique>.

3.46 Internationally, the Five Eyes is generally considered to be the most comprehensive and closest intelligence sharing and co-operation arrangement. However, there are other intelligence sharing networks. For example, the "Club de Berne" is reportedly an intelligence sharing arrangement involving all 28 EU countries. There is also the European Union's Frontex Risk Analysis Network, which links the intelligence networks of individual European countries to share knowledge and analysis of irregular migration and cross-border criminal activities.[105]

3.47 The Five Eyes is by far New Zealand's most valuable intelligence arrangement, giving us knowledge and capability far beyond what we could afford on our own. Having said that, the members of the Five Eyes are not the only foreign partners that New Zealand shares and co-operates with on intelligence matters. New Zealand also has other bilateral intelligence relationships with friendly countries around the world. The significance of our co-operation with them differs based on the extent to which our interests overlap with theirs.

Assessment

3.48 The large volume of information available and collected is often in raw form and in bits and pieces. While the collection agencies perform some limited analysis, for example decrypting, translating and consolidating information, the intelligence still needs to be assessed for its veracity, filtered for relevance and contextualised for decision-makers. New Zealand has a dedicated assessments agency to perform this function: the NAB, which is a business unit within DPMC.

3.49 The NAB provides short situational reports and long-term strategic assessments on overseas political, economic, environmental and security developments. It does not collect intelligence. Rather, NAB's role is to interpret information from a variety of sources (which might include a blend of secret and open source information) in order to illuminate issues for decision-makers. For example, the NAB may undertake an analysis of geo-political and economic power shifts in the balance of oil supply and demand, and what this may mean for New Zealand's resource security. This report would be provided to those ministers and agencies with responsibility for ensuring New Zealand has sufficient energy resources to meet current and future demand. The NAB does not offer advice on what actions the government might take. The Director, Intelligence and Assessments, is directly accountable to the Prime Minister for the content and quality of the NAB's assessments.

3.50 The Combined Threat Assessment Group (CTAG) is an interdepartmental assessment unit that is located within the NZSIS. Representatives include the GCSB, Police, Defence Intelligence and the Aviation Security Service. Unlike the NAB, the CTAG's focus is purely on assessing terrorist threats to New Zealanders and New Zealand, and providing advice on the domestic terrorism threat level.

[105] Frontex "Strategic analysis", accessed at <http://frontex.europa.eu/intelligence/strategic-analysis/>.

3.51 The Police and Defence Intelligence units also assess security intelligence relevant to their particular areas of responsibility such as the supply of illicit drugs or foreign military capabilities.

Oversight

3.52 In New Zealand there are several layers of oversight that apply to the Agencies. At a statutory level, the Directors of the GCSB and NZSIS and all employees are obliged to comply with New Zealand law and must report breaches where they occur. The Minister responsible for the Agencies exercises oversight on behalf of the executive branch of government and, along with the Commissioner of Security Warrants, authorises the Agencies' intrusive activities. The Inspector-General and the Intelligence and Security Committee ("ISC") were both introduced in 1996 to increase the level of oversight of the Agencies. Since then, both roles have been strengthened with greater powers and better institutional arrangements, as described below.

Internal mechanisms

3.53 The directors of the GCSB and NZSIS have statutory responsibilities to ensure the Agencies act free from any political influence.[106] The NZSIS's Director of Security determines how the NZSIS collects intelligence in the interests of security.[107] The GCSB's cyber security activities and any co-operation with the NZSIS, Police and NZDF are at the discretion of the GCSB Director.[108] Both directors also have a role in applying for relevant intelligence warrants[109] and, in the case of the GCSB Director, authorising certain activities.[110]

3.54 The Agencies also have a range of other director-approved internal policies and compliance procedures, including procedures for accessing and retaining data collected, to ensure their activities comply with their obligations under New Zealand law. A small number of these policies have been published on the Agencies' websites, providing a degree of public insight into the Agencies' internal mechanisms.[111]

Ministerial oversight

3.55 On 6 October 2014, the Prime Minister announced new ministerial arrangements for intelligence and security matters. Previously, the Prime Minister held the roles of Minister Responsible for the GCSB and Minister in Charge of the NZSIS. Under the new arrangements, these portfolios are held by a different Minister, while the Prime Minister fills the new role of Minister for National Security and Intelligence.

---

[106] GCSB Act, s 8D(3) and NZSIS Act, s 4AA(1).
[107] NZSIS Act, s 4(1)(a).
[108] GCSB Act, s 8(4).
[109] GCSB Act, s 15A and NZSIS Act, s 4A(4).
[110] GCSB Act, s 16.
[111] See for example the GCSB's Nationality Policy and Incidental Intelligence Policy, accessed at <http://www.gcsb.govt.nz/publications/>.

3.56 The Minister for National Security and Intelligence, the Prime Minister, is responsible for leadership of the national security system and the overall policy settings and legislative framework of the sector.

3.57 The Minister Responsible for the GCSB and Minister in Charge of the NZSIS operates within the framework set by the Minister for National Security and Intelligence and is responsible for:

- exercising ministerial oversight of the Agencies
- approving applications for warrants and authorisations under the GCSB and NZSIS Acts
- submitting papers, including business cases for investment, to Cabinet for approval
- contributing to the development of the Four Year Plan, and
- approving the presentation of annual reports to Parliament.

3.58 This portfolio is currently held by Hon Christopher Finlayson QC, who is also the Attorney-General.

Commissioner of Security Warrants

3.59 The Commissioner of Security Warrants, who must be a former judge, has a role in authorising warrants and authorisations for the Agencies. He or she is appointed by the Governor-General on the recommendation of the Prime Minister following consultation with the Leader of the Opposition.[112]

3.60 In relation to the NZSIS's activities, the Commissioner advises the responsible Minister on domestic intelligence warrant applications and jointly issues those warrants with the Minister.[113] The Commissioner is also involved in jointly issuing warrants and authorisations with the Minister responsible for the GCSB if the warrant or authorisation is for the purpose of intercepting the private communications of a New Zealand citizen or permanent resident.[114]

3.61 The current Commissioner is Sir Bruce Robertson. In his oral evidence before the UK Joint Committee on the Draft Investigatory Powers Bill, Sir Bruce explained the process he undertakes before granting a warrant. It involves inspecting the detail of the application and meeting with the Agencies' legal and operational staff to discuss why they are seeking a warrant and why they consider it meets the tests of necessity and proportionality. The Agencies' legislation does not restrict the Commissioner to just considering the legality of

[112] NZSIS Act, s 5A(2).
[113] NZSIS Act, s 5A(5)(a)–(d).
[114] GCSB Act, s 15B. The circumstances in which the GCSB can intercept the private communications of New Zealanders is limited by section 14 of the GCSB Act, discussed further in Chapter 5 below.

proposed activities when granting warrants. However, in practice Sir Bruce places less emphasis on his assessment of diplomatic and "high policy" matters.[115]

Auditor-General, Privacy Commissioner, Office of the Ombudsman

3.62 The Controller and Auditor-General, an Officer of Parliament, provides independent assurance that public sector organisations, including the GCSB and NZSIS, are operating and accounting for their performance in accordance with Parliament's intentions.

3.63 While the Agencies are both exempt from certain principles in the Privacy Act 1993, they are still subject to principles 6 and 7: the right of a person to request access to information held about them and to request correction of that information. Anyone can complain to the Privacy Commissioner if they think the GCSB or NZSIS has breached principle 6 or 7, and the Commissioner can inquire into such complaints.

3.64 The 2013 amendments to the GCSB Act also included a requirement for the GCSB to develop a personal information policy in consultation with the Privacy Commissioner and the Inspector-General.[116] The policy must be regularly audited and the Privacy Commissioner advised of the results.[117] If the results reveal issues that need to be addressed, the Privacy Commissioner can provide a report to the Inspector-General on those issues.[118]

3.65 The Agencies are both subject to the Official Information Act 1982, under which any New Zealand citizen or permanent resident and any person in New Zealand can request information held by an agency.[119] If the Agencies refuse to release or delay releasing information, or if a requester is unhappy with the response, the requester can complain to the Ombudsman who is an Officer of Parliament. The Ombudsman may decide to investigate and make a recommendation to the Agencies where necessary. The recommendation becomes binding 21 working days after it is made unless it is vetoed by Cabinet.

Inspector-General of Intelligence and Security

3.66 The Inspector-General of Intelligence and Security is a statutory role established to assist the Minister responsible for the Agencies to ensure their activities comply with New Zealand law. The Inspector-General and Deputy Inspector-General are appointed by the Governor-General

[115] Joint Committee on the Draft Investigatory Powers Bill "Oral Evidence: Draft Investigatory Powers Bill" (HC 651, 6 January 2016), accessed at <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/oral/26679.html>.
[116] GCSB Act, s 25A.
[117] GCSB Act, s 25A(2)(b) and (3).
[118] GCSB Act, s 25A(4).
[119] Official Information Act 1982, s 12 and sch 1.

on the recommendation of the Prime Minister following consultation with the Intelligence and Security Committee.[120]

3.67 The Inspector-General of Intelligence and Security Act 1996 was amended in 2013 to expand the Inspector-General's inquiry functions. The Inspector-General can now initiate inquiries into the propriety of the Agencies' actions or practices on his or her own motion, without requiring the concurrence of the Minister.[121] Underpinning these individual inquiries are regular and sometimes unscheduled inspections of the Agencies' procedures and compliance systems.[122] The Inspector-General also independently investigates complaints by the New Zealand public or employees or former employees of the Agencies who have been adversely affected by any act, omission, practice, policy, or procedure of the Agencies.[123]

3.68 To accommodate the expanded functions, more resources were added to the Inspector-General's office including the appointment of a Deputy Inspector-General and a team of investigative staff.

3.69 To carry out his or her functions, the Inspector-General has wide powers of access to the Agencies' security records and their premises, including the GCSB's two interception stations at Tangimoana and Waihopai.[124] The Inspector-General also has the power to require any person to give evidence on oath or provide documents that may be relevant to an inquiry.[125]

Intelligence and Security Committee

3.70 The Intelligence and Security Committee ("ISC") is a statutory committee established by the Intelligence and Security Committee Act 1996, rather than a committee of Parliament as is the case with select committees. The ISC examines the policy, administration and expenditure of the Agencies, considers their annual reports and conducts an annual financial review of their performance. It also considers Bills or other matters relating to the Agencies referred to it by Parliament, and any matters referred by the Prime Minister due to their security or intelligence implications.[126]

3.71 The ISC has five members – the Prime Minister, the leader of the opposition, two members of Parliament ("MPs") nominated by the Prime Minister after consultation with the leaders of parties in Government, and one MP nominated by the leader of the opposition after

[120] Inspector-General of Intelligence and Security Act 1996 (IGIS Act), s 5(2).
[121] IGIS Act, s 11(1)(a) and (ca).
[122] IGIS Act, s 11(1)(d) and (da).
[123] IGIS Act, s 11(1)(b), (ba) and (c).
[124] IGIS Act, ss 20 and 21.
[125] IGIS Act, s 23.
[126] Intelligence and Security Committee Act 1996 (ISC Act), s 6(1).

consultation with the leaders of parties not in Government.[127] Members serve on the ISC in their capacity as MPs, not as representatives of the Government.[128]

3.72 The ISC cannot inquire into any matter that is operationally sensitive, including matters that relate to intelligence collection methods or sources.[129] It is also prohibited from inquiring into issues within the jurisdiction of the Inspector-General and from inquiring into individual complaints about the activities of the Agencies.[130] Due to the confidential and secret nature of the matters discussed, all of the ISC's proceedings except for its financial review of the Agencies are held in private unless the members unanimously resolve to do otherwise.[131]

3.73 The ISC receives and considers the annual reports of the Agencies.[132] These annual reports include a detailed statement on warrants issued for the Agencies' activities.[133] In the case of the NZSIS, the statement on warrants includes the interception and seizure methods used under the warrants and a general assessment of the importance of the warrants.[134]

Protections for whistle-blowers

3.74 In New Zealand, the Protected Disclosures Act 2000 allows employees of the Agencies to report any serious wrongdoing to the Inspector-General. The Inspector-General is considered the appropriate authority because of the highly secret nature of the work and the Inspector-General's wide powers of inquiry into the Agencies' activities. The Agencies are also required by legislation to have internal procedures to facilitate such disclosures and we understand both agencies have such policies in place.

3.75 Whistle-blowing can be a big risk for employees. The Inspector-General of Intelligence and Security Act acknowledges this and provides protections for whistle-blowers against any direct penalty or discriminatory treatment arising out of making a disclosure. The employee also has additional protections outlined in the Protected Disclosures Act such as immunity from criminal proceedings that could ordinarily be brought if a person discloses classified information.[135]

---

[127] ISC Act, s 7.
[128] ISC Act, s 7(4).
[129] ISC Act, s 6(2)(b).
[130] ISC Act, s 6(2)(a) and (c).
[131] ISC Act, s 12(2) and 12(2A).
[132] ISC Act, s 6(1)(c).
[133] GCSB Act, s 12 and NZSIS Act, s 4K(1).
[134] NZSIS Act, s 4K(2).
[135] Protected Disclosures Act 2000, s 18. Section 11 of the GCSB Act prohibits any employee of the GCSB from disclosing any information gained in the course of their employment except if it is done in accordance with the person's official duties or as authorised by the Minister. Any employee who discloses information outside of these circumstances can be sentenced to prison for up to three years or have to pay a fine of up to NZ$5,000.

Chapter 4: Transparency and Accountability

4.1 In this chapter we recommend the existing pieces of legislation be replaced with a single Act dealing with the Agencies, their oversight and potentially the assessment of intelligence. We also make recommendations to strengthen the accountability of the Agencies. Finally, we propose amendments to ensure the Inspector-General of Intelligence and Security and the Intelligence and Security Committee are well-placed to oversee the activities of the intelligence community.

The need for robust oversight

4.2 As previous chapters have illustrated, intelligence and security agencies are a necessity for a modern democratic state to detect and protect itself against national security threats, and to advance its economic and international interests. These agencies use special and intrusive powers to carry out their mandate. Some of these powers limit fundamental human rights and could be unlawful if not for specific legislative authorisation. Intelligence and security agencies are also equipped with advanced technological tools. There have been examples in some countries in the past of intelligence and security agencies over-collecting information when they are not adequately controlled by the executive.

4.3 The flexible concept of "national security" also raises the risk that intelligence and security agencies may be used by the executive to pursue illegitimate aims.[136] This was particularly apparent in the Cold War when states used intelligence and security agencies to carry out surveillance of organisations and persons legitimately exercising their rights to freedom of expression, assembly and association.[137]

4.4 Independent external oversight is therefore essential to ensure that by working to secure populations against internal and external threats and advance the interests of the nation as a whole, intelligence and security agencies do not undermine democracy or the rights of individuals in the process. As publicly funded agencies, they must also be held accountable for how they use public money. Oversight must ensure the Agencies are operating efficiently and effectively in the interests of the country and in accordance with the values of its citizens.

[136] European Commission for Democracy through Law (Venice Commission) *Report on the democratic oversight of the security services* (Strasbourg, 11 June 2007) at 4.
[137] Aidan Wills & Ors *Parliamentary oversight of security and intelligence and security agencies in the European Union* (European Parliament, Brussels, June 2011) at 85.

Striking a balance

4.5 The secret nature of the Agencies' operations makes effective oversight much more difficult to achieve. Non-government organisations and journalists are not allowed the same levels of access or transparency as they can expect from other government agencies. The challenge is balancing the Agencies' need for secrecy to carry out their functions with the public's expectations of transparency, political impartiality and accountability.

4.6 As discussed in the previous chapter, oversight occurs at many levels: from internal controls and compliance mechanisms to ministerial authorisation of the Agencies' activities and appropriate involvement of independent institutions such as the Privacy Commissioner and Controller and Auditor-General. Not all checks and balances are readily apparent; some are built into the organisational structure of the system. For example, intelligence collection, assessment and policy formation have historically been separated. This helps to ensure objective assessments that are not tailored to support the pre-conceptions of collection agencies or the policy preoccupations of the day. A merger of these separate functions into one agency could increase the risk of "intelligence failures". The USA' decision to invade Iraq based on intelligence of Iraq's Weapons of Mass Destruction capability is a cautionary tale of what can happen if collection and assessment functions are not truly objective and at arm's length from policymaking.[138]

4.7 The amount of oversight a country has should be proportionate to the size of its intelligence and security agencies. The USA has an Inspector-General for each agency and one for the entire intelligence and security sector, which comprises 17 separate organisations. It has two parliamentary oversight committees with robust powers of inquiry: the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence. Its total intelligence appropriation was US$50.3 billion (approximately NZ$70.8 billion) in 2015.[139]

4.8 In Australia, the total budget for the intelligence community in 2010 was A$1.07 billion (approximately NZ$1.16 billion).[140] While the total current spending is not made public,[141] that number has increased since 2010. More recently, an additional A$450 million (approximately NZ$489 million) was announced in budget 2015 to strengthen intelligence

[138] See Commission on the Intelligence Capabilities of the USA regarding Weapons of Mass Destruction *Report to the President of the USA* (USA, 31 March 2005).
[139] Office of the Director of National Intelligence "US Intelligence Community Budget", accessed at <http://www.dni.gov/index.php/intelligence-community/ic-policies-reports/ic-policies-2?highlight=WyJidWRnZXQiXQ==>.
[140] Robert Cornall AO and Dr Rufus Black *2011 Independent Review of the Intelligence Community Report* (AU, 2011) at 16.
[141] The budgets for the intelligence agencies that are part of Defence – including the Australian Signals Directorate (ASD), the GCSB's equivalent – are not publicly released and are subsumed within the total defence budget in official documentation. However, the budgets for the Australian Security Intelligence Organisation (ASIO) and Australian Secret Intelligence Service (ASIS) are available. ASIO's appropriation for 2015–16 is A$415 million and ASIS's is A$257 million (Appropriation Act (No 1) 2015–2016, sch 1).

capabilities.[142] Australia has an Inspector-General of Intelligence and Security, a joint parliamentary committee and an Independent National Security Legislation Monitor.

4.9 Canada has an independent, external review Committee of five members for its NZSIS equivalent agency and a single Commissioner for its GCSB equivalent agency, but no formal parliamentary oversight. Its total national security budget for 2015 was C$439 million (approximately NZ$483 million).[143]

4.10 Relative to these countries, New Zealand's spending on intelligence is low. The total expenditure for the NZSIS and GCSB in the year to 30 June 2015 was approximately NZ$130 million.[144]

Improving oversight in New Zealand

4.11 The substantial amendments to the Inspector-General of Intelligence and Security Act in 2013 and the subsequent increase in resources for the Inspector-General's Office marked a great leap forward for New Zealand's intelligence and security oversight. The changes extended the Inspector-General's work programme to require annual checks on the Agencies' compliance systems and enabled the Inspector-General to launch inquiries into matters of propriety without requiring the approval of the responsible Minister. Since these changes, we think it is fair to describe the Office of the Inspector-General as more independent, robust and assertive. We have, however, identified some important areas for improvement, which we detail below.

4.12 Some submitters suggested consolidating our existing oversight mechanisms into a centralised entity. From what we have observed, the current system of oversight is now generally working well and is appropriately structured to meet New Zealand's needs. Different parts of the system serve different purposes and separation is yet another check and balance. We therefore do not think the system requires major structural change. Instead, we are recommending enhancements in six key areas:

- consolidating legislation relating to the Agencies and their oversight (a single Act)
- integrating the Agencies within the public sector

---

[142] Australian Government *Budget 2015–16 Overview: Keeping Australia Safe*, accessed at <http://www.budget.gov.au/2015-16/content/overview/html/overview-18.htm>.

[143] Government of Canada *Budget 2015, Chapter 4.3: Protecting Canadians*, accessed at <http://www.budget.gc.ca/2015/docs/plan/ch4-3-eng.html>. It is unclear whether the national security budget covers more than the NZSIS and GCSB equivalents.
The new Canadian government has promised to create, by the end of 2016, a statutory committee of parliamentarians to review government departments and agencies with national security responsibilities. See Prime Minister of Canada Justin Trudeau "Minister of Public Safety and Emergency Preparedness Mandate Letter", accessed at <http://pm.gc.ca/eng/ministerial-mandate-letters>.

[144] Comprised of $44,770,000 for the NZSIS (New Zealand Security Intelligence Service *Annual Report for the year ended 30 June 2015* at 29) and $86,834,000 for the GCSB (Government Communications Security Bureau *Annual Report for the year ended 30 June 2015* at 31).

- centralising intelligence assessments
- enhancing the independence of the Inspector-General of Intelligence and Security and expanding the scope of the complaints and inquiry functions
- expanding the Intelligence and Security Committee's oversight of the Agencies' operational activities, and
- setting out an explicit process for when the Agencies co-operate or share intelligence with foreign jurisdictions and organisations.

Single Act

4.13 The legislative framework governing the Agencies and their oversight is complex and spread over a number of legislative instruments, making it relatively inaccessible to members of the public. Some submitters suggested replacing these individual instruments with a single, coherent piece of legislation developed from first principles. We agree.

4.14 A single Act would give a comprehensive and much clearer view of the Agencies' functions and powers, and the checks and balances that apply to the operation of their powers. It would avoid inconsistencies and gaps between various statutes and enable a consistent set of fundamental principles to be applied to the Agencies and their oversight.

4.15 We note other jurisdictions have gone some way toward more unified legislation. In the UK, for example, the Intelligence Services Act 1994 sets out the functions of the GCHQ (GCSB's equivalent), MI6 (the UK's foreign human intelligence agency) and the Intelligence and Security Committee. The GCHQ, MI6 and MI5 (the UK's national security intelligence agency) all obtain warrants for their activities under the same Act, the Regulation of Investigatory Powers Act 2000.

4.16 We propose a single Intelligence and Security Act to cover the objectives, functions and powers of the Agencies, the role of our proposed new panel of judicial commissioners (discussed in Chapter 6), and the external oversight roles of the Intelligence and Security Committee and the Inspector-General of Intelligence and Security. As a starting point, we set out in Annex E a possible framework for the single Act. Our recommendations about specific aspects of the legislation are discussed in more detail throughout this report.

4.17 The purpose of the Act should be to protect New Zealand as a free, open and democratic society. This reflects the Agencies' role in assisting the government to fulfil its obligation to ensure its citizens can go about their lawful business safely and without undue interference with their human rights. The purposes of intelligence collection should be limited to those areas where there is a high risk of harm to New Zealand's national interests. In setting out the functions and powers of the Agencies, the Act should reflect this balance between protecting national security and protecting human rights.

4.18 Every action taken towards setting priorities and collecting, analysing, assessing and using intelligence should be done with integrity and in accordance with New Zealand law, including human rights law. Importantly, the single Act should retain the current legislative provisions that require the Agencies to ensure their activities are free from all political influence.[145]

Recommendations

1. The objectives, functions and powers of the Agencies and their oversight should be consolidated into a single Act. The purpose of the Act should be to protect New Zealand as a free, open and democratic society.

2. The single Act should require that every action taken towards setting priorities and collecting, analysing, assessing and using intelligence should be done with integrity and in accordance with New Zealand law, including human rights law. The Act should also retain the current legislative requirement that the Agencies conduct their activities free from all political influence.

Integrating the Agencies within the public sector

4.19 As noted in Chapter 3, the NZSIS is not a public service department but the GCSB is with some limited exceptions. The State Services Commission made a submission to us outlining its view that the appropriate starting point for the NZSIS's and GCSB's legislative settings is for both agencies to sit within the Public Service departmental framework provided by the State Sector Act 1998. We agree with the Commission's view and highlight some of the implications below.

4.20 Some aspects of the State Sector Act would not be appropriate to apply to the Agencies because of the unique nature of some aspects of their work. We recommend the government work with the State Services Commission on the appropriate exemptions or exceptions from the State Sector Act.

4.21 Under the current legislation, both the Director of Security and the Director of the GCSB are required to regularly consult with the Leader of the Opposition for the purpose of keeping him or her informed about matters relating to security and matters relating to the GCSB's intelligence gathering and assistance functions.[146] We think it is in the interests of the Agencies to keep the Leader of the Opposition up to date. The Agencies should therefore continue to consult with the Leader of the Opposition and, as they see fit, the leader of any

[145] GCSB Act, s 8D(3) and NZSIS Act, s 4AA.
[146] GCSB Act, s 8D(4) and NZSIS Act 1969, s 4AA(3).

other political party in Parliament as defined in the Standing Orders of the House of Representatives.

Bringing the NZSIS into the public service

4.22 We recommend the NZSIS should be established as a public service department and relevant provisions of the State Sector Act 1988 should apply to it. The purpose behind the State Sector Act is to promote and uphold public sector departments that operate in the collective interests of government while remaining politically neutral and maintaining appropriate standards of integrity and conduct.[147] Bringing the NZSIS into the public sector proper would support the move toward greater transparency. It should bring about positive changes to the NZSIS's secret culture and help build shared values with the wider public management system. It may attract a wider range of talent from within the public service and make the NZSIS a more appealing career option for senior leaders. As Ms Kitteridge observed in her 2013 review, secondments will help the intelligence community better understand public service norms and provide an opportunity for the wider public service to understand intelligence concerns better.[148]

4.23 Making the NZSIS a public service department would mean the Director of Security or an Acting Director of Security, if required, would be appointed (or removed from office for just cause) by the State Services Commissioner in the same way as other state sector chief executives.[149] The State Services Commissioner would set the remuneration and terms and conditions of employment and undertake regular performance reviews.

4.24 Being a public service department would also mean that the State Services Commissioner could set a minimum standard of integrity and conduct for NZSIS employees. The Commissioner's current Standards of Integrity and Conduct for the public service are designed to reinforce the spirit of service and to encourage behaviour that is fair, impartial, responsible and trustworthy.[150] These standards already apply to the GCSB.

4.25 The Commissioner's Standards of Integrity and Conduct may need to be tailored to account for the unique nature of some aspects of the NZSIS's human intelligence work. We therefore recommend that the NZSIS be required to formulate a Code of Conduct that elaborates on the legislative principles in the proposed new Act. This could be either a variation of the State Services Commissioner's Standards of Integrity and Conduct or a bespoke Code of Conduct. It should be agreed in consultation with the State Services Commissioner. This should ensure

[147] State Sector Act 1988 (SSA), s 1A.
[148] Rebecca Kitteridge *Review of Compliance at the Government Communications Security Bureau* (March 2013) at 58.
[149] SSA 1988, ss 6(d) and 40. The convention of informing the Leader of the Opposition should remain unaffected by this change.
[150] State Services Commission *Standards of Integrity and Conduct: A code of conduct issued by the State Services Commissioner under the State Sector Act 1988, section 57* (June 2007) accessed at <http://www.ssc.govt.nz/code>.

that the resulting Code of Conduct for the NZSIS is consistent with the standards that apply to the rest of the public service and the GCSB.

Extending additional State Sector Act provisions to the GCSB

4.26 In 2003 the GCSB became part of the public service but was not subject to some of the provisions in the State Sector Act. As with the NZSIS, we recommend the relevant State Sector Act provisions relating to the appointment, reappointment, remuneration, performance review and removal from office of the chief executive or acting chief executive be applied to the GCSB.

Recommendations

3. The NZSIS should be established as a public service department and all relevant provisions of the State Sector Act 1988 should apply, subject to specific exemptions or exceptions as appropriate.

4. The NZSIS Director of Security and the Director of GCSB should be appointed (or removed from office for just cause) by the State Services Commissioner. The State Services Commissioner should set the remuneration and terms and conditions of employment and undertake regular performance reviews.

5. The NZSIS should be required to prepare a Code of Conduct based on the principles of the proposed single Act. This could be either a variation of the State Services Commissioner's Standards of Integrity and Conduct or a bespoke Code of Conduct. The Code should be developed in consultation with the State Services Commissioner.

6. The Agencies should continue to consult with the Leader of the Opposition about matters relating to security and the GCSB's intelligence gathering and assistance functions. The Agencies should also, as they see fit, consult with the leader of any other political party in Parliament as defined in the Standing Orders of the House of Representatives about such matters.

Arrangements with foreign partners

4.27 For reasons we have already discussed,[151] we are satisfied that the benefits New Zealand derives from its international intelligence sharing and co-operation arrangements by way of the transfer of technology, skills and expertise is valuable for a country of our size and limited

[151] See above at paragraph 3.42.

resources. New Zealand simply cannot "go it alone" in this globalised world of transnational threats.

4.28 We consider it is in New Zealand's national interest to maintain its collaboration with the Five Eyes partnership for as long as it continues to result in a net benefit for us. However, there are risks and costs associated with this close relationship. Continuation of our involvement depends in part on how much we contribute to research, development and intelligence collection. Close co-operation on operational matters also creates a risk of some loss of independence, both operationally and potentially also in relation to our intelligence, defence and foreign policy settings. The Agencies must keep at the forefront of their minds New Zealand's national interests, which do not and cannot exactly coincide with those of any other country, no matter how friendly or close. The Agencies should continue to collaborate with foreign partners only to the extent compatible with New Zealand's laws and national interests.[152]

4.29 In future there may be other bilateral or multilateral arrangements that New Zealand wishes to enter into. We therefore recommend that the legislation clearly enable the Agencies to co-operate and share intelligence with foreign jurisdictions and international organisations where that is consistent with the purposes of the single Act.

4.30 Any future bilateral or multilateral arrangements entered into with foreign jurisdictions or international organisations should be referred to the Intelligence and Security Committee to be noted. This would help ensure that such arrangements are consistent with the Agencies' obligations to act in accordance with New Zealand law, including human rights standards. It would also enable a level of Parliamentary oversight of the Agencies' international engagement.

4.31 The Agencies also co-operate or share intelligence with foreign jurisdictions and international organisations on an *ad hoc* basis. To provide for such situations, we recommend the responsible Minister formulate standard terms on which such co-operation or sharing should occur and refer them to the Inspector-General for comment. The terms should be consistent with the Agencies' obligations to act in accordance with New Zealand law, including human rights obligations. For example, they should require the Agencies to have regard to any risk of torture or capital punishment. Once finalised, the standard terms should be referred to the Intelligence and Security Committee to be noted.

4.32 We note that the Agencies may not always be in a position to guarantee the methods used by foreign agencies to obtain intelligence that is shared with New Zealand. However, the Agencies should ensure that their own co-operation and sharing activities are compliant with New Zealand law.

[152] On occasion, foreign partners submit requests to the GCSB for assistance with intelligence gathering. We were informed that, in practice, very few of these requests are fulfilled due to constraints in terms of capability, capacity and/or geography. We were assured that requests are only fulfilled where they align with New Zealand's intelligence gathering priorities and fall within the GCSB's statutory mandate.

4.33 The Government should consider including appropriate restrictions (for both formal and *ad hoc* intelligence sharing arrangements) on the circumstances in which information collected by the Agencies about New Zealanders can be shared with foreign jurisdictions and international organisations.

Recommendations

7. The legislation should explicitly enable the Agencies to co-operate and share intelligence with foreign jurisdictions and international organisations.

8. There should be a requirement that this co-operation and sharing be consistent with the purposes of the single Act and the Agencies' obligations to act in accordance with New Zealand law, including human rights obligations.

9. Any future bilateral or multilateral arrangements entered into with foreign jurisdictions or international organisations should be referred to the Intelligence and Security Committee ("ISC") to be noted.

10. The Minister responsible for the Agencies should formulate standard terms for *ad hoc* intelligence co-operation or sharing with foreign jurisdictions and international organisations outside of bilateral or multilateral arrangements. The terms should be consistent with the Agencies' obligations to act in accordance with New Zealand law, including human rights obligations, and be referred to the Inspector-General for comment. Once finalised, the standard terms should be referred to the ISC to be noted.

11. For both formal and *ad hoc* intelligence sharing arrangements, 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.

Centralising intelligence assessments

4.34 Both the National Assessments Bureau ("NAB") and the Combined Threat Assessments Group ("CTAG") have an independent assessment mandate, while operating from within other agencies (NAB is a part of the DPMC and CTAG is within NZSIS). They use similar methods and in some areas their products overlap. To emphasise this independence and encourage more integration of the assessment functions, we recommend the government should review the current placement of CTAG within NZSIS and consider whether it might more appropriately be situated within the NAB.

4.35 We also suggest that the government should consider establishing the NAB as a departmental agency to provide for stronger operational autonomy and to help strengthen its focus on customer-service delivery. Independent assessments are an essential part of a well-functioning intelligence sector: an internal and informal check to ensure the Agencies collect intelligence of relevance to New Zealand's national security priorities. As it is a core element of the NZIC, we recommend the government consider including the functions of the NAB in the single Act. Its function should be to assess and prepare reports relating to New Zealand's national security and economic and international interests, and to provide these reports to relevant decision-makers.

4.36 The NAB should have a clear focus on the recipients of intelligence, especially in relation to its largest user the Ministry of Foreign Affairs and Trade, and make appropriate use of both secret and publicly available information. We encourage the NAB to engage more with the academic profession and public think-tanks, and to explore the possibility of making its assessments publicly available where appropriate. We note that Australia adopted a new National Terrorism Threat Advisory System in late 2015 that includes a purpose of "providing public advice on the nature of the threat and what it means for people".[153] We think the New Zealand government should consider facilitating more public engagement along similar lines.

Recommendations

12. The government should consider including the role and functions of the National Assessments Bureau ("NAB") in the single Act. Its function should be to assess and prepare reports relating to New Zealand's national security and economic and international interests, and to provide these reports to the relevant decision-makers.

13. The government should review the current placement of the Combined Threat Assessments Group within the NZSIS and consider whether it might more appropriately be situated within the NAB.

Better intelligence co-ordination

4.37 New Zealand is fortunate in that it has a relatively small number of agencies involved in the collection and assessment of intelligence. However, historically they have tended to operate separately and remotely from each other, which has meant that finished intelligence products do not always meet the needs of the decision-maker. The 2014 New Zealand Intelligence Community ("NZIC") Performance Improvement Framework report concluded that New

[153] Australian Government "National Terrorism Threat Advisory System", accessed at <http://www.nationalsecurity.gov.au/Securityandyourcommunity/Pages/National-Terrorism-Threat-Advisory-System.aspx>.

Zealand's national security and intelligence priorities were inadequately defined. The report also highlighted the NZIC's lack of understanding of the needs and priorities of decision-makers.[154] The position has improved through the co-location of the GCSB, NZSIS and NAB in a single building. But we suggest a central co-ordination role would provide further momentum to this change and better meet the needs of intelligence users.

4.38 The two secret agencies, the GCSB and NZSIS, are currently separated based on how they collect information (signals intelligence versus human intelligence) and whether they are collecting foreign intelligence or intelligence relating to New Zealand's security. Although these separations may have made sense historically, they are less applicable in the modern technological and threat context where all-source intelligence analysis is necessary to "connect the dots". A central co-ordinator would go a long way towards achieving more efficient use of resources towards commonly identified priorities and activities.

4.39 We suggest that the government consider establishing a National Intelligence and Security Adviser ("NISA") to oversee and co-ordinate the GCSB, NZSIS and NAB. This would facilitate efficiencies in budgetary and operational matters, and a more effective overview of how the wider NZIC's budget is spent. The NISA could be the principal adviser to the government on matters of intelligence and security. He or she could provide leadership and take a whole-of-government view regarding these matters. The NISA could also oversee and direct the implementation of a more flexible budget to ensure the activities of the GCSB, NZSIS, NAB and the wider NZIC are aligned with the government's national security priorities. The government may also wish to consider whether a version of these priorities could be made public.

4.40 We note that jurisdictions overseas have comparable structures. We were advised that Canada, for example, has a National Security Adviser who is the principal adviser to the Canadian Prime Minister on national security matters. He or she also ensures the activities of individual agencies, as well as the activities between agencies, are coherent.

4.41 If the government does not consider it appropriate to establish a NISA at this stage, it might consider whether the Security Intelligence Board (a component board of the Officials' Committee for Domestic and External Security Co-ordination governance system) should take on a similar role.

Role of the Inspector-General of Intelligence and Security

4.42 The changes to the Inspector-General of Intelligence and Security Act in 2013, including an expansion in functions and resources, have substantially strengthened oversight of the Agencies. Although the changes have only been in place for two and a half years, we observed that the Inspector-General is taking a more active role in the oversight of the Agencies.

[154] Peter Bushnell & Garry Wilson *Performance Improvement Framework: Review of the agencies in the core New Zealand Intelligence Community (NZIC)* (State Services Commission, July 2014) at 6.

4.43 Since her appointment in May 2014, the current Inspector-General has initiated a number of inquiries, on her own motion or as a result of specific complaints. They include the release of certain information by the NZSIS under the Official Information Act 1982, the security vetting practices of the NZSIS, the GCSB's activities in the South Pacific, the GCSB's process for determining its foreign intelligence activity, and New Zealand's possible engagement with the USA Central Intelligence Agency's detention and interrogation programme.[155] These inquiries are in addition to the Inspector-General's regular reviews of warrants, access authorisations and internal compliance systems.

4.44 During the course of our review we met with the Inspector-General and the Deputy Inspector-General on a number of occasions to discuss their observations of the Agencies and their activities, and how oversight could be improved. In arriving at our recommendations, we have taken account of their suggestions and relevant submissions received from the public.

Term of appointment

4.45 The legislation allows for the Inspector-General and Deputy Inspector-General each to be appointed for a three-year term.[156] Both can be reappointed for further three-year terms, but in the case of the Inspector-General, he or she can only be reappointed once.[157]

4.46 The work of the Inspector-General requires specialised knowledge and expertise which, to a large extent, can only be acquired while holding the role. To allow time to develop this expertise and to obtain the benefit of it, we recommend extending the initial term of appointment for the Inspector-General to five years. The current reappointment provision should remain.

Independence

4.47 The Inspector-General is New Zealand's main external check on the Agencies. It is crucial that the Inspector-General's independence is maintained to ensure a balanced and politically-neutral assessment of the Agencies' activities.

4.48 Section 4 of the Inspector-General of Intelligence and Security Act 1996 currently frames the role of the Inspector-General as assisting the responsible Minister in the oversight and review of the Agencies, in particular, to ensure that the activities of the Agencies comply with the law, and to independently investigate complaints. There are real strengths to the Inspector-General reporting to the Minister responsible for the Agencies, not least because the Minister is familiar with the detail of the Agencies' work and is in a position to bring about change where needed. However, we think section 4 of the Act conveys the sense that the Inspector-General is an instrument of the Minister and not truly independent.

---

[155] Inspector-General of Intelligence and Security *Annual Report for the year ended 30 June 2015* (21 October 2015).

[156] IGIS Act, s 6(1)(a).

[157] IGIS Act, s 6(1)(b).

4.49 We recommend section 4 be replaced with a clear statutory statement on the Inspector-General's role. The purpose of the Inspector-General should be to ensure the Agencies are acting in compliance with their legislative framework, to independently investigate complaints about the Agencies, and to advise the government and the Intelligence and Security Committee of Parliament on matters relating to the oversight of the Agencies. The addition of a reporting line to the Intelligence and Security Committee is new and we discuss this recommendation further in paragraphs 4.55 to 4.56 below.

Funding

4.50 We were made aware that, although the operating costs of the Inspector-General's office are funded from the Ministry of Justice's non-Ministry appropriations, in practice, funds from the Agencies were diverted to cover the operational costs of the expanded office in 2013. This practice is inconsistent with the independent nature of the Inspector-General's oversight role. We recommend that the Inspector-General's office be funded through an appropriation that is separate from that of the Agencies.

Appointment

4.51 The Inspector-General and Deputy Inspector-General are appointed by the Governor-General on the recommendation of the Prime Minister following consultation with the Intelligence and Security Committee of Parliament.[158] We note that this process is similar in comparable jurisdictions. For example, the Australian Inspector-General is appointed by the Prime Minister in consultation with the Leader of the Opposition.[159] The UK Intelligence Services Commissioner and the Interception of Communications Commissioner are both appointed by the Prime Minister.[160]

4.52 Some submitters expressed concern with the appointment process. We agree that it does not have the appearance of a sufficient degree of independence from the executive. We therefore recommend that the Inspector-General and Deputy Inspector-General be appointed in the same way as the Judicial Conduct Commissioner and members of the Independent Police Conduct Authority: by the Governor-General on the recommendation of the House of Representatives.[161]

Work programme

4.53 Under the current legislation, the Inspector-General is required to submit a work programme to the Minister responsible for the Agencies for approval.[162] As Inspector-General Cheryl Gwyn notes in her 2015 annual report, in practice this does not mean that the Minister

[158] IGIS Act, s 5(2).
[159] Inspector-General of Intelligence and Security Act 1986 (AU), s 6(2) and (3).
[160] Regulation of Investigatory Powers Act 2000 (UK), ss 57(1) and 59(1).
[161] Judicial Conduct Commissioner and Judicial Conduct Panel Act 2004, s 7(2); Independent Police Conduct Authority Act 1988, s 5(1).
[162] IGIS Act, s 11(1)(e).

approves each item on the work programme, especially those inquiries that the Inspector-General initiates on her own motion.[163] Instead, the Minister is informed of the work programme and given the opportunity to make suggestions.[164] We think this is the right approach.

4.54 However, the legislation needs to reflect the true nature of the responsible Minister's involvement and should not leave any room for doubt. The Minister should not approve the Inspector-General's work programme; he or she should receive and comment on a draft. This would remove the executive's potential ability to determine what the Inspector-General can and cannot inquire into. The legislation should also explicitly permit the Inspector-General to make the work programme publicly available.

Inquiring into the Agencies and their activities

4.55 The scope of the Inspector-General's wide inquiry functions should remain as they are. The Inspector-General can inquire into any matter relating to the Agencies' compliance with New Zealand law, including human rights law, and into the propriety of particular activities of the Agencies.[165] We recommend the Inspector-General should be able to initiate both kinds of inquiries at his or her own motion, at the request of the Minister responsible for the Agencies or the Prime Minister, or at the request of the Intelligence and Security Committee.

4.56 The addition of the Intelligence and Security Committee provides an opportunity for representatives from political parties other than those in government to have input into what the Inspector-General inquires into. Where the Inspector-General undertakes an inquiry at the request of the Intelligence and Security Committee, he or she should report back to the Committee on any findings. The Minister's response to the findings should also be made available to the Committee.

4.57 Where an inquiry is initiated at the Inspector-General's own motion or at the request of the responsible Minister or the Prime Minister, we recommend the Inspector-General should be allowed to present his or her findings to the Intelligence and Security Committee with the agreement of the responsible Minister or Prime Minister. The current provision allowing the Minister to provide his or her response to the Committee should remain.[166] This change will help to ensure the Committee remains informed of the Agencies' activities and is better placed to provide effective oversight.

[163] Inspector-General of Intelligence and Security *Annual Report for the year ended 30 June 2015* (21 October 2015) at 10.
[164] Inspector-General of Intelligence and Security *Annual Report for the year ended 30 June 2015* (21 October 2015) at 10.
[165] IGIS Act, s 11(1)(a) and (ca).
[166] IGIS Act, s 25(6)(b). The current provision states: "As soon as practicable after receiving a report from the Inspector-General, the Minister may provide his or her response to the Intelligence and Security Committee."

Inquiring into complaints

4.58 Pursuing a complaint in the New Zealand courts can be a significant financial undertaking and can be particularly challenging if it involves classified information. The Inspector-General performs a vital function as an independent and relatively inexpensive redress mechanism for New Zealand persons[167] and current or former employees of the Agencies who may have been adversely affected by the activities, omissions, practices, policies or procedures of the Agencies.[168]

4.59 People who do not fall into the category of "New Zealand person" might also be affected by particular activities of the Agencies.[169] For example, the NZSIS has the ability to make recommendations in respect of decisions made under the Immigration Act 2009 to issue visas to travel to New Zealand or a permit to remain in or enter New Zealand. We recommend broadening the category of persons who can complain to the Inspector-General so that any person affected by the Agencies' activity will have an opportunity for redress.

4.60 However, we recognise there is a risk of a large number of complaints, including some that it may not be appropriate to respond to (such as complaints by individuals employed by foreign intelligence services intended to surface information about the Agencies' activities). We also think that the right to complain to the Inspector-General should be a right enjoyed by a New Zealand person. The Inspector-General should, therefore, be free to decide whether to inquire into a complaint by a non-New Zealand person and, if an inquiry is conducted, whether to respond to the complainant. The exercise of this discretion should be absolute and should not be subject to challenge by way of judicial review.

Review of warrants, authorisations and compliance systems

4.61 The Inspector-General is required to review annually the effectiveness and appropriateness of the Agencies' compliance procedures that ensure their warrants and authorisations are issued and executed in accordance with the law.[170] In practice, we understand the Inspector-General reviews all warrants and authorisations and selects a few to undertake a comprehensive end-to-end review. This includes reviewing the Agencies' case for gathering the intelligence, what

[167] Section 2 of the IGIS Act defines New Zealand persons as a New Zealand citizen, a person ordinarily resident in New Zealand, an unincorporated body of persons of which more than 50 percent of the members are New Zealand citizens or persons ordinarily resident in New Zealand, or a body corporate which is incorporated in New Zealand. A New Zealand person does not include a subsidiary of any body corporate incorporated outside New Zealand, a company or building society in which over 25 percent of shares or voting power is held by any overseas person(s), or any nominee of an overseas person.
[168] IGIS Act, s 11(1)(b) and (ba).
[169] IGIS Act, s 2.
[170] IGIS Act, s 11(d)(i).

intelligence was collected under the warrant or authorisation and how the intelligence was used.[171]

4.62 We consider this the appropriate level of scrutiny. The legislation should clarify that the Inspector-General's review of authorisations is not merely in relation to procedural matters, but also includes a look behind the face of the authorisation from the point at which the Agencies make a case for the intelligence to its collection, use, storage and destruction.

4.63 This review function will continue under the new authorisation framework we are recommending, with some changes to the Inspector-General's role with regard to tier 3 authorisations (policy statements issued by the Minister responsible for the Agencies). We discuss this further in Chapter 6 below.

New functions

4.64 Collecting open source and secret information is not an end in itself. The Agencies share this information with other operational and policy-making departments in government and with ministers to inform decision-making. In some instances the information will need to flow in the other direction – from relevant government agencies to the GCSB and NZSIS to help identify or investigate national security threats. In Chapter 7 of this report we set out a framework under which these activities should occur. The Inspector-General should monitor and review the operation of these arrangements as part of his or her regular inquiry functions.

4.65 The changes we are proposing to the Agencies' legislative framework are significant. No doubt there will be some unforeseen challenges that arise between now and the next scheduled independent review in five to seven years. In the interim, we think the Inspector-General is best positioned to identify potential concerns or issues with the new framework through his or her regular inspection and inquiry activities. The Inspector-General may wish to include in his or her annual report any comments on the operation of the single Act and any matters arising.

Restrictions on inquiries and reviews

4.66 The legislation presently restricts the Inspector-General's ability to inquire into the Agencies' activities in a minor but fundamental way. The Inspector-General is not permitted to "inquire into any matter that is operationally sensitive, including any matter that relates to intelligence collection and production methods or sources of information" except if it is strictly necessary to perform his or her functions.[172]

---

[171] Joint Committee on the Draft Investigatory Powers Bill "Written Evidence: Draft Investigatory Powers Bill" (IPB0158, 14 January 2016), accessed at <http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-investigatory-powers-bill/publications/?type=Written>.

[172] IGIS Act, s 11(4).

4.67 The wide ambit of the Inspector-General's inquiries means that in most instances he or she will need to look into operationally sensitive matters. In practice we understand neither agency has sought to limit the scope of the Inspector-General's inquiries. But we do not think the Inspector-General should be required by legislation to make a case for necessity every time. Comparable jurisdictions overseas do not restrict their independent oversight entities in this way.[173] We recommend this restriction be removed.

Access to information and premises

4.68 The legislation allows the Inspector-General to access all security records in the custody or control of the Agencies, to enter any premise or place occupied by the Agencies at any reasonable time, and to require any person to produce relevant information.[174] As the Inspector-General indicates in her annual report, she receives the full co-operation of the Agencies and has access to all premises, information and communications technology systems and documents.[175] We are satisfied that the legislation does not unnecessarily inhibit the Inspector-General from conducting her inquiries and reviews.

4.69 However, we note that the provisions enabling the Inspector-General to access information only explicitly apply where the Inspector-General is conducting an inquiry.[176] The Inspector-General's functions are not confined to inquiries; he or she also reviews and audits the activities of the Agencies. We recommend that the legislative references to inquiries should be updated to reflect the wide functions and duties of the role.

Consultation and the Advisory Panel

4.70 The legislation currently allows for the Inspector-General, when inquiring into and reviewing the activities of the Agencies, to consult with the Controller and Auditor-General, an Ombudsman, the Privacy Commissioner, a Human Rights Commissioner and the Independent Police Conduct Authority.[177] The ability to consult enables better co-ordination of oversight across these different areas and should remain.

4.71 The amendments to the Inspector-General of Intelligence and Security Act 1996 in 2013 also established a statutory Advisory Panel to assist the Inspector-General. We understand the Panel provides a useful sounding board for the Inspector-General on matters she may be considering. The two independent members, who were appointed in October 2014, are

[173] For example, the Australian Inspector-General of Intelligence and Security may conduct formal inquiries into any matter arising from a complaint, at the Inspector-General's own initiative, or in response to a ministerial request. The Inspector-General of Intelligence and Security Act 1986 does place some limits on the Inspector-General's functions, but not in relation to operationally sensitive matters.
[174] IGIS Act, ss 20, 21 and 23.
[175] Inspector-General of Intelligence and Security *Annual Report for the year ended 30 June 2015* (21 October 2015) at 13.
[176] See, for example, IGIS Act, ss 20(1) ("the Inspector-General shall, for the purposes of any inquiry") and 21 ("for the purposes of any inquiry under this Act").
[177] IGIS Act, s 12(2) and (3).

security cleared and hold office for an initial term of five years.[178] The Inspector-General is also a member of the Panel.

4.72 The Panel also acts as a check on the Inspector-General role. Panel members can report to the Prime Minister on any matter relating to intelligence and security if the Panel considers that the matter should be drawn to the Prime Minister's attention.[179] We consider this direct reporting line to the Prime Minister is appropriate but is inconsistent with the Inspector-General's own membership of the Panel.[180] We therefore recommend that the Inspector-General should no longer be a member of the Panel.

Protected disclosures (Whistle blowing)

4.73 Under the Protected Disclosures Act 2000, the Inspector-General is the only appropriate authority in New Zealand to whom an employee of the Agencies can disclose information about serious wrongdoing within the Agencies that needs to be investigated.[181] This is because of the highly classified nature of the work and the Inspector-General's wide powers of inquiry into the propriety of the Agencies' activities.

4.74 The Inspector-General of Intelligence and Security Act 1996 also provides in more general terms for employees to bring "any matter to the attention of the Inspector-General". Although it is widely assumed that "any matter" would include "whistle-blowing" events, as the Protected Disclosures Act was enacted four years after the Inspector-General of Intelligence and Security Act it is not entirely clear that this is in fact the case.

4.75 We recommend the government make a minor change to the legislation to clarify that the relevant sections of the Protected Disclosures Act would apply in the event of a protected disclosure by an employee of the Agencies.

Recommendations

14. We recommend section 4 of the Inspector-General of Intelligence and Security Act be replaced with a clear statutory statement on the Inspector-General's role. The purpose of the Inspector-General should be to ensure the Agencies are acting in compliance with their legislative framework, to independently investigate complaints about the Agencies, and to advise the government and the Intelligence and Security Committee of Parliament on matters relating to the oversight of the Agencies.

[178] IGIS Act, s 15C(5) and Inspector-General of Intelligence and Security *Annual Report for the year ended 30 June 2015* (21 October 2015) at 8.
[179] IGIS Act, s 15B(4).
[180] IGIS Act, s 15C(1)(b).
[181] Protected Disclosures Act 2000, s 12(b).

15. In order to ensure the independence of the Inspector-General, he or she should be appointed by the Governor-General on the recommendation of the House of Representatives and the Inspector-General's Office should be funded through an appropriation that is separate from that of the Agencies.

16. The Inspector-General should be appointed for an initial term of five years to allow sufficient time to build expertise in the technical and specialised work of the Agencies. The current reappointment provision should continue (that is, the ability to be reappointed for one further three-year term).

17. The Minister responsible for the Agencies should receive and comment on (but not approve) the Inspector-General's draft work programme. The legislation should permit the work programme to be made publicly available.

18. Where the Inspector-General undertakes an inquiry at the request of the Intelligence and Security Committee, he or she should report back to the Committee on any findings. The Minister's response to the findings should be made available to the Committee.

19. Where the inquiry is initiated at the Inspector-General's own motion or at the request of the responsible Minister or the Prime Minister, the Inspector-General should be allowed, with the agreement of the responsible Minister or Prime Minister, to present his or her findings to the Intelligence and Security Committee. The current provision allowing the Minister to provide his or her response to the Committee should remain.

20. The category of persons who can complain to the Inspector-General should be extended beyond New Zealand persons. The Inspector-General should have discretion as to whether to inquire into any complaint by a non-New Zealand person. The exercise of this discretion should not be subject to a judicial review challenge.

21. The legislation should clarify that the Inspector-General's review of authorisations is not merely in relation to procedural matters but is a comprehensive look behind the face of the authorisation. This includes reviewing the Agencies' case for an authorisation and how the authorisation was implemented.

22. The current restriction on the Inspector-General inquiring into operationally sensitive matters unless strictly necessary to perform his or her functions should be removed.

23. In order to preserve the independent nature of its role, the Advisory Panel should no longer include the Inspector-General.

24. The legislation should be amended to clarify that the relevant sections of the Protected Disclosures Act apply in the event of a protected disclosure by an employee of the Agencies.

Role of the Intelligence and Security Committee

Membership of the Committee

4.76 The ISC is currently a statutory committee made up of five members including the Prime Minister and the Leader of the Opposition. Some submitters suggested the ISC be established as a parliamentary select committee. Membership on select committees is broader than the ISC and proportional to party membership in Parliament. Unlike the ISC, there is also a presumption that select committee hearings are open to the public, unless the evidence is private or secret.

4.77 Because the ISC frequently deals with highly sensitive secret information, we recognise that there needs to be some restrictions on how it conducts its business and on its members that are not characteristic of normal select committees. Therefore, we recommend it remain a statutory committee for now and that the government keep this issue under consideration in future reviews.

4.78 However, we recommend increasing the maximum size of the Committee to allow for more flexibility in representation. The membership of the Committee should be increased to allow for a minimum of five and a maximum of seven members. The appropriate number should be determined by the Prime Minister after consultation with the Leader of the Opposition. The members should also be nominated by the Prime Minister after consultation with the Leader of the Opposition and subsequently be endorsed by the House of Representatives. We note that it is a convention in New Zealand and similar foreign jurisdictions to nominate senior members of Parliament to such committees. In keeping with this increased flexibility, we also recommend that the Committee elect its own chairperson. This would not necessarily be the Prime Minister, who is the current chairperson.

New functions

4.79 In keeping with our expanded view of the composition of the core NZIC, the government should consider extending the ISC's examination and review functions to the NAB. The ISC

could examine the policy, administration, and expenditure of the NAB and conduct an annual financial review of the performance of the NAB.

4.80 Complementing our recommendation in paragraphs 4.55 and 4.56 above to allow the Inspector-General to report to the ISC, we recommend the ISC be authorised to request (but not require) the Inspector-General 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.

4.81 One of the functions of the ISC is to consider any Bill in relation to the Agencies referred to it by Parliament.[182] This is subject to some restrictions: when considering proposed legislation, the ISC cannot inquire into operationally sensitive matters or any matter that is under the jurisdiction of the Inspector-General.[183] The ISC is also required to conduct its proceedings in private unless members decide otherwise.[184] By contrast, as mentioned above, there is a presumption that select committee hearings on proposed legislation are open to the public, unless the evidence is private or secret. Select committee membership is also broader and the minister responsible for the relevant Bill does not sit as a member of the subject select committee considering it.

4.82 We do not think the ISC should replace the role of a subject select committee when considering proposed legislation in relation to the Agencies. We think the government should in general refer proposed legislation relating to intelligence and security matters to an appropriate subject select committee. However, if there is classified material that needs to be considered in the context of the proposed legislation, the government should consider placing this before the ISC. The ISC would then report its conclusions on that material to the select committee. This process would allow all relevant information to be taken into account, while also helping the ISC to build its knowledge of intelligence and security matters.

Recommendations

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

26. The members of the ISC should be nominated by the Prime Minister after consultation with the Leader of the Opposition and subsequently be endorsed by the House of Representatives. The Committee should also elect its own chairperson.

[182] ISC Act, s 6(1)(b).
[183] ISC Act, s 6(2)(a) and (b).
[184] ISC Act, s 12(2).

27. The government should consider extending the ISC's examination and review functions to the National Assessments Bureau.

28. The ISC should be authorised to request (but not require) the Inspector-General 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.

29. The government should in general refer proposed legislation relating to intelligence and security matters to an appropriate select committee. It should consider referring specific classified material in the context of proposed legislation to the ISC, which would then report its conclusions to the select committee.

Chapter 5: What should the Agencies do?

Role of the intelligence and security agencies

5.1 A fundamental question for this review is what the proper role of New Zealand's intelligence and security agencies should be, as this will guide consideration of how they should operate. This Chapter considers what functions the Agencies should have and the purposes for which those functions should be carried out. We recommend that the Agencies have shared objectives and functions to allow them to work together more effectively.

5.2 Under the current legislation, the Agencies are responsible for contributing to the protection and advancement of a broad range of interests – from protecting against specific security threats such as terrorism and cyber attacks through to advancing New Zealand's economic and international interests.

5.3 The Agencies have separate functions and different ways of operating due to their distinct histories. As noted earlier in this report, the traditional separation between the use of signals capability and human sources is reflected in the Agencies' governing legislation. For example, the Agencies are subject to different warranting requirements, which hampers their ability to work together effectively to protect against security threats. This issue is discussed further in Chapter 6.

5.4 The increasing use of technology and blurring of national boundaries have changed the nature of security threats and therefore the means by which they need to be countered. For example, terrorist groups are becoming more sophisticated in their use of technology. There is an increasing need for intelligence and security agencies to respond to this challenge by working together to share their expertise. While human sources often provide initial leads by detecting suspicious behaviour and alerting authorities, signals expertise is sometimes necessary to help establish the identity of potential wrongdoers. Signals expertise can also assist human sources to assess a target's intentions by, for example, monitoring their online activities.

The NZSIS' current objectives and functions

5.5 The NZSIS collects intelligence for the purpose of protecting against threats to the state, whether those threats originate from within or outside New Zealand. It specialises in human intelligence (HUMINT) activities, which involve the use of human sources to gather intelligence. In some circumstances, it requests technical signals intelligence (SIGINT) assistance from the GCSB.

5.6 The NZSIS does not have any specific objectives set out in legislation. Its intelligence function is to obtain, correlate and evaluate intelligence relevant to security, and communicate it to any person in the interests of security. "Security" is defined in the Act as:[185]

- protecting New Zealand from espionage, sabotage and subversion
- identifying foreign capabilities, intentions or activities within or relating to New Zealand that impact on New Zealand's international or economic well-being
- protecting New Zealand from activities within or relating to New Zealand that:
  - are influenced by foreign persons or organisations
  - are clandestine, deceptive or threaten the safety of any person, and
  - adversely impact New Zealand's international or economic well-being.
- preventing terrorist acts and any acts related to the carrying out or facilitating of terrorist acts.

5.7 The NZSIS also has functions relating to protective security. "Protective security" encompasses the protection of information, people and assets against security threats (for example, vetting government employees who need security clearance to access sensitive information). This function is discussed further below.

The GCSB's current objectives and functions

5.8 The GCSB collects foreign intelligence. It also contributes to domestic security by using its technical signals intelligence expertise to protect New Zealand's cyber security and assist other specified government agencies to carry out their functions where those agencies have the mandate, but not the capacity or capability, to do so themselves.

5.9 The GCSB's objectives are to contribute to New Zealand's national security, international relations and well-being, and economic well-being. It has a broader role than the NZSIS in that it exists for the purposes of advancing New Zealand's interests, as well as protecting against threats to those interests.

5.10 Its functions are:[186]

- gathering and analysing intelligence about:
  - the capabilities, intentions and activities of foreign persons or organisations, in accordance with the government's requirements, and

[185] NZSIS Act, s 2(1) (definition of "security").
[186] GCSB Act, ss 8A, 8B and 8C.

- information infrastructures[187]

- providing intelligence, and any analysis of it, to the Minister responsible for the GCSB and any person authorised by the Minister to receive it

- co-operating with and assisting public authorities (whether in New Zealand or overseas) and any other entity authorised by the Minister in regard to the protection of communications and information infrastructures (for example, protecting against cyber attacks), and

- co-operating with and assisting the NZSIS, Police and NZDF to carry out their lawful functions, subject to any restrictions that apply to those agencies.

Collecting information

5.11 The primary function of both agencies is to collect intelligence. The NZSIS primarily collects intelligence for the purpose of protecting against threats to New Zealand, whether the source of the threat is domestic or foreign. The GCSB primarily collects foreign intelligence, but for a broader range of purposes than the NZSIS. This is reflected in its objectives, which include contributing to New Zealand's international and economic well-being in addition to national security.

5.12 While GCSB's collection function is broader in scope than NZSIS's, in practice it is more constrained in terms of when or how it can collect information about New Zealanders, as discussed below.

Restriction on the GCSB intercepting New Zealanders' private communications

5.13 The scope of the GCSB's intelligence collection activities is limited by section 14 of the GCSB Act. Section 14 prohibits the GSCB from doing anything for the purpose of intercepting the private communications of New Zealand citizens or permanent residents, unless one of the limitations applies (discussed below).

5.14 Section 14 means the GCSB cannot generally collect intelligence about New Zealanders, even if it would otherwise be relevant to the performance of the GCSB's foreign intelligence function. However, the protection offered by section 14 is not as comprehensive as is commonly understood. There are a range of somewhat confusing limitations on its scope. The section 14 restriction:

- only applies where the GCSB is performing its intelligence function, not its cyber security and assistance functions

[187] GCSB Act, s 4: **information infrastructure** includes electromagnetic emissions, communications systems and networks, information technology systems and networks, and any communications contained in or relating to them.

- does not expressly cover New Zealand organisations (only citizens and permanent residents)
- does not apply to the extent that a New Zealander falls within the definition of a "foreign person" or "foreign organisation" (known as the "agent of a foreign power" exception)
- only applies to communications that are "private", and
- does not prevent incidental interception of New Zealanders' communications.

5.15 Some of these limitations are discussed in further detail below.

Private communications

5.16 The section 14 restriction on intercepting New Zealanders' communications only applies to communications that are "private", as defined in section 4 of the Act:

> Private communication–
>
> (a) means a communication between 2 or more parties made under circumstances that may reasonably be taken to indicate that any party to the communication desires it to be confined to the parties to the communication; but
>
> (b) does not include a communication occurring in circumstances in which any party ought reasonably to expect that the communication may be intercepted by some other person not having the express or implied consent of any party to do so.

5.17 This definition is based on (and is very similar to) the definition of "private communication" in the Crimes Act 1961.[188] The Crimes Act makes it an offence to intercept private communications by means of an interception device.[189] More recently, the Crimes Act definition has also been incorporated into the Search and Surveillance Act 2012 provisions on surveillance device warrants for law enforcement purposes.[190]

5.18 The term "private communication" was introduced to section 14 of the GCSB Act when it was amended in 2013. Prior to the amendment, section 14 simply referred to the "communications" (broadly defined)[191] of a New Zealand citizen or permanent resident. It also applied to all of the GCSB's activities, not just its intelligence function.

5.19 A range of submitters on the 2013 Bill to amend the GCSB Act opposed the use of the term "private communication". Criticisms included that:

---

[188] Crimes Act 1961, ss 216A and 216B.
[189] Crimes Act, s 216B.
[190] Search and Surveillance Act 2012, ss 3 and 46.
[191] GCSB Act, s 4: **communication** includes signs, signals, impulses, writing, images, sounds, information or data that a person or machine produces, sends, receives, processes, or holds in any medium.

- it was circular, because under paragraph (b) of the definition the privacy of a communication depends on the likelihood of interception occurring, and
- it may not cover metadata, because it requires the communication to be between two or more parties (which does not contemplate machine-produced data).

5.20 These issues with the definition of "private communication" have continued to attract media attention since the 2013 amendments.[192] The Law Commission has also criticised the circularity of the definition of "private communication" in the context of the Crimes Act, noting "the likelihood of a privacy encroachment (through interception) should not be determinative of the application of the privacy protection".[193] The Commission recommended changing the definition to a "reasonable expectation of privacy" test. The government is still considering this recommendation.

5.21 Despite these criticisms, when the 2013 amendments were before Parliament, the Intelligence and Security Committee recommended keeping the term in the Bill, saying it "had acquired a degree of orthodoxy" and was preferable to "the more problematic and imprecise phrase 'communication of a person'", which had no developed jurisprudence.[194]

5.22 We note our terms of reference require us to consider the definition of "private communication". However, as we discuss below, we recommend that section 14 should be removed and that protection should be provided for New Zealanders in a different way. As such, there will no longer be any need for a definition of "private communication" in the Act. We therefore do not make any specific recommendations about the definition.

Incidental interception of New Zealanders' communications

5.23 Section 14 only prevents actions *for the purpose of* intercepting private communications of New Zealanders. The GCSB does not breach the law if it obtains intelligence about New Zealanders in the course of collecting foreign intelligence and is not deliberately targeting their communications.

5.24 The Act also explicitly provides for "incidentally obtained intelligence", which is intelligence acquired in the course of gathering foreign intelligence that is not itself foreign intelligence. Incidental interception is unavoidable given the nature of signals intelligence. As discussed in Chapter 3, it is often not possible for the GCSB to identify specific communications of interest and whether they relate to New Zealanders until a broader set of communications (most of which will never be examined by an analyst) has been intercepted and filtered.

---

[192] Denis Tegg "Loophole that legalises official snooping" (New Zealand Herald, 15 August 2014), accessed at <http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11308965>.
[193] Law Commission *Invasion of Privacy: Penalties and Remedies* (NZLC R 113, January 2010) at [3.66].
[194] Government Communications and Security Bureau and Related Legislation Bill (109–2) (Select Committee report) at 3.

5.25 Any incidentally obtained intelligence can only be retained or disclosed in accordance with the Act.[195] However, these grounds for retention are quite broad. Communications intercepted under a warrant, access authorisation or director authorisation[196] (incidentally or otherwise) must be destroyed *unless* they are relevant to the GCSB's objectives or its intelligence or cyber security functions.[197] On the face of it, this would allow the GCSB to retain any incidentally obtained intelligence that is relevant to New Zealand's national security or international and economic well-being,[198] or to the security of communications and information infrastructures.[199]

5.26 There is also an exception to the general requirement in the Act to destroy information irrelevant to the GCSB's objectives and functions. Incidentally obtained intelligence may be retained and communicated to a relevant public authority for the purposes of:[200]

- preventing or detecting serious crime in New Zealand or overseas
- preventing or responding to threats to human life, or
- identifying, preventing or responding to threats or potential threats to the security or defence of New Zealand or another country.

5.27 We note that the GCSB currently takes a conservative approach to incidentally obtained intelligence. Under its nationality policy, such information must be destroyed unless one of the grounds for communicating it to another authority applies (for example, if the information is relevant to preventing or detecting serious crime). Incidentally obtained intelligence about New Zealanders is not retained on the basis that it is relevant to the GCSB's objectives and functions.[201] However, on the face of it the legislation appears to allow for this.[202]

The "agent of a foreign power" exception

5.28 The GCSB can intercept the private communications of a New Zealand citizen or permanent resident (with an appropriate warrant or authorisation) if they fall within the definition of a

---

[195] GCSB Act, ss 14(2), 23 and 25.
[196] Section 16 of the GCSB Act allows the Director of GCSB to authorise interception of communications using an interception device where the device is not connected to an information infrastructure or installed in a place to intercept communications in that place (eg, interception of satellite and radio transmissions).
[197] GCSB Act, ss 14(2) and 23.
[198] GCSB Act, s 7 (objectives).
[199] GCSB Act, s 8A.
[200] GCSB Act, s 25.
[201] Government Communications Security Bureau *Nationality Policy* at [19], accessed at <http://www.gcsb.govt.nz/assets/GCSB-Documents/GCSB-Nationality-Policy.pdf>; Government Communications Security Bureau *Incidental Intelligence Policy,* accessed at <http://www.gcsb.govt.nz/assets/GCSB-Documents/Incidental-Intelligence-Policy.pdf>.
[202] Section 14(2) explicitly states that incidentally obtained intelligence "must not be retained or disclosed *except in accordance with sections 23 and 25*". Section 25 provides for the retention of information relevant to GCSB's objectives and functions.

"foreign person" or "foreign organisation".[203] These definitions capture a person acting in his or her capacity as an agent or representative of a foreign person or organisation.[204] This is commonly referred to as the "agent of a foreign power" exception.

5.29 Although the legislation does not require it, the GCSB's policy is to treat a New Zealander as an agent of a foreign power only after obtaining a formal authorisation from its Director.[205]

5.30 The definition of "foreign organisation" is quite broad. For example, it covers companies operating in New Zealand that are subsidiaries of foreign-owned companies, many of which are staffed largely by New Zealanders. It also covers international organisations, such as aid organisations.

5.31 We understand that the agent of a foreign power exception has proved difficult for the GCSB to apply. A lead that the GCSB receives about a person may be general (for example, they may simply be alerted to the fact that a person who appears to be a New Zealander is located in an area occupied by a terrorist organisation). That information may be insufficient to establish whether the person is an agent or representative of a foreign person or organisation. In that situation, the GCSB has no ability to investigate further, not even to establish the nationality of the person in question. While it could in these circumstances refer the lead to the NZSIS, the NZSIS may not have the means to pursue it.

Assisting other government agencies

5.32 Unlike the GCSB, the NZSIS does not have a specific statutory function of assisting other entities. It can co-operate with other public authorities, both in New Zealand and abroad, but only to the extent practicable and necessary to assist the NZSIS in the performance of its own functions.[206]

5.33 We consider this is too restrictive, as we have identified situations in which the use of human sources may assist the GCSB, Police and Defence in carrying out their functions. The Police may need assistance to install surveillance devices (for example, to gather evidence about a suspected child sexual exploitation operation). The NZSIS Act does not currently allow for this kind of assistance.

5.34 NZSIS officers may also be deployed with the NZDF in some situations. They collect intelligence that can help to ensure the safety of troops and inform strategic decisions in the field. The NZSIS already provides this type of assistance to the NZDF on the basis that this falls within its security intelligence function. However, we consider this is an important role that should be more explicit in the legislation.

---

[203] GCSB Act, s 14(1).
[204] GCSB Act, s 4 (definitions of "foreign person" and "foreign organisation").
[205] Government Communications Security Bureau *Nationality Policy* at [13], accessed at <http://www.gcsb.govt.nz/assets/GCSB-Documents/GCSB-Nationality-Policy.pdf>.
[206] NZSIS Act, s 4(1)(c).

5.35 As discussed below, we recommend that both agencies should have an assistance function.

Protective security

5.36 Both agencies have functions relating to protective security. Protective security focuses on ensuring the security of people, information and physical resources, both in New Zealand and overseas. The Agencies' protective security services are provided both to government (for example, the NZSIS vets government employees who need security clearance to access sensitive information) and to private sector entities whose activities or infrastructure are important to New Zealand (for example, the GCSB's cyber security role).

5.37 The NZSIS's protective security functions include:[207]

- advising Ministers, other government departments, public authorities and any other person the Director of Security considers should receive advice, on protective measures relevant to security
- conducting inquiries into whether particular individuals should be granted security clearances and making recommendations based on those inquiries, and
- making recommendations in respect of matters to be decided under the Citizenship Act 1977 or the Immigration Act 2009 as they relate to security.

5.38 The GCSB's protective security functions include:[208]

- co-operating with, advising and assisting public authorities (including overseas authorities) and any other entity authorised by the Minister on the protection, security and integrity of:
  - communications (including those processed, stored or communicated through information infrastructures)
  - information infrastructures of importance to the New Zealand government
- doing anything necessary or desirable to protect the security and integrity of the communications and infrastructures referred to above, including identifying and responding to threats or potential threats to those communications and infrastructures, and
- reporting on the above functions and providing intelligence gathered, and analysis of it to the Minister and any person or office holder (whether in New Zealand or overseas) who is authorised by the Minister to receive it.

[207] NZSIS Act, s 4.
[208] GCSB Act, s 8A.

What should the Agencies' objectives be?

5.39 We consider that the Agencies' objectives should be sufficiently broad to enable them to perform their role of assisting the government to protect New Zealand's national security and advance its economic and international interests in a continually changing international environment. This flexibility is necessary in order to achieve the purpose of the proposed single Act, which is to protect New Zealand as a free, open and democratic society.

5.40 Over the course of this review, we have not identified any inadequacies with the current scope of the Agencies' combined objectives. They are comprehensive and appear sufficiently broad to enable the government to respond to new threats that may arise in future. However, we do not see any compelling reason for continuing the current distinction between the two Agencies' objectives. In our view, they both exist in order to assist the government in protecting and advancing New Zealand's interests, and their objectives should reflect that.

5.41 Currently, the NZSIS can only perform its functions in so far as they relate to "security". Unlike the GCSB, the NZSIS does not have a role in contributing to the advancement of New Zealand's economic or international well-being more broadly. We consider that both agencies should be able to contribute to these objectives to the extent that they fall within the intelligence priorities set by the government. This would broaden the NZSIS's potential sphere of operation. However, any concern about the impact on individuals would be addressed by limiting the objectives for which the Agencies can collect information for the purpose of targeting New Zealanders, as discussed below.

5.42 The Agencies should continue to be required to carry out their functions in accordance with the government's priorities. This is an important safeguard to ensure the Agencies carry out their activities in accordance with agreed national security priorities. As we have suggested in Chapter 4 (see paragraph 4.39), the Government should also consider making a version of the national security priorities public because of their importance in determining the Agencies' activities.

5.43 We recommend that the Agencies should have common objectives. They should carry out their intelligence collection functions in pursuit of those objectives only. These objectives should be to contribute to:

- the protection of New Zealand's national security, including its economic security and the maintenance of international security (which can indirectly affect domestic security)[209]
- New Zealand's international relations and well-being, and
- New Zealand's economic well-being.

[209] We recommend defining national security in the legislation, as discussed in paragraphs 5.78–5.85 below.

5.44 As the proposed objectives are broad and enabling, we also recommend safeguards to ensure the Agencies carry out their activities lawfully, appropriately and in accordance with the national security priorities set by the government. These safeguards include:

- maintaining the current separation of intelligence collection from decision-making and enforcement (discussed under the heading "Specialist collection agencies" below)
- limiting the circumstances in which the Agencies can collect information about New Zealanders (discussed under the heading "Protecting New Zealanders" below), and
- introducing a comprehensive authorisation framework covering the full range of the Agencies' activities (discussed in Chapter 6).

Recommendations

30. The Agencies should have common objectives and should carry out their functions in pursuit of those objectives only. The objectives should be to contribute to:
    - the protection of New Zealand's national security, including its economic security and the maintenance of international security (which can indirectly affect domestic security)
    - New Zealand's international relations and well-being, and
    - New Zealand's economic well-being.

What should the Agencies' functions be?

Specialist collection agencies

5.45 The Agencies' primary role is to use their specialist capabilities to collect intelligence, including secret intelligence, and to make it available to those individuals and agencies whose role it is to act on it. With the exception of the GCSB's cyber security role, which includes taking steps to protect information systems where necessary, the Agencies do not have any enforcement powers or the mandate to take action to mitigate or disrupt threats from occurring.

5.46 Separating the collection of intelligence from decision-making and enforcement is an important check on the power of the state over individuals. This review has not identified any reason why the distinction should be blurred at this stage.

5.47 We consider that the Agencies' role as specialist collection agencies should continue. This involves collecting, analysing, sharing and providing advice on intelligence. Other government agencies should remain responsible for making decisions and taking action on the basis of the

intelligence they receive from the Agencies and other sources. While we note that intelligence agencies in other jurisdictions have a role in carrying out activities for purposes other than collection if directed,[210] we do not consider that this function is necessary in the New Zealand context.

5.48 However, we do consider the GCSB's role in proactively protecting information systems from cyber attacks is appropriate and should continue. This is because its highly specialised technical expertise is needed to take the necessary protective action, for example enabling computer systems to detect malicious internet traffic and prevent it from reaching its destination. Any duplication of this skill and the highly specialised equipment it requires should be minimised to avoid unnecessary expense. We note that equivalent agencies in other comparable jurisdictions perform a similar function.

Common functions

5.49 As outlined earlier in this report, the Agencies' functions and ways of operating are largely the result of their separate origins. Their governing legislation reflects this and has not kept pace with technology and the changing nature of threats to New Zealand's security and interests. This is particularly the case with the legislation governing the NZSIS, which dates back to 1969 and has not been subject to any recent review similar to that of the GCSB legislation in 2013. The outdated legislation hampers the Agencies' ability to work together to protect against threats to security.

5.50 We consider that in line with the common objectives we are proposing, the Agencies should have common functions. Along with our recommendations for a single Act and a common authorisation framework, this should go a long way toward allowing the Agencies' unique capabilities to be used more effectively and efficiently.

5.51 These common functions should include:

- collecting and analysing intelligence in accordance with the government's priorities
- providing protective security advice and assistance to other entities, and
- co-operating with and assisting other specified government agencies.

Collecting intelligence

5.52 The Agencies' intelligence collection function should include:

- collecting and analysing intelligence in accordance with the government's priorities

[210] For example, section 6 (1)(e) of the Intelligence Services Act 2001 (AU) provides that one of the functions of ASIS is "to undertake such other activities as the responsible Minister directs relating to the capabilities, intentions or activities of people or organisations outside Australia".

- providing any intelligence collected and any analysis of the intelligence to:
    - the Minister
    - the National Assessments Bureau for assessment, and
    - any person, office holder, entity or class of persons, office holders or entities (whether in New Zealand or overseas) authorised by the Minister to receive the intelligence.

Protective security

5.53 The Agencies' protective security function should include co-operating with, advising and assisting public authorities (including overseas authorities) and any other person, office holder, entity or class of persons, office holders or entities authorised by the Minister on protective security matters.

5.54 "Protective security" should be defined to include the Agencies' current functions in relation to the protection of information, people and assets against security threats (for example, cyber security, information assurance and vetting).

5.55 We support the government's proposal to create a national Computer Emergency Response Team (CERT),[211] as outlined in the refreshed Cyber Security Strategy released on 10 December 2015.[212] A CERT will provide a single entry point for individuals and businesses to seek assistance and advice on how to protect themselves from cyber intrusions. This should go a long way towards addressing concerns raised in public submissions that the GCSB is not the best agency to protect New Zealanders from cyber attacks due to its conflicting role as an intelligence gatherer. We consider that a CERT will complement the GCSB's continuing role in using its specialist cyber expertise to protect New Zealand's critical infrastructure from the risk of significant harm caused by sophisticated cyber attacks.

Assisting other government agencies

5.56 The Agencies' assistance function should include:

- co-operating with each other, and with Police and NZDF, and assisting those agencies to carry out their functions in accordance with their governing legislation, and

[211] CERT was previously an acronym for "Computer Emergency Response Team'. New Zealand's Cyber Security Strategy 2015 notes that since 1997, 'CERT' has been a registered trademark owned by Carnegie Mellon University and is no longer used as an acronym. New Zealand is requesting permission to use the CERT trademark.

[212] New Zealand's Cyber Security Strategy "Ensuring New Zealand is secure, resilient and prosperous online" (Department of the Prime Minister and Cabinet, December 2015), accessed at <http://www.dpmc.govt.nz/dpmc/publications/nzcss>.

- co-operating with and assisting any other government agency or entity (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.

5.57 The NZSIS does not currently have an assistance function. While the circumstances in which the NZSIS will need to assist others are likely to be less common than for the GCSB, in principle we consider Police and NZDF should be able to use the NZSIS's specialist capabilities if and when they are needed. We note that the NZSIS does already assist Police, NZDF and the GCSB where it falls within their security intelligence function. In our view, it would be preferable for the legislation to provide explicitly for the NZSIS to assist Police, NZDF and the GCSB in the performance of those agencies' functions. These agencies (in particular the NZSIS and Police due to their close working relationship and the importance of separating intelligence collection from enforcement), should develop joint operating protocols governing how they work together.

5.58 When assisting another agency, the Agencies should be required to act within the scope of that agency's statutory powers and any relevant warrants. This is currently the case under the GCSB's assistance function.

5.59 We did consider whether to allow for broader use of the Agencies' capabilities, particularly the GCSB's signals intelligence methods, when assisting Police to carry out their lawful functions. Currently the GCSB can only use its capabilities in a limited way when assisting Police due to the specific nature of Police warrants. There is some merit in allowing the Police access to the specific skills and capabilities of the Agencies. However, if the Agencies were able to use their capabilities in a way that went beyond the current scope of Police warrants, that would in effect amount to an expansion of Police powers. Any such expansion would need to be considered in the context of the Search and Surveillance Act 2012, which deals with Police warrants and powers. It should not occur through a back door. We are therefore of the view that this issue would be more appropriately considered as part of a review of the Search and Surveillance Act, which is due to commence in 2016.[213]

5.60 We also observe that the Agencies can already use their own powers and capabilities to collect intelligence relating to serious crime where it is relevant to national security or, in the case of the GCSB, New Zealand's economic and international well-being. This may encompass crimes such as terrorism and transnational crimes impacting on New Zealand's interests (for example, money laundering and drug trafficking). It is only where the crime being investigated falls outside those areas that the assistance function would need to be engaged.

[213] Search and Surveillance Act 2012, s 357. The review will be carried out jointly by the Law Commission and the Ministry of Justice, and must commence by 30 June 2016.

Recommendations

31. The Agencies should have common functions. These common functions should include:

Collecting intelligence

- Collecting and analysing intelligence in accordance with the government's priorities.
- Providing any intelligence collected and any analysis of the intelligence to:
  - the Minister
  - the National Assessments Bureau for assessment, and
  - any person, office holder, entity or class of persons, office holders or entities (whether in New Zealand or overseas) authorised by the Minister to receive the intelligence.

Protective security

- Co-operating with, advising and assisting public authorities (including overseas authorities) and any other person, office holder, entity or class of persons, office holders or entities authorised by the Minister on protective security matters.
- "Protective security" should be defined to include the Agencies' current functions in relation to the protection of information, people and assets against security threats (for example, cyber security, information assurance and vetting).

Assisting other government agencies

- Co-operating with each other, and with Police and the Defence Force, and assisting those agencies to carry out their functions in accordance with their governing legislation, and
- Co-operating with and assisting any other government agency or entity (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.

32. The Agencies should, as a matter of practice, develop joint operating protocols with other government agencies (for example, between the NZSIS and Police).

Protecting New Zealanders

5.61 The government, as part of its role in protecting national security, has an obligation to protect the rights of its citizens and permanent residents. We consider this is appropriately achieved by applying a higher threshold for authorising activities directed at New Zealanders than in respect of foreign citizens, whose own states are responsible for protecting their rights.

5.62 Some submitters argued that the same protections should apply to everyone because human rights apply internationally. We agree that governments should consider human rights when taking an action that affects an individual, regardless of nationality. For example, compliance with New Zealand's human rights obligations would be a relevant consideration when deciding whether to issue an authorisation to collect foreign intelligence. However, we consider that the government should afford greater protection to New Zealanders because citizenship and residence affords certain privileges.

Threats to national security

5.63 We recommend that the Agencies should be able to undertake activity for the purpose of targeting New Zealand citizens and permanent residents, and organisations with their centre of management and control in New Zealand, where it can be demonstrated that it is necessary in order to protect national security. They should only be able to carry out activities for the wider purposes of contributing to or advancing New Zealand's economic or international well-being where those activities target foreign persons and organisations.[214] For the sake of clarity, we note this should not prevent the Agencies from targeting a New Zealander with more than one objective, as long as the activity is necessary to protect national security. For example, protecting against serious threats to New Zealand's cyber security contributes to New Zealand's economic well-being, as well as national security.

5.64 In general, we do not consider it to be appropriate for New Zealanders to be the subject of the Agencies' intrusive powers for the broader purposes of advancing New Zealand's economic and international interests. Such an approach would be inconsistent with New Zealand's status as a free and democratic country and would entail an unjustifiable intrusion on New Zealanders' privacy and liberty. We note that the UK and Australia take a similar approach of limiting targeting of citizens, permanent residents or (in the case of the UK) persons inside the country to situations where there are national security implications.[215]

5.65 This is a significant limitation on the Agencies' ability to target New Zealanders. The NZSIS can currently obtain domestic intelligence warrants to target New Zealanders for the purpose of protecting against adverse impacts on New Zealand's economic or international well-being.[216]

---

[214] We discuss the definitions of "foreign person" and "foreign organisation" in paragraphs 5.73 to 5.77 below.
[215] Regulation of Investigatory Powers Act 2000 (UK), s 5(5) (protection is afforded to people inside the British Islands, rather than citizens and permanent residents) and Telecommunications (Interception and Access) Act 1979 (AU), s 11D(5).
[216] NZSIS Act, ss 2 (definition of "security") and 4A.

The GCSB, although subject to restrictions on intercepting the private communications of New Zealanders, can target New Zealanders for economic or international well-being purposes if they fall within the definitions of "foreign person" or "foreign organisation". Those definitions are currently quite broad and we recommend that they be reviewed, as we discuss below.[217]

Intercepting private communications

5.66 Currently, the NZSIS may collect information about New Zealanders in carrying out its functions. The GCSB, being primarily a foreign intelligence agency, may only collect intelligence about New Zealand citizens and permanent residents for the purpose of protecting cyber security or assisting domestic agencies (the NZSIS, Police and NZDF) to carry out their functions (unless they fall within the definition of "foreign person" or "foreign organisation", in which case they can be targeted for foreign intelligence purposes).

5.67 Section 14 of the GCSB Act prohibits the GCSB from doing anything for the purpose of intercepting the private communications of New Zealand citizens and permanent residents when carrying out its function of collecting intelligence. We consider that this restriction, while intended to protect New Zealanders, is a blunt tool and does not provide the best means of protecting individual rights in situations where there is a threat to national security. As we have explained above,[218] it does not provide the comprehensive protection to New Zealanders that it might appear. The myriad of difficult-to-interpret limitations on the scope of section 14 contribute, in our view, to a lack of clarity for New Zealanders about what privacy protections they are entitled to.

5.68 Difficulties in interpreting section 14 have also led to the GCSB taking an overly cautious approach and discontinuing valuable lines of investigation. We have learnt of situations where the GCSB was unable to collect potentially important intelligence because of a possible domestic link, even where the overall purpose of the investigation is to collect foreign intelligence. For example, the GCSB cannot investigate a New Zealander who is in contact with a foreign intelligence service to find out about an operation that threatens New Zealanders or New Zealand's interests.

5.69 The GCSB has limited ability to assist in situations where a New Zealander's safety is at risk. For example, if a New Zealander is taken hostage in a foreign country, there may be little or no information about the hostage-takers. The most effective way to locate the hostage may be by analysing the hostage's own communications. The GCSB would have the relevant expertise and capabilities to do this, but cannot easily do so under its current legislation due to the restriction on intercepting New Zealanders' private communications. The Police may be able to obtain assistance from its overseas counterparts in some cases, but this may result in undue delay.

[217] See paragraphs 5.73–5.77.
[218] See paragraphs 5.23 and 5.27.

5.70 There are also situations where New Zealanders may need to be targeted for national security purposes, which the GCSB has difficulty doing under the current legislation. For example, section 14 would likely prevent GCSB from searching for New Zealanders who are taking part in violent extremist activity overseas or are in contact with criminal or terrorist organisations.

5.71 We therefore recommend that the restriction on the GCSB taking any action for the purpose of intercepting New Zealanders' private communications be removed. The restriction is incompatible with the proposed objective of protecting national security, which can be at risk from internal as well as external threats.

5.72 Combined with our recommendations to give the Agencies common functions and objectives, this would mean that the GCSB would be able to collect information about New Zealanders in a broader range of circumstances than it can currently. However, the authorisation regime we are recommending will provide clearer protections for New Zealanders. All intrusive activity targeting New Zealanders (including those who fall within the revised definitions of "foreign person" and "foreign organisation", as we discuss below) will require a warrant with both judicial and ministerial approval. We consider this is a more effective way to protect New Zealanders' rights while allowing the government to maintain our security and advance our interests. The authorisation process we propose is discussed in Chapter 6.

The "agent of a foreign power" exception

5.73 As we have discussed,[219] the GCSB Act currently defines "foreign person" and "foreign organisation" as including New Zealand citizens and permanent residents acting as representatives of such persons or entities. To the extent that a New Zealander falls within the definition of a "foreign person" or "foreign organisation", they can be targeted despite the current restriction on intercepting New Zealanders' private communications. Because we have recommended removing the restriction in section 14 of the GCSB Act, the "agent of a foreign power" exception (as it is commonly referred to) will no longer be relevant in that context.

5.74 However, removing the "agent of a foreign power" exception entirely may cause difficulty. We recognise that there are some instances in which it may be necessary to target a New Zealander linked with a foreign entity for purposes that are broader than national security. For example, a New Zealand citizen or permanent resident could hold an influential position in, or owe allegiance to, a foreign government or a terrorist organisation. They may be the best (or only) source of information about intended actions by that government or organisation that may have a significant impact on New Zealand's trade or foreign policy. There may be value in the government retaining the ability to target these types of people on the basis that they qualify as a foreign person or organisation.

5.75 The current definitions of "foreign person" and "foreign organisation" were inserted for a different purpose than that which they would fulfil under the legislative framework we

[219] See paragraphs 5.28–5.30 above.

propose. As they stand, we consider the definitions to be too wide, in relation to both the type of entities involved and the level of connection required between the individual and the entity. The definitions appear to be capable of covering New Zealanders in situations that we would not consider appropriate. For example, they could encompass New Zealanders working for a non-governmental organisation that takes a stance perceived to be detrimental to New Zealand's economic interests.

5.76 We therefore recommend that the government review the definitions of "foreign person" and "foreign organisation" in order to narrow the circumstances in which they can apply to New Zealanders.

5.77 Before targeting any New Zealander (whether as an agent of a foreign power or otherwise), the Agencies would need to obtain a warrant approved by both the Attorney-General and a judicial commissioner (a 'tier 1 authorisation', as we discuss in the following chapter). The Attorney and Commissioner would need to be satisfied that the proposed activity is necessary and proportionate.[220] This would include being satisfied that the information required cannot reasonably be obtained in another way (for example, by targeting a non-New Zealander) and is sufficiently important to justify the intrusion on the New Zealander's privacy. We anticipate these criteria will only be met in a small number of cases outside of the national security area.

Recommendations

33. The legislation should clearly set out the circumstances in which the Agencies can direct their activities towards New Zealand citizens and permanent residents, and organisations with their centre of management and control in New Zealand ("New Zealanders").

34. The Agencies should be able to carry out activity for the purpose of targeting New Zealanders where it is necessary in order to protect national security. They should only be able to carry out activities for the wider purposes of contributing to New Zealand's economic and international well-being where those activities target foreign persons and organisations.

35. The government should review the definitions of "foreign person" and "foreign organisation" in order to narrow the circumstances in which they can apply to New Zealanders.

[220] See the table following paragraph 6.38 below.

36. The restriction on the GCSB taking any action for the purpose of intercepting New Zealanders' private communications when performing its intelligence function (section 14 of the GCSB Act) should be removed.

37. Instead, protections for New Zealanders should be implemented through a strengthened authorisation framework. If an agency wishes to carry out activity for the purpose of targeting a New Zealander (including those falling within the narrowed definitions of "foreign person" and "foreign organisation"), a warrant approved by both the Attorney-General and a judicial commissioner should be required.

38. Our terms of reference explicitly require us to consider the definition of "private communication" in the GCSB Act. Because we are recommending that section 14 of the Act be removed, the term "private communication" would no longer need to be used or defined in the legislation.

What is national security?

5.78 The term "national security" is not defined in legislation but is used widely across the statute book.

5.79 The current Government's "all hazards", cross-government approach to national security is broad and includes identifying, protecting against and responding to threats to New Zealand and New Zealanders, ranging from preventable activities such as terrorism and serious crime, through to natural disasters. This broad concept of national security extends beyond preventing and responding to immediate threats to actively managing future risks. This includes contributing to international efforts to promote order and protect human rights in unstable parts of the world. In the current global environment, international order is an important factor in achieving domestic security.

5.80 Some jurisdictions, such as the UK, have chosen not to define national security in their legislation in order to retain more flexibility to respond to a continually evolving threat environment. However, we consider it is preferable to define "national security" in legislation. This is because we are recommending there be a distinction between protecting national security and the Agencies' other objectives for the purpose of collecting information about New Zealanders.

5.81 The definition of "national security" in relation to the Agencies' objectives should be broad in order to reflect the wide-ranging and changing nature of threats to New Zealand's status as a free, open and democratic society. However, it should be narrower in scope than the "all hazards" approach referred to above, which is relevant to the functions of a broader range of

government agencies. The definition should be restricted to *protecting* New Zealand's interests, including its economic and international security. While we consider the Agencies also have a legitimate role in *advancing* New Zealand's economic and international interests in order to compete globally, consideration must be given to the importance of the information to be collected relative to the potential impact on individual rights in collecting it.

5.82 We note that the definition of "security" in the NZSIS Act refers to terms such as "subversion" and specific crimes such as "espionage", "sabotage" and "terrorist act". We propose the use of a less prescriptive and "time bound" definition that continues to capture these activities, but better describes the nature of the threats the Agencies should contribute to protecting against.

5.83 We suggest that national security could be defined as follows:

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 or 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 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.

5.84 In respect of threats to New Zealand's status as a free and democratic society, its economic security or its international relations, we consider that the definition should only cover potentially unlawful activities or acts of foreign interference. This will ensure that the Agencies cannot collect information about New Zealanders for the purpose of investigating activities such as lawful protest or dissent.

5.85 Protecting against threats to international security would include contributing to international efforts to promote order and protect human rights in unstable parts of the world, which can indirectly affect New Zealand's security. This would also include assisting the government to comply with New Zealand's international security obligations, such as United Nations Security Council resolutions.

Recommendations

39. "National security" should be defined in legislation. This is because we are recommending a distinction between national security and the Agencies' other objectives for the purpose of defining the situations in which they may direct their activities at New Zealanders.

40. The definition should be broad in order to reflect the wide-ranging and rapidly changing nature of threats to New Zealand's status as a free, open and democratic society. It should be defined as follows:

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 or safety of New Zealanders overseas
- threats, or potential threats, that may cause serious harm to the life, 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 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.

Chapter 6: How should the Agencies operate?

6.1 In the last chapter we discussed what functions the Agencies should have and the purposes for which those functions should be carried out. Just as important is the question of *how* those functions should be performed. The powers of the Agencies often give rise to the greatest level of public concern, given the potential impact on individuals.

6.2 In this chapter we discuss what powers and immunities the Agencies need to perform their functions effectively and the safeguards that should apply to the exercise of those powers. We begin by setting out a comprehensive authorisation framework, requiring external authorisation for all of the Agencies' intelligence collection and protective security activities[221] that involve gathering information about individuals and organisations.

6.3 Our aim is to ensure the Agencies' activities are reasonable and involve no greater intrusion on individuals' privacy than is necessary and proportionate in the circumstances. They should also be consistent with the Agencies' functions and objectives, and aligned with the government's national security priorities. At the same time, for the Agencies to add value to government decision-making, the authorisation regime needs to provide them with enough flexibility to perform their functions effectively.

The Agencies' current authorisation frameworks

6.4 The position under the existing legislation is unsatisfactory on a number of levels. First, the application of different authorisation requirements to the two agencies can result in confusion and make it difficult for them to work together effectively.

6.5 For example, in order to assess the risk to New Zealand from returning foreign terrorist fighters, the NZSIS may need to find out how many New Zealanders are fighting with terrorist organisations overseas. Under the current authorisation regime in the NZSIS Act, the NZSIS could not obtain a warrant to do this because its warrants must identify the particular person of interest. The NZSIS, as a human intelligence agency, also would not have the technical capability to identify these individuals remotely.

6.6 The GCSB could have the technical capability to search for New Zealanders operating in areas controlled by terrorist organisations and analyse whether they are of security concern. However, currently it could not assist NZSIS because of the narrow nature of NZSIS warrants. The GCSB also could not apply for its own warrant to do the search given the restriction on its ability to intercept the private communications of New Zealanders.

[221] As we noted in Chapter 5, when performing their assistance function the Agencies would be required to act within the scope of the other agency's powers (and, accordingly, any relevant warrants held by that agency).

6.7 Second, there are significant gaps in the legislation. Many of the NZSIS's activities rely on the fact that something is not otherwise unlawful – for instance, carrying out surveillance in public places. Under the GCSB legislation, interception warrants are only required for interception using particular methods. This results in uncertainty for both the Agencies and the public. Given the intrusive nature of the Agencies' activities, we consider all of their powers should be subject to an authorisation regime.

6.8 Third, the legislation does not provide the public, or even lawyers, with a clear and consistent understanding of what the Agencies actually do and what protections apply. It is not difficult to see why people are suspicious of the Agencies' activities when viewed in that light. Consistent with New Zealand's status as a free and democratic society, it is crucial that the Agencies have a mandate from the public. The legislation should facilitate this by making it clear, to the greatest extent possible, what the Agencies can obtain authorisation to do and what safeguards apply to protect individuals' rights and freedoms.

6.9 The issues described above do not inspire public confidence and create operational difficulties for the Agencies. The new authorisation regime we propose would improve on the current position both in terms of transparency and accountability, and workability for the Agencies.

Authorisation of the NZSIS's activities

6.10 Intelligence warrants under the NZSIS Act are separated into two categories: "domestic intelligence warrants" and "foreign intelligence warrants". Foreign intelligence is defined as "intelligence relating to 1 or more foreign organisations or foreign persons".[222] A foreign intelligence warrant can only be issued where there are reasonable grounds for believing that:[223]

- no New Zealand citizen or permanent resident (New Zealander) is identified as a person who will be subject to the warrant, and
- any place specified in the proposed warrant is occupied by a foreign person or organisation.

6.11 This means a domestic intelligence warrant is required if a New Zealander or a place occupied by a New Zealander is identified as a target. Domestic intelligence warrants must be issued jointly by the responsible Minister and the Commissioner of Security Warrants,[224] while foreign intelligence warrants are issued by the Minister alone.[225]

[222] NZSIS Act, s 2 (definition of "foreign", paragraph (b)).
[223] NZSIS Act, s 4A(2)(b).
[224] NZSIS Act, s 4A(1).
[225] NZSIS Act, s 4A(2).

6.12 Before issuing an intelligence warrant, the Minister (and, for domestic warrants, the Commissioner), must be satisfied that:[226]

- the proposed activity is necessary to detect activities prejudicial to security or for the purpose of gathering foreign intelligence information essential to security
- the value of the information sought to be obtained justifies the proposed activity
- the information is not likely to be obtained by any other means, and
- the information is not legally privileged.

6.13 The Minister is also required to consult the Minister of Foreign Affairs before issuing a warrant relating to the identification of foreign capabilities, intentions or activities.[227]

6.14 Both domestic and foreign intelligence warrants issued under the NZSIS Act must be specific. That is, they must specify particular people whose communications are to be intercepted or, if their identity is unknown, the place or facility in respect of which communications can be intercepted.[228] They cannot relate to a class of people or places. The type of document or communication to be intercepted must also be specified.

6.15 This can create problems in some situations. For example, the NZSIS may be aware that a foreign delegation is travelling to New Zealand with intelligence agents as part of the group, but they may not know the identity of the intelligence agents until they are on their way to, or have arrived in, the country. Under the current scheme, the NZSIS could not obtain a warrant in advance to target those people on arrival.

6.16 The NZSIS Act does not fully reflect the range of activities the NZSIS may need to be involved in. The warrant provisions only cover interception or seizure of communications or things, electronic tracking and (under temporary provisions introduced in December 2014)[229] visual surveillance. In reality, the NZSIS undertakes a much wider range of activities that are not referenced in the legislation or subject to any legislative authorisation regime. They are currently done on the basis that they do not involve any unlawful activity.

6.17 For example, the NZSIS may obtain metadata such as mobile phone records from telecommunications providers in reliance on its exemption from certain principles in the Privacy Act 1993, recruit human sources to obtain information and carry out in-person surveillance in public areas.

[226] NZSIS Act, s 4A(3).
[227] NZSIS Act, ss 4A(5) and 2(1) (definition of "security").
[228] NZSIS Act, s 4B(1).
[229] Under the Countering Foreign Terrorist Fighters Legislation Bill. See Chapter 8 for further information about these changes and recommendations relating to visual surveillance.

Authorisation of the GCSB's activities

6.18 The GCSB Act provides for two types of ministerial authorisations: 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) that the GCSB cannot otherwise lawfully access.

6.19 Unlike NZSIS warrants, interception warrants obtained under the GCSB Act can apply to classes of people or places, or to communications sent from or to an overseas country. This allows the GCSB to draw on a wider pool of information than the NZSIS, consistently with the nature of signals intelligence methods.

6.20 As discussed in Chapter 5, section 14 of the GCSB Act restricts the ability of the Director and employees of the GCSB to do anything for the purpose of intercepting the private communications of New Zealanders. However, limitations on the scope of section 14 mean there are still situations where the GCSB can target New Zealanders (for example, where GCSB is performing its cyber security function, or if the New Zealander qualifies as a "foreign person" or "foreign organisation"). In these situations, the relevant warrant or access authorisation must be issued jointly by the Minister responsible for the GCSB and the Commissioner of Security Warrants.[230]

6.21 Warrants and authorisations that are not for the purpose of intercepting the private communications of New Zealanders are issued by the Minister alone.

6.22 Before issuing a warrant or authorisation, the Minister (and, where applicable, the Commissioner) must be satisfied that:[231]

- the proposed activity is for the purpose of performing one of the GCSB's functions
- the outcome sought to be achieved justifies the proposed activity
- the outcome is not likely to be achieved by any other means
- there are satisfactory arrangements in place to ensure that nothing will be done in reliance on the warrant or authorisation beyond what is necessary for the proper performance of the GCSB's functions, and
- there are satisfactory arrangements in place to ensure the nature and consequences of acts done under the warrant or authorisation will be reasonable.

[230] GCSB Act, s 15B.
[231] GCSB Act, s 15A(2).

6.23 As a matter of practice, the current Government also requires the GCSB to obtain the consent of individuals or organisations it wishes to provide cyber security services to before a warrant or access authorisation will be granted. However, this is not required by the legislation.

6.24 The GCSB only requires an interception warrant for certain methods of interception. A warrant is required to install an interception device in a place to intercept communications occurring in that place (for example, using listening devices), or to connect an interception device to an information infrastructure (for example, to intercept communications passing over a particular telecommunications network).[232] Communications can be intercepted by other means with only an internal authorisation from the Director of the GCSB, provided: [233]

- the interception is for the purpose of performing the GCSB's cyber security or intelligence function, and
- any access to an information infrastructure is limited to communication links between computers or remote terminals (otherwise, an access authorisation is required[234]).

6.25 This Director authorisation process may apply, for example, to the interception of radio and satellite communications.

6.26 There is a general prohibition on warrants or authorisations being granted, or the GCSB's warrantless powers being exercised, for the purpose of intercepting communications of New Zealanders that are privileged in proceedings in a court of law.[235]

A comprehensive authorisation regime

6.27 We recommend the new legislation should establish a comprehensive and consistent authorisation regime for both agencies. It should require some form of authorisation for all of the Agencies' intelligence collection and protective security activities that involve gathering information about individuals and organisations, proportionate to the level of intrusion involved. This would serve a number of purposes:

- it would simplify the legislation, making it easier for the Agencies and the public to understand what the Agencies' powers are and the circumstances in which they can be exercised
- it would provide a greater level of accountability and oversight for those activities that are not currently subject to an authorisation process, and
- it would improve the Agencies' ability to work together effectively by removing the current inconsistencies between the two Acts.

[232] GCSB Act, s 15(1).
[233] GCSB Act, s 16(2).
[234] GCSB Act, s 15(2).
[235] GCSB Act, s 15C.

6.28 We propose a tiered system of three different types of authorisation, with increasing levels of scrutiny applying to activities that would breach the general law if not authorised, and those targeting New Zealanders. This would help to ensure that the level of scrutiny applied is proportionate to the potential impact of the activity on individuals' rights. The three tiers we propose are:

- Tier 1 authorisation: Warrant issued after approval by both the Attorney-General and a judicial commissioner
- Tier 2 authorisation: Warrant issued by the Attorney-General
- Tier 3 authorisation: Policy statement issued by the Minister responsible for the Agencies.

6.29 A decision-tree outlining our proposed authorisation framework is set out in Annex F.

6.30 Any activity that would be unlawful but for the authorisation would require approval by the Attorney-General at a minimum. Where the Agencies wish to target a New Zealander, a tier 1 authorisation with the additional safeguard of approval by a judicial commissioner would be required. This would act as an independent check on the power of the executive branch. Tier 3 authorisations would only cover activities that are permitted under the general law, such as collecting information that is publicly available.

6.31 We did consider whether, by requiring authorisation at some level for all of the Agencies' intelligence and security activities, we might risk excluding the use of novel capabilities or methods. However, we think it is important that the Agencies' powers are clearly spelled out. Provided those powers are not defined in an overly restrictive way, there should still be sufficient flexibility under the framework we propose. If further changes are needed in the future to accommodate new methods, that is something that can be considered by the next periodic review in five to seven years. We also note that the Agencies themselves supported having an authorisation framework that covers all of their activities, as it would give them greater certainty that they are acting lawfully.

Restrictions on the Agencies' activities and protections for New Zealanders

6.32 As a starting point, the Agencies should not undertake any activity unless it is necessary for the performance of their functions and is authorised in accordance with the legislation. This should be spelled out expressly for the avoidance of doubt (as it is, for example, in legislation governing the Australian and Canadian intelligence and security agencies).[236]

6.33 As we discussed in Chapter 5, the Agencies should only be able to target New Zealanders where it is necessary for the purpose of protecting national security (except to the extent the New Zealander falls within the revised definition of "foreign person" or "foreign

[236] Intelligence Services Act 2001 (AU), s 12 and National Defence Act 1985 (CA), s 273.66.

organisation"). We have also recommended removing the current restriction in section 14 of the GCSB Act on intercepting the private communications of New Zealanders.

6.34 In place of section 14, we recommend putting in place clearer and more consistent protections for New Zealanders through the authorisation framework. If the proposed activity is for the purpose of targeting a New Zealand citizen, permanent resident or an organisation with its centre of management and control in New Zealand, a tier 1 authorisation approved by both the Attorney-General and a judicial commissioner should be required. This would be the case for all New Zealanders, even if they may also be classified as a "foreign person" or "foreign organisation" under the statutory definitions. The process for approval of tier 1 authorisations is discussed in further detail below.

6.35 There may be cases where an agency incidentally obtains intelligence about a New Zealander under a tier 2 authorisation, although that New Zealander was not being directly targeted. For example, while a foreign intelligence agent's communications are being monitored they might be in contact with a New Zealander and information about that New Zealander may be obtained as a result. We recommend that a separate "review warrant" (obtained in the same manner as tier 1 authorisations) should be required if the Agencies wish to analyse incidentally obtained intelligence for the purpose of an operation or investigation targeting a New Zealander. Unless a review warrant is obtained or one of the grounds for disclosing incidentally obtained information to public authorities is met,[237] the incidentally obtained intelligence would need to be destroyed.

6.36 This will ensure incidental interception cannot be used as a way around the authorisation requirements. While we saw nothing to suggest that the Agencies do this in practice, we are concerned that the current legislation may, in theory, allow for it (as discussed in paragraphs 5.23–5.29 above).

6.37 Review warrants would only relate to information that has already been collected incidentally. However, we note for the avoidance of doubt that if the Agencies identified a New Zealander of interest while acting under a tier 2 authorisation and wished to investigate that person, they would require a tier 1 authorisation to do so.

On what basis would authorisations be granted?

6.38 Currently the criteria that the Minister and/or Commissioner of Security Warrants must be satisfied of before approving an authorisation are different between the two Acts. Under the new authorisation framework we propose, the same criteria should apply for all tier 1 and tier 2 authorisations, as set out in the table below.

[237] These are the grounds currently contained in section 25 of the GCSB Act, which should be retained as a basis for sharing information with other authorities (preventing or detecting serious crime; preventing, avoiding or responding to loss of human life; or identifying, preventing, or responding to threats or potential threats to the security or defence of New Zealand or any other country). We note that if the Agencies wish to analyse incidentally obtained material for the purpose of an operation or investigation targeting a New Zealander, they would require a review warrant even if these grounds are engaged.

Recommended criteria	Current criteria[238]	Reason for change
The proposed activity is necessary either: • for the proper performance of the Agencies' functions, or • to test, maintain or develop capabilities or train employees for the purpose of performing the Agencies' functions.	GCSB Act: The activity is for the purpose of performing a function of the GCSB. NZSIS Act: The activity is necessary for the detection of activities prejudicial to security, or for the purpose of gathering foreign intelligence information essential to security.	To clarify that: • The activity must meet the test of being *necessary* for the *proper performance* of the Agencies' functions (which is currently unclear in the GCSB Act). • The Agencies can obtain authorisations to allow training and capability development. This is important to enable the Agencies to perform their functions effectively in the mid to long term.
The proposed activity is proportionate to the purpose for which the authorisation is sought.	Both Acts: The outcome sought to be achieved justifies the proposed activity.	Similar in effect, but with a more explicit requirement for a proportionality assessment.
The outcome sought *cannot reasonably* be achieved by less intrusive means.	GCSB and NZSIS Acts: The outcome sought is *not likely* to be achieved by other means.	The Agencies, Attorney-General and judicial commissioner should be expressly required to consider whether less intrusive methods can be used.
There are satisfactory arrangements in place to ensure nothing will be done in reliance on the authorisation beyond what is reasonable and necessary for the proper performance of a function of the Agencies.	GCSB Act: same as recommended. NZSIS Act: no equivalent requirement.	Both agencies should be required to satisfy the Attorney-General (and judicial commissioner, where relevant) that they have appropriate protections in place to ensure staff act reasonably and do not exceed their mandate.
There are satisfactory arrangements in place to ensure that information is only obtained, retained, used and disclosed in accordance with the Act.	No equivalent.	This requirement will act as an additional safeguard to help ensure that information obtained under authorisations is dealt with lawfully and appropriately. Similar requirements exist in the UK and Canadian legislation.

[238] GCSB Act, s 15A(2) and NZSIS Act, s 4A(3).

6.39 Some of the criteria we are recommending are carried over from one or both of the existing Acts, while others are new or amended. The first and most fundamental criterion is that the proposed activity must be necessary for the proper performance of one of the Agencies' functions. However, this in itself is not a sufficient restriction given the functions of the Agencies are necessarily quite broad (with more specific direction given through the government's national security priorities). The remaining criteria put additional protections in place to ensure that the Agencies' activities are necessary, reasonable and involve the lowest level of intrusion on rights that is possible in the circumstances.

6.40 The legislation should also contain a separate provision to ensure the Agencies do not intercept any communications of New Zealanders that they have reason to believe are privileged (similar to the current section 15C in the GCSB Act). We note the NZSIS Act currently deals with this through the warranting criteria, but in our view it is more appropriately addressed as a separate requirement.

Tier 1 and 2 authorisations

6.41 A tier 1 or tier 2 authorisation would be required where the activity the Agencies are proposing to carry out would be unlawful but for the authorisation.

6.42 If the proposed activity is for the purpose of targeting a New Zealand citizen or permanent resident, or an organisation that has its centre of management and control in New Zealand, the Agencies would require a tier 1 authorisation. This type of authorisation would need to be approved by both the Attorney-General and a judicial commissioner. The Attorney-General would need to be satisfied that the statutory criteria are met and that the authorisation should be issued. The judicial commissioner would need to be satisfied that it is lawful to issue the authorisation. This dual approval process is discussed further at paragraph 6.76 below.

6.43 Tier 2 authorisations would be issued by the Attorney-General alone without review by a judicial commissioner. They could be obtained for activity targeting foreign persons and organisations.

6.44 Before approving a tier 1 or 2 authorisation, the Attorney-General would be required to refer the application to the Minister of Foreign Affairs for comment if the proposed activity is likely to have implications for New Zealand's foreign policy or international relations. We would expect the Attorney-General and Minister of Foreign Affairs to agree on a process for determining when this would be required. This referral requirement is similar to existing provisions in the legislation and is necessary to ensure that any risks to New Zealand's international relations are taken into account during the authorisation process.

6.45 Tier 1 and 2 authorisations could permit the following types of activity:

- interception of communications, including metadata

- acquisition of information held by third parties (such as telecommunications companies, internet service providers, banks and government agencies – who would be required to comply where reasonably practicable – and overseas intelligence agencies)
- accessing an information infrastructure
- surveillance (including using video, listening and tracking devices, as well as in-person surveillance where it would otherwise be unlawful – such as on private property), and
- use of human sources where this is likely to involve a breach of the law (for example, an agent embedding themselves in a terrorist group to obtain information may become implicated in attack planning).

6.46 The legislation should also allow tier 1 and 2 authorisations to permit other reasonable activities necessary to give effect to them, such as entry onto private premises in order to install surveillance devices.

6.47 A tier 1 or 2 authorisation would only be required to the extent that the proposed activities are unable to be carried out in accordance with a tier 3 authorisation or the general law. For example, a tier 1 or 2 authorisation would not generally be required to intercept communications that are broadcast publicly or to carry out surveillance in a public place.

6.48 A tier 1 or 2 authorisation would be required in order to access information held by overseas intelligence agencies, unless the foreign agency has obtained the information in a way that would be covered by a tier 3 authorisation if it occurred in New Zealand. Under the existing legislation, access to partner information is not explicitly addressed. We consider information obtained through partner agencies should be subject to the same safeguards as if the information was obtained by the Agencies. We were told that as a matter of practice the Agencies do not seek to access information from foreign partners that they could not lawfully obtain themselves. However, this should be made explicit in the legislation.

6.49 A tier 1 or 2 authorisation would also be required for all interception of communications or metadata that is not permitted under the general law. This is a change from the current position. As discussed above, the GCSB Act currently allows the GCSB to carry out certain types of interception with an internal authorisation from the Director. We see no basis for distinguishing between different interception methods in this way.[239] The level of intrusion on individuals' privacy is the same regardless of how the interception is carried out, so the same level of protection should apply.

6.50 We note, for the avoidance of doubt, that authorisations would be able to cover multiple types of activity. For example, the GCSB may need to intercept communications and request information from a foreign partner in relation to the same investigation. In such cases it should not be required to obtain two separate authorisations, provided both types of activity

[239] GCSB Act, s 16. See paragraph 6.23 above.

are covered in a relevant authorisation. Conversely, the Agencies could if they wish have multiple authorisations in place to support a particular investigation.

6.51 Tier 1 and 2 authorisations should be valid for up to 12 months, as is currently the case. We did not see any reason to reduce this period, and are concerned that doing so would significantly increase the administrative burden on the Agencies, the Attorney-General and the judicial commissioners.

6.52 We suggest two minor changes to address operational issues we were alerted to and, we hope, to reduce the need for the Agencies to waste valuable time and resources seeking new authorisations to cater for minor changes in circumstances. Where an individual is required to be identified in an authorisation, the legislation should, where appropriate, allow this to occur through a description (for example, a job title or code name) rather than a name. The legislation should also provide for authorisations to be amended or revoked.

Metadata

6.53 We considered whether any distinction should be drawn between the content of communications and metadata under the authorisation regime we are proposing. Metadata is data about data – for example, the sender of an email or the time of a phone call. We concluded that interception of metadata should be subject to the same level of scrutiny as interception of the content of communications, for two reasons.

6.54 First, metadata can reveal a significant amount about a person's private life. For instance, it might allow intelligence agencies to determine a person's movements and who they have been in contact with. Because of this, interception of metadata can be just as intrusive as interception of content (although that is by no means always the case). Given this potential, it seems appropriate that metadata should be subject to the same level of protection as content.

6.55 Second, there is no universally accepted definition of metadata. While some types of information are almost certainly metadata (such as the time of a phone call), other classes of data (such as the subject line of an email) fall into a grey area that is subject to considerable debate. In addition, the types of metadata that exist are continually evolving. In light of this, we consider that having separate authorisation requirements for metadata would create unnecessary bureaucracy and uncertainty. The Agencies and those responsible for issuing authorisations would need to determine in each case what category the particular information sought falls within. Often, the Agencies will need to access both content and metadata, so two types of authorisations would be required.

6.56 We therefore concluded it would be simpler and more consistent with the nature of privacy interests to treat metadata and content in the same way for authorisation purposes.

Scope of authorisations

6.57 We recommend that the following types of tier 1 and tier 2 authorisations could, subject to the restrictions noted below, be "purpose-based". That is, they could specify the type of information sought and the operational purposes for which it is required rather than identifying a particular person, premise or thing as the target:

- tier 1 and tier 2 authorisations to intercept communications (including metadata)
- tier 1 and tier 2 authorisations to acquire information held by third parties (including foreign partners)
- tier 2 authorisations to access an information infrastructure
- tier 2 authorisations to carry out surveillance

6.58 The operational purpose(s) specified in the authorisation would need to be more specific than the Agencies' objectives. For example, it would be insufficient to say that certain information is required to protect national security. The authorisation would need to specify why the information is needed at a level down from the Agencies' broad objectives. An interception authorisation might, for example, enable interception of communications inside Islamic State ("ISIL")-controlled territory in Syria for the purpose of identifying New Zealanders who are fighting for or otherwise supporting ISIL.

6.59 We consider the ability to obtain purpose-based authorisations is necessary to enable the Agencies to perform their functions effectively, particularly at the stage of identifying initial leads for further investigation. At this early stage, the Agencies often will not have sufficient information to identify a specific person as a target, so their activities would be unduly limited if this was required. To use the example given above, a specific authorisation would not enable the Agencies to identify New Zealanders fighting for ISIL because their identities would not be known at the time the authorisation was required.

6.60 As the UK Intelligence and Security Committee has said:[240]

> The Agencies can use targeted interception only after they have discovered that a threat exists. They require separate capabilities to uncover those threats in the first place, so that they can generate leads and obtain the information they need to then target those individuals.

6.61 The UK's new draft Investigatory Powers Bill therefore allows for purpose-based warrants.[241]

6.62 Purpose-based authorisations will also make it easier for the Agencies to be sufficiently responsive when leads are received at short notice. For example, the NZSIS may be informed

[240] Intelligence and Security Committee of Parliament *Privacy and Security: A Modern and Transparent Legal Framework* (UK, March 2015) at 3.
[241] Draft Investigatory Powers Bill (UK, 4 November 2015), cls 111, 125, 140 and 153–154, accessed at <https://www.gov.uk/government/publications/draft-investigatory-powers-bill>.

that a foreign intelligence officer is intending to travel to New Zealand the day before he or she arrives. Under the current arrangements, the NZSIS must obtain a new warrant each time this occurs. The time delay in obtaining a warrant and then setting up a surveillance operation means the NZSIS may not always be able to respond in these types of situations. Under the new framework we are proposing, the NZSIS could have a purpose-based tier 2 authorisation already in place that would allow it to commence surveillance of foreign intelligence officers immediately on arrival.

6.63 While we recommend providing for purpose-based authorisations in appropriate circumstances, the legislation should contain a presumption in favour of targeted authorisations. The Attorney-General, and the judicial commissioner in the case of tier 1 authorisations, would only be able to issue a purpose-based authorisation where satisfied it is necessary and proportionate in the circumstances, and that the outcome sought could not reasonably be achieved through the use of targeted authorisations. The Attorney-General could also impose restrictions and conditions on authorisations. This would help to avoid the proliferation of overly broad authorisations, while still allowing the Agencies sufficient flexibility to perform their functions effectively.

6.64 In relation to the remaining types of authorisations:

- Tier 1 and tier 2 authorisations permitting the use of human sources should be required to identify the source or agent (by code name if necessary) and the information that person will be tasked to obtain. Given the sensitivities involved in human source operations, it is appropriate that they be considered on a case-by-case basis. We note for clarity that an authorisation would only be required where the source may need to engage in unlawful activity. Otherwise lawful use of human sources would be governed by a tier 3 authorisation.

- Tier 1 authorisations allowing surveillance would need to identify the specific target (by identity, place or selector such as a phone number). We note, however, that surveillance authorisations should only be required for activity that is not already covered by another type of authorisation. For example, some types of information showing a person's location could be obtained under an interception authorisation but might also be seen as a type of surveillance. In such cases the Agencies would not require both types of authorisation; an interception authorisation would be sufficient.

- Tier 1 authorisations allowing access to information infrastructures would need to specify the information infrastructure or class of information infrastructures to be targeted. If a class of information infrastructures is specified, this would need to be done at a sufficient level of particularity so that the Attorney-General and judicial commissioner can reasonably foresee the extent of interference with individuals' rights and assess whether it is necessary and proportionate.

Tier 3 authorisations

6.65 The lowest level of authorisation would be a policy statement approved by the Minister responsible for the Agencies. Tier 3 authorisations would apply to the Agencies' intelligence and security activities that involve gathering information about individuals and organisations but are lawful without an authorisation. This would include things such as:

- open source intelligence collection
- physical surveillance in public places
- use of human sources in situations that would not involve any breach of the law
- access to information infrastructures or interception of communications with lawful consent (for example, for cyber security purposes)[242]
- use of cover and assumed identities (this will be specifically enabled elsewhere in the legislation, as discussed further below)[243]
- community engagement.[244]

6.66 The activities falling within this category are already carried out, but generally without any form of external authorisation (the exception being access to information infrastructures with consent, which as a matter of practice is covered by an authorisation). Tier 3 authorisations would provide a greater level of oversight and accountability for these activities. They would also give guidance to the Agencies on any grey areas where it may be unclear whether a particular type of activity is lawful and/or appropriate without a tier 1 or 2 authorisation (for example, by setting out the circumstances in which consent will be sufficient to access an information infrastructure). This will help to ensure the Agencies comply with the law.

6.67 Tier 3 authorisations could apply for up to three years before requiring renewal. Each tier 3 authorisation would set out what information or activity it applies to, the purposes for which that information can be collected or activity carried out, the methods that can be used and any protections that need to be put in place (for example, privacy protections). The level of detail included may vary depending on the subject matter. The Minister could also specify in a

[242] For the sake of clarity, we note this would not allow the Agencies general access to the intelligence databases of foreign partners, which would require an appropriate level of authorisation depending on the content. The relevant tier 3 authorisation would need to set out who has the appropriate level of authority to grant lawful consent in relation to the information that will be accessed.

[243] See paragraphs 6.106–6.119.

[244] In general, the Police should continue to have primary responsibility for community outreach on safety issues. However, there may be situations where the NZSIS or GCSB need to speak to members of the public. Consistently with our comments regarding the need for increased openness and transparency about the Agencies' work, they should be able to do this in appropriate circumstances. This could usefully be clarified in a tier 3 authorisation. A joint operating protocol between the Police and the NZSIS would also help to clarify their respective roles in this area (see paragraph 5.57).

tier 3 authorisation that a tier 1 or 2 authorisation must be sought for particular activities, for example because of the level of risk or intrusion on privacy associated with the activity.

6.68 The criteria for tier 1 and 2 authorisations discussed above[245] would not directly apply to tier 3 authorisations, since they would cover a much broader range of activity than tier 1 or 2 authorisations (for example, all open source collection). However, the Minister should, before issuing a tier 3 authorisation, be satisfied that there are appropriate internal mechanisms in place to ensure that any activity carried out under it will be consistent with those criteria. For example, although surveillance in a public place would not generally require a tier 1 or 2 authorisation, the relevant tier 3 authorisation might require such activity to be signed off by a person of a specified level of seniority. This would help to ensure that a proper assessment of necessity and proportionality is made.

6.69 Each tier 3 authorisation would need to be referred to the Inspector-General for comment before it is approved. The Inspector-General would be able to advise the Minister as to the legality of the statement and suggest any changes he or she considers to be desirable.

6.70 We note that while the activities listed in paragraph 6.65 above are generally lawful, employees of the Agencies may still need to commit minor breaches of the law in the course of carrying them out. For example, it is lawful to follow a target in a car in a public place, but an NZSIS officer may need to commit a minor traffic infringement such as speeding so as not to lose them. As we discuss in paragraphs 6.120–6.133 below, we recommend the Agencies' immunities should extend to certain minor breaches of the law carried out in the course of acting under a tier 3 authorisation.

Records and reporting

6.71 We make two further recommendations that will facilitate effective oversight of the Agencies' activities. The Agencies should be required to keep a register of all authorisations issued (tiers 1, 2 and 3). The GCSB is already required to keep a register of warrants and authorisations,[246] but there is no such requirement for the NZSIS. The register should be made available to the Inspector-General, the Minister responsible for the Agencies, the Attorney-General and the judicial commissioners.

6.72 In addition, the Agencies' annual reports should include reporting on the outcome of tier 1 and tier 2 authorisations (including review warrants). For example, the report might state that intelligence was obtained and provided to another agency or minister, or that an investigation against a person was discontinued. If necessary, this could occur in a classified version of the report only and be redacted in the public version. The purpose would be to allow the Inspector-General to monitor whether the Agencies are accurately judging necessity and proportionality when seeking authorisations, and implementing them appropriately.

[245] See paragraph 6.38.
[246] GCSB Act, s 19.

The Attorney-General's role

6.73 We recommend that the Attorney-General, rather than the Minister responsible for the Agencies, should approve tier 1 and 2 authorisations. As the principal law officer of the Crown, he or she is the appropriate member of the executive branch to take into account human rights implications and ensure the rule of law is upheld.[247] This is particularly important in the case of tier 2 authorisations, which will not involve any judicial approval. At the same time, as a member of the executive the Attorney-General (unlike a judicial commissioner) is able to assess whether a particular activity is in the national interest. In this sense the Attorney-General is able to perform a dual role that neither the responsible Minister nor a judicial commissioner could fulfil alone.

6.74 We see a real advantage in the Attorney-General also being the Minister responsible for the Agencies, as is currently the case. That should not prevent him or her from approving authorisations. To the contrary, it will allow the Attorney-General to develop a greater understanding of the Agencies' activities and the broader environment they operate in. This may assist in making assessments, for example, about the relative seriousness of a particular threat or whether information can be obtained in a less intrusive manner.

6.75 We acknowledge that if the Attorney-General is not responsible for the Agencies, he or she may as a matter of practice wish to consult the responsible minister before issuing authorisations in some situations. However, we do not propose to include an explicit consultation requirement in the legislation. In our view that would create an additional and unjustified layer of bureaucracy to a process that may already require consideration by three individuals (the Attorney-General, the Minister of Foreign Affairs and a judicial commissioner), depending on the authorisation in question.

Joint approval of tier 1 authorisations

6.76 We have recommended that tier 1 authorisations should only be issued after approval by the Attorney-General and a judicial commissioner. Both the Attorney-General and the judicial commissioner would need to be satisfied that the statutory criteria for issuing the authorisation are met. Among other things, these criteria will require the Attorney-General and judicial commissioner to be satisfied that the proposed activity is necessary and proportionate.[248]

6.77 If the Agencies wish to treat a New Zealander as an "agent of a foreign power", the Attorney-General and judicial commissioner would both need to be satisfied that the person falls within

[247] By way of comparison, we note that the Attorney-General issues security and intelligence warrants in some other jurisdictions, such as Australia and the USA. In Australia, the Attorney-General is both responsible for the Australian Security Intelligence Organisation and issues warrants in respect of its activities.
[248] The full criteria are set out at paragraph 6.38 above and the table that follows.

the revised, narrower definitions of "foreign person" and "foreign organisation", as we discussed in the previous chapter.[249]

6.78 The Attorney-General would also need to be satisfied that it is appropriate to issue the authorisation, taking into account broader national interest considerations (such as any risks to New Zealand's international relations). Even if the criteria for issuing an authorisation are met, he or she may still decline to approve the application. The judicial commissioner, by contrast, will consider the application from a legal perspective. This would still involve making an assessment about whether there is a sufficient evidential basis for concluding that the statutory criteria are met. In addition, judicial commissioners would be free to raise any broader concerns with the Attorney-General, although the Attorney-General would make the ultimate decision on matters of national interest.

6.79 This is similar to the approach under the existing legislation in the sense that both judicial and executive consideration is required for the authorisation of activities relating to New Zealanders. However, in our view the nature of the judicial commissioners' role should be clarified to ensure that judicial approval is appropriately focused on legal factors. This will serve to emphasise the independence of the judicial commissioners from the executive and help to ensure impartiality is maintained. For the avoidance of doubt, we do not suggest that the current Commissioner of Security Warrants lacks independence or impartiality. We do see scope, however, for independence to be compromised if judicial commissioners are asked to make non-legal judgements about what activities it is appropriate for the Agencies to be undertaking.

6.80 We see this recommendation as simply formalising the current practice. In this respect we refer to the evidence given by the current Commissioner of Security Warrants, Sir Bruce Robertson, to the UK Joint Committee on the Draft Investigatory Powers Bill.[250] Sir Bruce told the Committee that while the legislation does not restrict him to purely legal considerations, in practice he sees his role as ensuring that the proposed activity is lawful (including that there is a proper evidential basis for it). He saw "high policy" and diplomatic repercussions as being ultimately a matter for the executive branch rather than a judge. We agree with that approach.

6.81 A range of submitters to our review supported solely judicial authorisation. In our view, a combined process involving both ministerial and judicial consideration provides the best balance. To a far greater extent than law enforcement warrants, intelligence and security authorisations require a careful balancing of the risks and benefits of activities to New Zealand's interests. This is ultimately a matter for the executive, not the judiciary. The Attorney-General's involvement will allow the wider context to be taken into account, while

[249] See paragraphs 5.73–5.77 above.
[250] Joint Committee on the Draft Investigatory Powers Bill *Oral Evidence: Draft Investigatory Powers Bill* (HC 651, 6 January 2016), accessed at <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/oral/26679.html>.

approval by a judicial commissioner will ensure a strong independent focus on the relevant legal requirements and any impacts on human rights.

6.82 In our view, dual approval of activities targeting New Zealanders by an independent judicial commissioner and the Attorney-General is consistent with the requirement under the Search and Surveillance Act for Police surveillance warrants to be issued by a judge. The Agencies, if anything, should have a stricter authorisation regime than Police given that their activities are generally carried out in secret and are rarely tested in a court of law.

6.83 We observe that there has also been a move toward greater judicial involvement in issuing intelligence warrants in other jurisdictions. In the UK, where all of the intelligence and security agencies' activities are currently authorised by secretaries of state only, two recent reports have recommended judicial involvement in the process.[251] The draft Investigatory Powers Bill, a revised version of which is expected to be introduced later this year, reflects these proposals. The draft Bill creates a process of approval by a secretary of state and review by a judicial commissioner on judicial review grounds for most of the intelligence agencies' activities.[252]

6.84 We considered whether judicial approval was appropriate for the Agencies' foreign intelligence activities as well. However, where the Agencies are gathering intelligence about foreign persons and organisations, there are different factors at play. The benefits and risks associated with these activities relate primarily to New Zealand's foreign policy, trade and defence interests. These are matters that ministers are best placed to weigh up.

6.85 We recognise that human rights and compliance with the rule of law remain important in relation to foreign intelligence activities. However, we consider that the Attorney-General, as the principal law officer of the Crown, is well qualified to take these matters into account. This is, in part, why we are recommending that authorisations be approved by the Attorney-General, rather than the Minister responsible for the Agencies (which is the position under the current legislation).

6.86 There is a balance to be struck between placing sufficient safeguards on the Agencies' activities, which are by their nature intrusive, while providing the Agencies with enough flexibility to perform their functions. If an authorisation process is unnecessarily long or cumbersome, it will prevent the Agencies from responding quickly to developing situations. Given the areas in which the Agencies operate, delay has the potential to result in serious consequences. Authorisation processes should therefore be as timely and efficient as possible while ensuring proper scrutiny. The benefits of increased oversight must be weighed against the corresponding decrease in efficiency and increase in compliance costs. In our view, this

[251] David Anderson QC *A Question of Trust: Report of the Investigatory Powers Review* (UK, June 2015) at [14.47]–[14.57], [14.64–67] and recommendation 30; Royal United Services Institute *A Democratic Licence to Operate: Report of the Independent Surveillance Review* (UK, July 2015) at [5.59]–[5.60] and recommendation 10.

[252] Draft Investigatory Powers Bill (UK, 4 November 2015), cls 19, 90, 109, 123, 138, 155, accessed at <https://www.gov.uk/government/publications/draft-investigatory-powers-bill>.

balance is best struck by requiring judicial approval of activities targeting New Zealanders, but not the Agencies' other activities.

Panel of Judicial Commissioners

6.87 Under the existing legislation, there is one Commissioner of Security Warrants (currently Sir Bruce Robertson) who jointly approves warrants relating to New Zealanders. In practice this requires him to make himself available frequently at short notice and respond promptly to warrant applications.

6.88 In our view this system could be improved. The NZSIS Act provides for the Attorney-General to act in substitution for the Commissioner of Security Warrants if he is unavailable.[253] There is no equivalent provision in the GCSB Act, so the GCSB is unable to obtain an authorisation requiring consideration by the Commissioner if he is unavailable. Further, in our view it is inappropriate for the Attorney-General to act in the Commissioner's place. The purpose of having a judicial commissioner involved is to ensure an assessment that is impartial and independent from the executive.

6.89 The current Commissioner told us that he considers around 4–6 warrant applications per month from each of the Agencies (so, about 8–12 per month in total). That number includes applications to renew or re-issue existing warrants that are due to expire. However, we envisage there may be a small increase in the number of applications that will need to be considered by a judicial commissioner if our recommendations are adopted. This is because tier 1 authorisations will be required for more types of activity than they are currently and the GCSB will be able to apply for them to target New Zealanders for the purpose of protecting national security.

6.90 We recommend there should be a panel of at least three judicial commissioners, headed by a Chief Commissioner of Intelligence Warrants. At least one judicial commissioner should be available at all times to ensure that applications can be dealt with promptly. The additional judicial commissioners could either be retired judges, as the current Commissioner is, or sitting judges. We see some benefit in having sitting judges as commissioners so that they could also be designated to hear cases involving security sensitive information, allowing their knowledge and expertise to be taken advantage of more widely.

6.91 While there is likely to be some increase in the workload of the commissioners, these would still be part time positions when shared between three. This should leave room for sitting judges to continue their usual duties while also performing the role of a commissioner.

[253] NZSIS Act, s 5G.

Recommendations

41. The legislation should require some form of authorisation for all of the Agencies' intelligence and security activities that involve gathering information about individuals and organisations, to ensure that appropriate safeguards apply to everything they do.

42. There should be a three-tiered approach to authorisation of the Agencies' activities, with higher levels of scrutiny applying to activity that targets a New Zealand citizen or permanent resident, or an organisation that has its centre of management and control in New Zealand ("New Zealander").

Tier 1 authorisation – warrant approved by the Attorney-General and a judicial commissioner

43. The highest level of authorisation would be a warrant approved by the Attorney-General and a judicial commissioner ("tier 1 authorisation"). A tier 1 authorisation should be required for any activity that would otherwise be unlawful that is for the purpose of targeting a New Zealander.

44. Tier 1 authorisations should be able to permit the following types of activity:

- interception of communications, including metadata
- acquisition of information held by third parties (such as telecommunications companies, internet service providers, banks and government agencies – who would be required to comply where reasonably practicable – and foreign intelligence agencies)
- accessing an information infrastructure
- surveillance (including using video, listening and electronic tracking devices, and physical surveillance)
- use of human sources.

45. Both the Attorney-General and judicial commissioner would need to be satisfied that the statutory criteria for issuing a tier 1 authorisation are met. The Attorney-General would also take into account broader national interest considerations and would have discretion to decline to issue an authorisation even if the criteria are met. The judicial commissioner would consider the legality of the application, including consistency with human rights laws.

46. The Attorney-General could, as is currently the case, be the Minister responsible for the Agencies as well, and this should not prevent him or her from approving authorisations. In fact, we see considerable benefit in the same person having this dual role.

47. As an additional safeguard, the legislation should provide for review warrants (issued through the same process as other tier 1 authorisations). A specific review warrant would be required if the Agencies wish to analyse incidentally obtained intelligence for the purpose of an operation or investigation targeting a New Zealander.

48. Any incidentally obtained intelligence should be destroyed unless a review warrant is obtained or one of the grounds for disclosing incidentally obtained information to public authorities is met.

Tier 2 authorisations – warrant approved by the Attorney-General

49. The second tier of authorisation would be a warrant issued by the Attorney-General ("tier 2 authorisation"). Tier 2 authorisations would be required for the same types of activity as tier 1 authorisations, but where it is not for the purpose of targeting a New Zealander.

Tier 3 authorisations – policy statement approved by the responsible Minister

50. The lowest level of authorisation would be a policy statement approved by the Minister responsible for the Agencies after being referred to the Inspector-General for comment ("tier 3 authorisation").

51. Tier 3 authorisations should apply to the Agencies' intelligence and security activities that involve gathering information about individuals and organisations but are lawful without a warrant or authorisation (for example, open source intelligence collection, surveillance in public places or access to information infrastructures with consent).

52. A tier 1 or 2 authorisation should not ordinarily be required for activity that is permitted under the general law. However, the Minister should be able to specify in a tier 3 authorisation that a higher level of authorisation must be sought for particular activities, for example because of the level of risk or intrusion on privacy associated with the activity.

53. Each tier 3 authorisation should set out what information or activity it applies to, the purposes for which that information can be collected or activity carried out, the methods that can be used and any protections that need to be put in place (for example, privacy protections).

54. Tier 3 authorisations should apply for a maximum of three years before requiring renewal.

Basis for granting tier 1 and 2 authorisations

55. Before issuing a tier 1 or 2 authorisation, the legislation should require the Attorney-General, and the judicial commissioner in the case of tier 1 authorisations, to be satisfied that:

- the proposed activity is necessary either:
  - for the proper performance of one of the Agencies' functions, or
  - to test, maintain or develop capabilities or train employees for the purpose of performing the Agencies' functions
- the proposed activity is proportionate to the purpose for which the warrant or 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 or authorisation 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 the Act.

56. The Attorney-General should be required to refer applications for tier 1 and tier 2 authorisations to the Minister of Foreign Affairs for comment if the proposed activity is likely to have implications for New Zealand's foreign policy or international relations.

Other matters relating to tier 1 and tier 2 authorisations

57. Tier 1 and 2 authorisations should be valid for up to 12 months, as is currently the case.

58. Instead of identifying a particular person, place or thing as the target, some tier 1 and tier 2 authorisations should be able to specify the type of information sought and the operational purposes for which it is required.

59. However, the legislation should contain a presumption in favour of targeted authorisations. The Attorney-General, and the judicial commissioner in the case of tier 1 authorisations, should only be able to issue a purpose-based authorisation where satisfied it is necessary and proportionate in the circumstances, and that the outcome sought could not reasonably be achieved through the use of a targeted authorisation.

60. The ability to obtain purpose-based authorisations should apply to the following types of authorisations:

- tier 1 and 2 authorisations to intercept communications, including metadata
- tier 1 and 2 authorisations to acquire information held by third parties (including foreign partners)
- tier 2 authorisations to access an information infrastructure
- tier 2 authorisations to carry out surveillance.

61. In relation to the remaining types of authorisations:

- tier 1 and 2 authorisations permitting the use of human sources should be required to identify the source and the information they are seeking to obtain
- tier 1 authorisations allowing surveillance should be required to identify the specific target (by identity, place or selector such as a phone number)
- tier 1 authorisations to access information infrastructures should be required to specify the information infrastructure or class of information infrastructures targeted.

62. Where an individual is required to be identified in an authorisation, the legislation should allow this to occur through a description (such as a job title or code name) where the individual cannot be identified by name, or to allow for role succession.

63. The legislation should also allow authorisations to be amended or revoked.

Records and reporting on authorisations

64. The Agencies should be required to keep a register of all authorisations issued (tiers 1, 2 and 3). The register should be made available to the Inspector-General, the Minister responsible for the Agencies, the Attorney-General and the judicial commissioners.

65. The Agencies' annual reports should include reporting on the outcome of tier 1 and tier 2 authorisations (including review warrants). This would allow the Inspector-General to monitor whether necessity and proportionality is being accurately judged at the point when authorisations are issued.

Judicial commissioners

66. A panel of at least three judicial commissioners should be introduced, headed by a Chief Commissioner of Intelligence Warrants (in place of the current single Commissioner of Security Warrants). At least one judicial commissioner should be available at all times to ensure that applications for tier 1 authorisations can be dealt with promptly.

67. The judicial commissioners should either be retired judges, as the current Commissioner is, or sitting judges, as the role will not be full time. This will expand the pool of potential candidates. Having sitting judges as commissioners would enable them to be designated to sit on national security-related cases as well.

Authorisation in urgent situations

6.92 Under the current legislative scheme, there is limited provision for authorisations to be obtained urgently. To the extent that the Acts do deal with this issue, they are inconsistent between the two agencies and between different types of warranted activity. This has resulted from various amendments over time. As noted above, only the NZSIS Act provides for substitution of the Commissioner when he or she is unavailable. On the other hand, the GCSB Act provides for substitution of the responsible Minister[254] while the NZSIS Act does not.

6.93 Temporary provisions in the NZSIS Act introduced as part of the Countering Foreign Terrorist Fighters Legislation Bill in December 2014 created a new urgent authorisation process.[255] The Director can authorise interception, seizure, tracking or visual surveillance for up to 24 hours in urgent situations where the delay associated with obtaining a warrant is likely to result in a loss of intelligence. This process can only be used for counter-terrorism purposes and only applies to the NZSIS. There is no equivalent process under the GCSB Act.

6.94 We recommend the introduction of a single, consistent approach to authorisation in urgent situations. This would more accurately reflect the reality that both agencies encounter situations where urgent action is required, and this is not confined to particular areas of the Agencies' operations (although it may be more common in certain contexts, such as counter-terrorism and counter-espionage investigations).

[254] GCSB Act, s 19A.
[255] NZSIS Act, s 4ID.

6.95 As a starting point, the legislation should require the Prime Minister to designate a minister to have a standing power to act on behalf of the Attorney-General in the event that the Attorney-General cannot be contacted. This will help to ensure that the Attorney-General or an acting minister is contactable at all times.

6.96 The Prime Minister should also be required to designate a minister to act on behalf of the Minister of Foreign Affairs when he or she is unavailable, for the purpose of being consulted on tier 1 and 2 authorisations. This will ensure applications are not held up indefinitely where, for example, the Minister is overseas.

6.97 There should also be an interim authorisation process applying in urgent situations. By "urgent", we refer to those cases where:

- there is an imminent threat to the life or safety of any person, or
- the delay associated with obtaining a tier 1 authorisation through the ordinary process is likely to seriously prejudice national security.

6.98 We considered a range of options, including the urgent Director authorisation process that currently applies to counter-terrorism investigations. As a general principle, we consider ministerial approval should be obtained wherever possible. Ministers are best placed to assess the overall national interest and also provide an important external perspective that a Director cannot.

6.99 We recommend that in urgent circumstances the Agencies should be able to commence activity that would otherwise require a tier 1 authorisation with the approval of the Attorney-General or, if the Attorney-General cannot be contacted, the minister designated to act on his or her behalf.

6.100 The Chief Commissioner of Intelligence Warrants would need to be notified immediately and could direct that the activity cease at any time. The Attorney-General and Commissioner would be provided with a full application for a tier 1 authorisation within 48 hours and would consider it in the ordinary way. If the Attorney-General or a judicial commissioner declined to confirm the authorisation, any intelligence collected would need to be destroyed unless one of the grounds for retaining and disclosing incidentally obtained intelligence is met (for example, if it relates to a threat to life or serious crime).[256]

6.101 We consider 48 hours is an appropriate amount of time to allow the relevant agency to prepare a full application for a tier 1 authorisation and for a judicial commissioner to consider it. Applications are required to set out all of the relevant information and the reasons the authorisation is sought in some detail. Some of the applications we saw ran to 20 pages. We note a 48 hour maximum period for urgent action is also consistent with the Search and

[256] See section 25 of the GCSB Act, which we recommend be retained with any necessary modifications.

Surveillance Act, which allows Police officers to conduct warrantless surveillance for 48 hours in urgent situations (although, in that case, without any external authorisation).[257]

6.102 We also recommend that in urgent situations the Attorney-General (or the minister designated to act on his or her behalf) should be able to grant a tier 1 authorisation (including interim authorisations) or a tier 2 authorisation orally – for example, over the phone – provided the director of the agency certifies the approval has been given. This is similar to the approach taken in the UK.[258] It should enable the Agencies to be sufficiently responsive while still ensuring the proposed activity is in the national interest and providing an important external perspective.

6.103 While the arrangements set out above should suffice in virtually all cases, it is possible – particularly in light of the recent attacks in Paris – to imagine circumstances in which immediate action might be required and a relevant minister cannot be contacted in the short space of time available. As a last resort, we recommend that the legislation also provide for an urgent Director authorisation. Such an authorisation could only be given where obtaining an interim authorisation or a tier 2 authorisation from the Attorney-General or designated minister is likely to cause delay to such an extent that the purpose of obtaining it would be defeated (for example, because the threat to life or safety is likely to eventuate before an interim authorisation could be obtained).

6.104 The agency would need to notify the Attorney-General (and, for activity requiring a tier 1 authorisation, the Chief Commissioner of Intelligence Warrants) without delay and provide a full application within 24 hours.

6.105 Any interim or oral authorisations and supporting documentation should be referred to the Inspector-General as soon as practicable. The Agencies should also be required to state in their annual reports how many times the urgent authorisation processes were used in the reporting year. These measures will enable oversight of the process by the Inspector-General and Intelligence and Security Committee, to help ensure it is being used appropriately.

[257] Search and Surveillance Act 2012, s 48.
[258] Regulation of Investigatory Powers Act 2000 (UK), s 7; Intelligence Services Act 1994 (UK), ss 5–7.

Recommendations

68. 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 (or another minister designated to act on his or her behalf). "Urgent" means where:

    - there is an imminent threat to the life or safety of any person, or
    - the delay associated with obtaining a tier 1 authorisation through the ordinary process is likely to seriously prejudice national security.

69. 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 and consider it in the ordinary way.

70. If the Commissioner or Attorney-General declines to confirm the authorisation, any intelligence collected under it should be destroyed unless one of the grounds for retaining and disclosing incidentally obtained intelligence is met.

71. In urgent situations a tier 1 authorisation (including an interim authorisation) or a tier 2 authorisation could be granted by the Attorney-General or designated minister orally – for example, over the phone – provided the director of the agency certifies the approval has been given.

72. The Prime Minister should be required to designate a minister to have a standing power to act on behalf of the Attorney-General in the event that the Attorney-General cannot be contacted.

73. The Prime Minister should also be required to designate a minister to act on behalf of the Minister of Foreign Affairs when he or she is unavailable, for the purpose of providing comment on tier 1 and tier 2 authorisation applications.

74. As a last resort, the legislation should provide for a Director authorisation. Such an authorisation could only be given where obtaining an interim authorisation or a tier 2 authorisation from the Attorney-General or designated minister would cause delay to such an extent that the purpose of obtaining it would be defeated (for example, because the threat to a person's life or safety is likely to eventuate before the authorisation could be obtained).

75. Where an urgent Director authorisation is granted, the Director should notify the Attorney-General (and, for activity requiring a tier 1 authorisation, the Chief Commissioner of Intelligence Warrants) without delay and provide a full application within 24 hours.

76. Any interim or oral authorisations and supporting documentation should be referred to the Inspector-General as soon as practicable.

77. Each agency should be required to state in its annual report how many times the urgent authorisation processes were used in the reporting year.

Cover for operations and employees

What is cover?

6.106 As discussed Chapter 2, much of the work of intelligence and security agencies is necessarily carried out in secret. If the Agencies' methods of detection and investigation became known to people who might harm New Zealand's interests, they could change their behaviour and means of communication to avoid detection.

6.107 To prevent this from occurring, the Agencies need to create and maintain cover for their operations. For example, NZSIS employees or sources may need to acquire false identity documents to avoid detection, or register companies to help establish a business cover. The GCSB may also need to adopt assumed identities to support operational activities, such as procuring services in a way that cannot be traced back to it.

6.108 In addition to creating cover for operations, NZSIS employees are required to keep the fact of their employment with the NZSIS secret. This secrecy is necessary to allow the NZSIS to operate effectively. If employees could be identified by targets and others as working for the NZSIS, that would impede their ability to carry out secret operations and potentially endanger NZSIS sources in contact with those employees. The NZSIS Act therefore makes it an offence to publish the fact that a person (other than the Director of Security) is an employee of the NZSIS.

6.109 To comply with the requirement to keep their employment secret, NZSIS staff may need to use alias biographical details in everyday life. This might include an NZSIS employee saying they work for another government agency when filling out official documentation. This has the potential to result in criminal liability (for example, it is an offence under section 342 of the Immigration Act 2009 to complete documents required at the border in a manner known to be false or misleading). Civil liability may also arise from the use of alias details in non-official documentation such as insurance policies.

6.110 While it is not an offence under the GCSB Act to publish the identity of GCSB staff, they may still need to use alias biographical details to facilitate specific operations and for broader reasons. For example, it may be unsafe for staff to travel overseas to certain countries if they are required to disclose the nature of their employment.

How is cover addressed under the current legislation?

6.111 Although the Agencies' ability to create and maintain cover is crucial to their effectiveness, it is not expressly addressed in their governing legislation. Specific provisions in other legislation provide for the creation of identity information, but only in relation to NZSIS officers or persons approved to undertake activity for the NZSIS (for example, a source or agent). These provisions provide for the creation and use of births, deaths and marriages registration information,[259] driver licences[260] and electronic identity credentials[261] (for using the government's RealMe identity verification service).

6.112 The individual provisions relating to cover are not comprehensive. They do not apply to the GCSB, which also needs to be able to carry out certain activities in a manner that cannot be traced back to it. The provisions also do not cover all relevant identity information. For example, the Passports Act 1992 does not provide for the issuing of passports under false personas. That position is undesirable. The authorities responsible for issuing identity information should not be put in a position of being asked to facilitate cover arrangements without clear statutory authority. All arrangements relating to the creation and use of assumed identities should be appropriately regulated and authorised.

6.113 We note there are examples in other jurisdictions of comprehensive regimes for providing cover for intelligence officers. For example, in Australia the Crimes Act 1914 sets out a process for both intelligence and law enforcement agencies to create assumed identities for officers and authorised civilians for the purpose of performing their functions.[262] The Act also requires government agencies and permits private entities to assist in providing evidence of those assumed identities.[263] Relevant immunities from criminal liability and indemnities against civil liability apply to those acting in accordance with the statutory regime.[264]

What changes are needed?

6.114 We consider legislation should explicitly provide for the Agencies to obtain, create and use any identification information necessary for the purpose of maintaining the secrecy of their authorised activities. This should include the ability to create cover for anyone authorised to undertake activity for the Agencies. In addition, the Agencies should have the ability to obtain, create and use identification information necessary to keep the identity of their employees secret. The use of these powers should be covered by a tier 3 authorisation (policy statement) to ensure they are exercised only where necessary and proportionate.

---

[259] Births, Deaths, Marriages and Relationships Registration Act 1995, s 65.
[260] Land Transport Act 1998, s 24A.
[261] Electronic Identity Verification Act 2012, s 11.
[262] Crimes Act 1914 (AU, Cth), Part IAC.
[263] Crimes Act 1914 (AU, Cth), ss 15KJ–15KK.
[264] Crimes Act 1914 (AU, Cth), ss 15KQ and 15KS. Authorised officers or civilians acquiring or using an assumed identity have criminal immunity and a civil indemnity from the Commonwealth. Third party government employees providing evidence of assumed identities are given criminal immunity.

6.115 "Identity information" should include anything that could be used to establish identity. This would cover things such as credit cards and shell companies in addition to traditional forms of identification (for example, passports and driver licences).

6.116 There should also be corresponding immunities from civil and criminal liability for reasonable acts done in good faith to maintain cover as part of an authorised operation, or to keep the fact of a person's employment confidential. This could include, for example, protection from liability relating to the use of false documentation or misrepresentation. Relevant immunities should also apply, so far as necessary, to people or agencies involved in creating identity information at the request of the NZSIS or GCSB. Immunities are discussed more broadly below.

6.117 We note the powers and immunities relating to cover could either be incorporated through general provisions in the legislation governing the Agencies or by inserting specific provisions in other legislation as is currently the case. We recommend the former option, as it is likely to ensure greater consistency of approach and avoid gaps in the legislative scheme.

6.118 As we have discussed above,[265] the use of cover and assumed identities should be governed by a tier 3 authorisation. The authorisation, which would be referred to the Inspector-General for comment before approval by the responsible Minister, should set out internal procedures to ensure the use of identity information is appropriately managed.

6.119 In addition to the NZSIS and GCSB, there are a range of other government agencies (such as Police) that may need to conduct undercover operations. While it is outside the scope of this review, the government may wish to consider whether any other legislative amendments are required to enable this.

Recommendations

78. The legislation should explicitly provide for the Agencies to obtain, create and use any identification information necessary for the purpose of maintaining the secret nature of their authorised activities. This should include the ability to create cover for anyone authorised to undertake activity for the Agencies.

79. "Identity information" should include anything that could be used to establish identity – such as credit cards and shell companies in additional to traditional forms of identification (such as passports and driver licences).

[265] See paragraph 6.65 onward.

80. The Agencies should also have the ability to obtain, create and use identification information necessary to keep the identity of their employees confidential.

81. The use of these powers should be covered by a tier 3 authorisation (policy statement) to ensure they are exercised only where necessary and proportionate.

82. There should be corresponding immunities from civil and criminal liability for reasonable acts done in good faith to create or maintain cover as part of an authorised operation or to keep the fact of a person's employment with the NZSIS or GCSB secret.

83. These powers and immunities should be incorporated through general provisions in the legislation governing the Agencies, rather than by inserting specific exceptions in other legislation as is currently the case.

Immunities

6.120 For the Agencies to perform their functions effectively, at times they need to carry out activity that would breach the law if not enabled under their legislation. This could be anything from intercepting private communications (which is a crime under the Crimes Act 1961) to breaking the speed limit or running a red light so as not to lose a target who is under surveillance.

6.121 Under the current legislation, both the Agencies and persons assisting them have immunity from civil and criminal liability where they are acting under warrants or authorisations[266] (and, in the GCSB's case, where they are acting under a Director authorisation[267]). The immunities are slightly different in scope between the two Acts. For example, the GCSB Act immunity covers any act done in good faith to *obtain* a warrant or authorisation, whereas the NZSIS Act does not.

6.122 As discussed above, the authorisation regime under the NZSIS Act does not cover all of the NZSIS's activities. Because the immunity in the Act depends on a warrant or authorisation being in place, there is currently a significant gap in the immunities available to the NZSIS. However, under the authorisation framework we are proposing, all of the Agencies' activities would be subject to some form of authorisation under the Act. This will help to ensure that immunities are available in appropriate cases.

6.123 We recommend that the same immunities should apply to both agencies. Although the nature of their activities may be different, employees of both agencies may need to do things

[266] NZSIS Act, s 4A(6) and GCSB Act, s 21.

[267] Section 16 allows GCSB to intercept communications using an interception device where the device is not connected to an information infrastructure or installed in a place to intercept communications in that place (for example, interception of satellite and radio transmissions).

that would otherwise be unlawful when carrying out authorised activity. Given we are proposing that the Agencies should share functions and an authorisation regime, their immunities should be the same in scope.

Immunity from criminal liability

6.124 Starting with the criminal immunity, we consider no person should be subject to criminal liability for acts carried out in good faith and in a reasonable manner that he or she reasonably believes are necessary to give effect to a tier 1 or tier 2 authorisation issued under the Agencies' legislation. In addition to employees of the Agencies, this immunity would be capable of applying to anyone assisting them, such as a telecommunications company or a human source or agent acting on behalf of the NZSIS.

6.125 The immunities should also extend to any relevant minor offences or infringements that may need to be committed in the course of investigations carried out under a tier 3 authorisation (policy statement). This should cover things such as breaches of road user rules that are reasonably required to facilitate surveillance in a public place. [268]

6.126 We do not consider it necessary or appropriate to extend the Agencies' criminal immunity to acts outside the scope of an authorisation (for example, to any act necessary for the proper performance of the Agencies' functions),[269] as has been done in some other jurisdictions.[270] Under the new authorisation regime we are proposing, some level of authorisation will be available and required for all of the Agencies' intrusive activities. Unlike under the current legislation, there will no longer be gaps in the activities that are covered by the authorisation regime. As such, there should be no reason for employees to commit unlawful acts in the pursuance of unauthorised activities. Immunities will be available to employees unless they are acting unreasonably, in bad faith or outside the scope of the relevant authorisation. We note the NZSIS supported the approach we are suggesting.

6.127 The GCSB Act also provides immunity in relation to acts done in good faith to obtain a warrant or authorisation. This is consistent with the immunities for Police under the Search and Surveillance Act 2012. We consider that retaining some protection for GCSB employees when obtaining tier 1 or tier 2 authorisations, and extending this to NZSIS employees, is desirable. This will cover off any possible criminal liability that might otherwise result from the use of certain types of information in support of authorisation applications.

---

[268] We note section 166 of the Land Transport Act 1998 allows the Land Transport Agency to grant exemptions from certain road user rules, which might be one way of dealing with this issue. If there are other relevant offences the immunities should extend to, they could be specified in the legislation.

[269] We note this approach has been taken in some jurisdictions (see, for example, section 14 of the Intelligence Services Act 2001 (AU)).

[270] For example, in Australia employees and agents of the Australian Signals Directorate and Australian Security Intelligence Service are immune from civil and criminal liability for acts done outside Australia (or in support of acts outside Australia) in the proper performance of the agencies' functions: Intelligence Services Act 2001 (AU), s 14.

6.128 For example, it is conceivable that a video or publication involving extreme violence (such as a beheading video posted online by a terrorist group) might provide valuable support for an application for an authorisation. However, copying objectionable material of this nature to provide to another person (such as the Attorney-General, when considering an application for an authorisation) may amount to an offence under the Films, Videos, and Publications Classification Act 1993.[271] Employees of the Agencies should not be put at risk of criminal prosecution in this type of situation.

6.129 We do, however, see merit in placing some additional restrictions on when this immunity will apply. In order to engage the immunity, the employee must reasonably believe their actions are necessary to obtain an authorisation, and the acts must be carried out in good faith, in a reasonable manner and in accordance with the purposes of the Act. These restrictions will help to ensure that the Agencies act at all times in accordance with their statutory mandate.

Immunity from civil liability

6.130 In addition to the civil immunities set out in the Agencies' legislation (which are currently identical in scope to their criminal immunities), GCSB employees are covered by the general civil immunity in the State Sector Act 1988. Public service chief executives and employees are immune from civil liability for good-faith actions or omissions in pursuance or intended pursuance of their duties, functions, or powers.[272] We have recommended in Chapter 4 that the NZSIS should also be part of the public service. This broader civil immunity would then apply to the NZSIS as well. In our view it is desirable for the Agencies' civil immunities to be the same in scope as other public service agencies.

6.131 However, as with the Agencies' criminal immunities, the civil immunity should be capable of applying to persons assisting the Agencies. This will ensure that people cannot be penalised for complying with requests for assistance from the Agencies. A civil immunity should therefore be provided for in the Agencies' legislation. In addition to employees of the Agencies, any person acting at the request or direction of the Agencies should be protected from civil liability for acts or omissions in good faith in the pursuance or intended pursuance of the Agencies' duties, functions or powers.

6.132 We note that the Crown can be held directly liable (as opposed to vicariously liable) for breaches of the New Zealand Bill of Rights Act 1990 by public officials. This means that even though an individual public sector employee may be immune from liability, if a person's human rights have been breached they may still have a remedy against the Crown for public law compensation.[273]

[271] Films, Videos, and Publications Classification Act 1993, s 123.
[272] State Sector Act 1988, s 86.
[273] *Simpson v Attorney-General (Baigent's case)* [1994] 3 NZLR 667 (CA).

Immunity when assisting other agencies

6.133 The discussion above refers to situations where the Agencies are performing their own functions under their legislation. Where the GCSB or NZSIS is assisting another agency to perform its functions, the legislation should provide that any immunities that would apply to the agency being assisted apply to the GCSB and/or NZSIS. This is in line with the fact that, when assisting another agency, the Agencies must act within the scope of that agency's powers. They should not have a broader immunity. We note that the civil immunity under the State Sector Act would continue to apply, so this would primarily be relevant in relation to criminal liability.

Recommendations

84. The same immunities should apply to both agencies, in line with our recommendations that the Agencies share functions and an authorisation regime.

85. Immunities should also apply to anyone required to assist the Agencies, such as telecommunications companies, or to human sources or agents acting at the Agencies' request or direction.

86. The legislation should provide that no person should be subject to criminal liability for acts carried out in good faith and in a reasonable manner that are necessary to give effect to a tier 1 or tier 2 authorisation.

87. Employees of the Agencies should also have immunity from criminal liability for acts carried out in good faith, in a reasonable manner and in accordance with the purposes of the Act to obtain a tier 1 or tier 2 authorisation.

88. The immunities for employees of the Agencies should also extend to any relevant minor offences or infringements that may need to be committed in the course of investigations carried out under a tier 3 authorisation (such as breaches of road user rules).

89. Employees of the Agencies and any person acting at the request or direction of the Agencies should be protected from civil liability for acts or omissions in good faith in the pursuance or intended pursuance of the Agencies' duties, functions or powers. This is the same protection as is provided to public sector employees under the State Sector Act 1988.

90. Where the GCSB or NZSIS is assisting another agency to perform its functions, any immunities that apply to the agency being assisted should also apply to the GCSB and/or NZSIS.

Chapter 7: Accessing and using information

7.1 In this chapter we suggest the legislation be amended to clarify what information the Agencies can access from other government agencies. We also recommend restrictions on the circumstances in which the information they collect can be accessed and retained.

7.2 Both agencies have internal policies and procedures to ensure staff only intercept, collect, access and use information if it relates to the performance of a statutory function or if access is needed to implement an authorisation. We recommend this be formalised by providing in legislation that the Agencies may only examine and use information they have intercepted or collected where it is necessary for the purpose of performing one or more of the Agencies' functions, or where one of the grounds for retaining and disclosing incidentally obtained information is met.

7.3 A tier 3 authorisation (policy statement) should establish procedures to ensure compliance with this requirement, including procedures to determine when intelligence obtained under one of the Agencies' functions can be used for the purpose of fulfilling another function. Compliance with the authorisation should be monitored by the Inspector-General as part of his or her existing functions.

7.4 The length of time for which data is retained varies depending on the type of information collected and whether it is relevant to the Agencies' functions. It would therefore be impractical to have a standard requirement for the Agencies to destroy all information collected within a particular timeframe.

7.5 The legislation already requires the Agencies to destroy all intercepted or collected information as soon as practicable unless the information relates directly or indirectly to the performance of the Agencies' functions[274] or, in the case of the GCSB, if the information relates to one of the purposes listed in section 25(2) of the current GCSB Act[275] and, in the case of the NZSIS, if it relates to the prevention or detection of serious crime.[276] We recommend the current GCSB legislative provisions on the retention, destruction and disclosure of incidentally obtained information (sections 23 and 25 of the current GCSB Act) be retained and extended to the NZSIS.

[274] GCSB Act, s 23 and NZSIS Act, s 4G.

[275] These include: preventing or detecting serious crime in New Zealand or overseas; preventing or avoiding the loss of human life on the high seas; preventing or responding to threats to human life in New Zealand or overseas; and identifying, preventing or responding to threats or potential threats to the security or defence of New Zealand or any other country. The GCSB is permitted to communicate this information to the appropriate public authority either in New Zealand or overseas.

[276] NZSIS Act, s 4H. The NZSIS is permitted to communicate this information to the New Zealand Police or to any other persons that the Director thinks fit.

Access to information held by government agencies

7.6 The Agencies need to collect a range of information from a variety of sources to perform their functions in accordance with statutory requirements. In some cases, the Agencies may need to access information lawfully collected and held by other agencies. For example, cross-referencing NZSIS information against Customs and Immigration information about flight check-ins and arrivals at the border may allow the NZSIS to detect the arrival of foreign spies or suspected terrorists in New Zealand.

7.7 Datasets held by other government agencies can contain personal information about a wide range of individuals, the majority of whom will not be a security concern and therefore will not be of any interest to the Agencies. But having access to some of these datasets may allow the Agencies to confirm a person's identity, determine whether an individual they wish to target is a New Zealander, verify information they have obtained through other secret means and sources, better understand a specific target's behaviour, or even ensure the safety of staff during field operations.

7.8 The Privacy Act 1993 sets out principles for how public and private sector agencies should collect, use, disclose, store and give access to personal information. The Agencies are exempt from certain principles in the Act, including those relating to the collection, use and disclosure of personal information.[277]

7.9 In some cases the legislation that gives certain public sector agencies the authority to collect personal information restricts disclosure to specific purposes or entities. For example, Customs collects personal information at the border but is prohibited from disclosing the information unless it is doing so for certain purposes such as protecting border security or protecting the health and safety of members of the public.[278] Where such a restriction exists, the Agencies cannot access the information unless expressly authorised by legislation.[279]

7.10 Where there is no specific legislative restriction on sharing information, we understand that the Agencies' exemption from the Privacy Act principles is generally interpreted as allowing them to access personal information held by other government agencies, but only on a case-by-case basis. Given the frequency with which the Agencies may need to access certain datasets (such as arrivals information, which needs to be constantly monitored), this presents obvious difficulties.

7.11 We think there is a case for the Agencies to access certain datasets of personal information collected and held by certain public sector agencies, and to access other types of information

[277] Privacy Act 1993, s 57.
[278] Customs and Excise Act 1994, s 282A.
[279] As discussed in Chapter 8, the Countering Terrorist Fighters Legislation Bill passed in December 2014 introduced a new legislative provision allowing the NZSIS to access New Zealand Customs Service databases. However, this access is only available for counter-terrorism investigation purposes (see the Customs and Excise Act 1994, s 280M).

on a case-by-case basis. But given the potential impact on the privacy of individuals, access must be justified as both necessary to perform a statutory function of the Agencies, and proportionate to the objective being achieved. Below we set out a framework under which the Agencies should access such information.

7.12 We note the recommendations below are intended to be enabling. They should not prevent the Agencies from accessing other types of information that they are already entitled to access (for example, under the Privacy Act exemption).

Access to datasets

7.13 We recommend the legislation explicitly permit the Agencies to access and retain the following datasets:

- Customs information about border-crossing craft and persons
- Immigration databases, including Advanced Passenger Processing data
- information held in Police's National Intelligence Application, and
- births, deaths, marriages and relationships registers and citizenship registers.[280]

7.14 We also suggest that the Justice and Electoral Select Committee consider whether broader access to an electronic copy of the electoral roll would be appropriate. [281]

7.15 By enabling access to these specific datasets, we do not suggest the Agencies should be able to see or use all of the potential types of information stored on these systems. The joint protocol we recommend below should identify the types of information that will be shared based on what the Agencies need it for. In particular, we understand access to the Police National Intelligence Application is only required for operational safety purposes. For example, the NZSIS may need to run criminal history checks on individuals their staff are likely to come into contact with during operations to avoid putting them in unnecessary danger.

7.16 In every case we recommend access to and retention of datasets should be subject to a joint protocol agreed between the Minister responsible for the Agencies and the Minister responsible for the relevant agency holding the information. The joint protocol should identify the types and scope of information that will be shared and the purposes for which the

[280] There is already provision for the NZSIS to access these registers under s 75F of the Births, Deaths, Marriages and Relationships Registration Act 1995 and reg 15 of the Citizenship Regulations 2002. However, this should be extended to the GCSB, as the GCSB also needs to confirm the nationality of persons of interest in order to ensure compliance with the legislative restrictions on targeting New Zealanders.

[281] Section 116 of the Electoral Act 1993 prevents the electoral roll from being supplied, in electronic form, to any person unless the request is for research relating to a scientific matter or human health; for use by an electoral official of a local authority for any election, by-election or poll; or for use by a candidate of a political party, a member of Parliament or any other person conducting an official publicity or information campaign on behalf of the Government of New Zealand relating to electoral matters.

Agencies will use it. The protocol should be agreed in consultation with the Privacy Commissioner, who would consider whether:

- the data is needed for the Agencies to discharge their statutory functions
- only as much information will be obtained and retained as is necessary to discharge the statutory functions
- the level of interference with individuals' right to privacy, both in relation to individuals who are of security interest and individuals who may be of no interest, is balanced against the value of the information to be gained, and
- the protocol sets out appropriate procedures for the use, retention and deletion of the dataset.

7.17 Every three years, the Minister responsible for the Agencies should review each protocol, specifically the operational and legal justification for the continued use and retention of the dataset. The Inspector-General of Intelligence and Security should monitor the Agencies' compliance with each protocol.

7.18 The Agencies must ensure the information they obtain is held on secure IT systems and that a range of internal compliance and audit mechanisms are in place. This should include appropriate and regular training for staff on their professional and legal responsibilities, and processes to ensure that staff only access datasets where justified.

Access on a case-by-case basis

7.19 Some of the information held by other government agencies that might assist the Agencies is required less frequently and only in relation to specific investigations. Direct access to the datasets containing this information is therefore unnecessary and unlikely to be proportionate. Access on a case-by-case basis is more appropriate in these types of situations.

7.20 As discussed above, the Agencies can generally access government information on a case-by-case basis under the Privacy Act exemption. However, there are statutory restrictions on other agencies' ability to share certain information. We were alerted to a number of types of information in this category that we think the Agencies need to be able to access in the context of specific investigations.

7.21 We therefore recommend the legislation allow Agencies to access the following information about identifiable individuals or organisations by request on a case-by-case basis:

- tax information held by the Inland Revenue Department[282]
- driver licence photographs held by the New Zealand Transport Agency, and[283]
- National Student Identification Numbers held by the Ministry of Education.[284]

7.22 Access to this information should be in accordance with a tier 2 authorisation if it relates to a foreign person or organisation, or a tier 1 authorisation if it relates to a New Zealand citizen, permanent resident or organisation. All authorisations will be subject to review by the Inspector-General under his or her existing functions.

Recommendations

91. The legislation should provide that the Agencies may only examine and use information intercepted or collected for the purpose of performing one or more of their functions, or where one of the grounds for retaining and disclosing incidentally obtained intelligence is met.

92. A tier 3 authorisation (policy statement) should establish procedures to ensure compliance with this requirement, including procedures to determine when intelligence obtained under one of the Agencies' functions can be used for the purpose of fulfilling another function. Compliance with the policy statement should be monitored by the Inspector-General as part of his or her existing functions.

93. The current GCSB legislative provisions on the retention, destruction and disclosure of incidentally obtained information (sections 23 and 25 of the current GCSB Act) should be retained and extended to the NZSIS.

[282] Section 81 of the Tax Administration Act 1994 prohibits communication of tax information except for specific purposes such as prosecution in New Zealand or overseas, or to specific entities such as the Directors of the Serious Fraud Office, Statistics New Zealand and the Department of Internal Affairs.
[283] Section 200 of the Land Transport Act 1998 restricts access to photographic images of driver licence holders to employees of the New Zealand Transport Agency acting in the course of their official duties; any constable enforcing certain local government and road user laws with written consent from the individual to whom the image relates or an appropriate warrant; or to the next of kin of a deceased individual to whom the image relates.
[284] Section 344 of the Education Act 1989 permits the Chief Executive of the Ministry of Education to authorise persons to use national student numbers only for limited purposes such as monitoring and ensuring student enrolment and attendance, and for statistical and research purposes.

Access to datasets

94. The legislation should enable the Agencies to access and retain the following electronic datasets:

- Customs information about border-crossing craft and persons
- Immigration databases, including Advanced Passenger Processing data
- information held in Police's National Intelligence Application, and
- births, deaths, marriages and relationships registers and citizenship registers.

95. The Justice and Electoral Select Committee should be invited to consider whether access by the Agencies to an electronic copy of the electoral roll would be appropriate.

96. Access to and retention of datasets should be subject to a joint protocol agreed between the Minister responsible for the NZSIS or GCSB and the Minister responsible for the relevant agency holding the information. The joint protocol should identify the types and scope of information that will be shared and the purposes for which the Agencies will use it.

97. The protocol should be agreed in consultation with the Privacy Commissioner, who would consider whether the access is both necessary to perform a statutory function of the Agencies and proportionate to the objective.

98. The Minister responsible for the Agencies should review the protocols every three years.

99. The Agencies should be required to ensure the information they obtain is held on secure IT systems and that a range of internal compliance and audit mechanisms are in place. This would include appropriate and regular training for staff on their professional and legal responsibilities and processes to ensure staff always justify their activity on the system.

100. The Inspector-General should monitor the Agencies' compliance with each protocol.

Access on a case-by-case basis

101. The legislation should provide for access to the following information about individuals on a case-by-case basis:

- 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.

102. Access should be in accordance with a tier 2 authorisation if the information relates to a foreign person or organisation, or a tier 1 authorisation if it relates to a New Zealand citizen, permanent resident or organisation.

Chapter 8: Countering foreign terrorist fighters

8.1 Our terms of reference require us to look specifically at whether the legislative provisions introduced by the Countering Foreign Terrorist Fighters Legislation Bill in December 2014 should continue beyond their expiry on 31 March 2017 in their present or a modified form. This chapter considers those amendments and makes a number of recommendations for further reform.

8.2 With the recent rise of the Islamic State in Iraq and the Levant ("ISIL"), the phenomenon of foreign terrorist fighters ("FTFs") travelling to Middle East conflict zones has become an international security issue. On 24 September 2014 the United Nations Security Council adopted Resolution 2178, which calls on UN member states to prevent the movement of terrorists by:

- ensuring effective border controls and controls on issuance of travel documents
- employing evidence-based traveller risk assessment and screening procedures, including collection and analysis of travel data
- exchanging operational information about actions or movements of terrorists and FTFs, and
- ensuring domestic laws establish serious criminal offences sufficient to prosecute and penalise people financing, planning or perpetrating terrorist acts.

8.3 While New Zealand has had fewer people looking to travel to fight overseas than some of our partners, we are not immune from radicalisation and extremist activity. In November 2015, the Prime Minister disclosed that there were between 30 and 40 people on a government watch list, some of whom were suspected of either raising money for ISIL or attempting to travel to Syria to fight. The NZSIS told us that between December 2014 and August 2015, an average of 37 individuals were under investigation by their counter-terrorism investigators each month. A number of New Zealand citizens are known to have travelled to Syria to fight for terrorist organisations. In addition, a small number of New Zealand women have travelled to Syria and are believed to have since married jihadist fighters.

8.4 Other New Zealanders onshore have expressed intentions to conduct domestic attacks or travel offshore to join terrorist groups. The passports of some of these individuals have been cancelled or suspended to prevent their travel. However, cancelling a person's passport does carry a risk that they will react violently or turn their attention to domestic attack planning. The NZSIS believes that unsophisticated attacks or spontaneous acts of violence, as have occurred in other Western countries, remain a possibility.

8.5 Following the Security Council's resolution, the New Zealand Government conducted a targeted review of whether its capacity, capability and powers were sufficient to respond to the evolving domestic threat associated with FTFs. The review focused on interim measures that could be put in place in advance of the 2015 statutory review. In particular, the targeted review considered:

- the ability of the NZSIS to investigate and monitor suspected FTFs and other violent extremists
- the government's statutory powers to restrict and disrupt the travel of suspected FTFs, and
- whether any specific criminal offences were needed to address the FTF threat.

8.6 The recommendations of the review resulted in the Countering Terrorist Fighters Legislation Bill, an omnibus Bill that made temporary amendments to the Passports Act 1992, Customs and Excise Act 1996 and NZSIS Act. The new provisions came into force on 12 December 2014 and are subject to an expiry date of 31 March 2017.

Extended powers to cancel, suspend or refuse to issue travel documents

8.7 Amendments made to the Passports Act allow the Minister of Internal Affairs to cancel or refuse to issue passports or other travel documents for up to 36 months.[285] Where the period is greater than 12 months, the Minister must review the decision every 12 months after inviting a written submission from the affected person. The cancellation period can be extended for a further 12 months on application to a judge.

8.8 Before cancelling or refusing to issue a travel document, the Minister must believe on reasonable grounds that:[286]

- the affected person is a danger to the security of New Zealand or another country because they intend to engage in:
  - a terrorist act[287]
  - the proliferation of weapons of mass destruction, or
  - unlawful activity that is carried out for the purpose of commercial or economic gain and likely to cause serious economic damage to New Zealand, and

[285] Passports Act 1992, s 45 and sch, cl 1–6.
[286] Passports Act 1992, s 45 and sch, cl 1–6.
[287] "Terrorist act" is defined in section 5 of the Terrorism Suppression Act 2002.

- the danger to security cannot be effectively averted by other means, and

- the cancellation or refusal will prevent or effectively impede the affected person's ability to carry out the intended action.

8.9 The NZSIS provides briefings to the Minister setting out the information relevant to the Minister's assessment.

8.10 Prior to the amendments, the Minister of Internal Affairs could cancel or refuse to issue travel documents for a maximum of 12 months (with the ability to extend that period for a further 12 months on application to a judge).[288] The cancellation or refusal grounds were similar, except the Minister had no ability to cancel or refuse to issue a travel document on the basis that the person was a threat to the security of a country other than New Zealand.

8.11 The amendments also introduced a new power to suspend a person's travel documents for up to 10 working days.[289] This sought to address situations where the NZSIS becomes aware at short notice of a person seeking to travel imminently to take part in a terrorist act. The temporary suspension power can be exercised where a report is being prepared about the danger the person presents to the security of New Zealand or another country and the person is likely to travel before the report is complete.

8.12 A range of protections apply to the extended powers in the Passports Act. Existing provisions in the Act provide that if the affected person is outside New Zealand, they remain a New Zealand citizen and the Minister must issue a journey-specific emergency travel document on request to allow them to return to New Zealand.[290] Under the new provisions, where the Minister chooses to cancel or refuse to issue a travel document for a period exceeding 12 months the affected person can make a written submission regarding the length of the cancellation or refusal.

Access to Customs information for counter-terrorism purposes

8.13 Under the changes to the Customs and Excise Act, the chief executive of Customs may allow the NZSIS or Police to access a Customs database for counter-terrorism investigation purposes.[291] The Chief Executive must consult the Privacy Commissioner before granting access.

8.14 The Customs and Excise Act already allowed Customs to disclose any information (including personal information) for the purposes of (among other things):[292]

- protecting the health and safety of the public, and

[288] Passports Act 1992, ss 4A, 8A, 20A, 25A, 27B and 27E.
[289] Passports Act 1992, sch, cl 7.
[290] Passports Act 1992, ss 23(3) and 45.
[291] Customs and Excise Act 1996, s 280M.
[292] Customs and Excise Act 1996, s 282A.

- detecting, preventing, investigating or prosecuting offences punishable by imprisonment.

8.15 However, it was unclear whether this permitted Police and the NZSIS to have direct access to Customs databases. The amendment to the Act clarified that such direct access was permissible in a counter-terrorism context. The question of direct access for other purposes was left to be addressed through a separate process given the narrow focus of the Countering Foreign Terrorist Fighters Legislation Bill.[293]

NZSIS counter-terrorism powers

8.16 Amendments to the NZSIS Act increased the powers of the NZSIS to undertake surveillance of suspected terrorists. The temporary provisions allow the NZSIS to obtain visual surveillance warrants[294] and undertake warrantless surveillance (authorised by the Director of Security) for a period of up to 24 hours in situations of emergency or urgency.[295] These powers only apply to surveillance that is necessary for the detection, investigation or prevention of an actual, potential or suspected terrorist act.

8.17 Prior to these amendments, the NZSIS had no ability to conduct video surveillance on private premises. This is in contrast to Police, who are able to conduct video surveillance for law enforcement purposes under the Search and Surveillance Act 2012.[296]

8.18 As an added protection for visual surveillance warrants, the Director of Security must provide a copy of a warrant to the Inspector-General as soon as practicable after it is issued.[297] As soon as practicable after a visual surveillance warrant expires, all records resulting from the surveillance must be destroyed except to the extent they are relevant to the detection of activities prejudicial to security or the gathering of foreign intelligence essential to security.[298]

8.19 Under the urgent Director authorisation process, the Minister and the Inspector-General must be notified immediately when an authorisation is made, as well as the Commissioner of Security Warrants where domestic targets are involved.[299] The Minister or Commissioner can direct the NZSIS to cease the activity without delay. If a Director's authorisation expires and a warrant is not sought in respect of the same subject, the Minister and (where applicable) the Commissioner must determine whether the authorisation was appropriately given and refer the matter to the Inspector-General for investigation.

[293] Countering Foreign Terrorist Fighters Legislation Bill (1–1) (explanatory note) at 5.
[294] NZSIS Act, s 4IB.
[295] NZSIS Act, s 4ID.
[296] Search and Surveillance Act 2012, s 46.
[297] NZSIS Act, s 4IB(9).
[298] NZSIS Act, s 4IB(10).
[299] NZSIS Act, s 4IE.

Should the new provisions be extended?

8.20 We have already addressed issues relating to the urgent authorisation process and access to government information in chapters 6 and 7. We deal with the provisions in the Passports Act and the NZSIS's visual surveillance powers below.

Disruption of travel

8.21 Many countries have recently adopted new measures (or strengthened existing measures) to disrupt the travel of potential FTFs. These measures are often controversial, as they impact on the fundamental right of individuals to leave a country. At the same time, governments are legitimately concerned to stem the flow of FTFs to conflict zones. The United Nations Security Council has recognised the need to prevent terrorists from travelling and has urged member states to take appropriate action.

8.22 The approaches taken in other jurisdictions have included significantly longer passport cancellation periods than the maximum permitted in New Zealand,[300] the ability to revoke the citizenship of dual nationals,[301] the ability to detain people to prevent the commission of terrorist acts,[302] and the creation of criminal offences for those who travel to or remain in specified conflict zones.[303] In light of the lower threat level faced by New Zealand compared to some of our partners and the significant human rights implications of such measures, we do not consider them to be appropriate in a New Zealand context.

8.23 We do think it is important as a matter of principle that New Zealand should seek to prevent nationals from travelling to conflict zones to participate in the kinds of acts to which the passport cancellation provisions apply.[304] However, any measures to achieve this must be justified in light of the impact on individuals' rights and appropriate safeguards should apply to their use. For this reason (as discussed further below) we recommend the involvement of a judicial commissioner wherever a person's travel document is cancelled or their application for a travel document is refused on security-related grounds.

Three-year cancellation and refusal period for travel documents

8.24 The amendments to the Passports Act in December 2014 allow the Minister of Internal Affairs to cancel or refuse to issue a travel document for up to three years, compared to a previous maximum of 12 months.

---

[300] Canadian Passport Order (CAN), ss 10.1–10.4 and 11.1 (10 years).
[301] British Nationality Act 1981 (UK), s 40; Australian Citizenship Act 2007, ss 33AA and 35 (as amended in December 2015 by the Australian Citizenship Amendment (Allegiance to Australia) Bill 2015).
[302] Criminal Code (CAN), ss 83.3, 810.011 and 811.
[303] Criminal Code Act 1995 (AU), ss 119.1–119.3.
[304] As set out in paragraph 8.8 above.

8.25 This amendment was made to address the small number of cases where information is available at the time a travel document is cancelled to suggest the person's intentions and circumstances are unlikely to change in the following 12 months. For example, intelligence might suggest they are not intending to travel for another 18 months, or are prepared to "lay low" until the 12-month cancellation period has passed.

8.26 Before the amendment, there was no ability to set a longer cancellation period in these cases. However, once the 12-month cancellation period expired, the Minister could refuse any application the individual made for a travel document. An affected person has no automatic right to obtain a travel document once the cancellation period has ended and the legislation does not limit the number of times that an application can be refused. In practice this meant that a person could be deprived of a travel document indefinitely, on a rolling 12-month basis. This resulted in considerable uncertainty for the affected person regarding the length of time for which they would be prevented from travelling.

8.27 Repeated refusals to issue a travel document are still possible under the amended provisions. This is necessary, in our view, as the Minister should not be placed in a position of being required to issue a travel document to a person who still poses a risk. However, we consider that the ability to provide for a longer cancellation period rather than relying on repeated refusals provides a greater level of transparency and certainty to the affected person. The requirement for 12 monthly reviews by the Minister means there is still an opportunity for the cancellation period to be shortened if circumstances change.

8.28 A three-year cancellation period is unlikely to be needed in most cases, and should not be treated as the default position. However, we recognise there may be cases where travel and attack planning extends over a long period, and a 12-month cancellation period may be insufficient. We consider the maximum three-year cancellation period should continue to be available in such cases.

8.29 Some of the public submissions we received suggested that decisions to cancel or refuse to issue travel documents on national security grounds should be judicially reviewed. We agree. Cancelling or refusing to issue a passport or other travel document impinges on a person's right to leave New Zealand and, as such, can have a significant impact on the individual concerned. We recommend the involvement of a judicial commissioner to ensure the power is only exercised in appropriate circumstances.

8.30 Any decision by the Minister of Internal Affairs under the relevant provisions in the Passports Act should be referred to the Chief Commissioner of Intelligence Warrants. A judicial commissioner should review the decision and have the ability to overturn it if one of the grounds for judicial review is made out. This automatic review process would be in addition to the existing ability for an affected person to seek judicial review of the Minister's decision.

10 working day suspension of travel documents

8.31 The amendments to the Passports Act also introduced a 10 working day temporary suspension period to prevent a person from travelling. This amendment addressed an obvious gap in the Act. Previously, if a suspected FTF was seeking to travel and the NZSIS was not alerted to this until shortly before departure, there was no ability to keep the person in the country while the process for cancelling their passport was completed. We note a similar provision has been introduced in Australia, allowing suspension for up to 14 days.[305]

8.32 In our view, allowing a travel document to be suspended for a maximum of 10 working days is a reasonable period to allow the NZSIS to gather all the relevant information and the Minister to fully consider it. Shortening the suspension period may lead to rushed decisions, which is undesirable given the significant impact of cancellation on the individual involved. We therefore recommend that the 10 working day suspension period be retained.

Grounds for cancelling or refusing to issue travel documents

8.33 Under the current provisions, the grounds on which the Minister can cancel or refuse to issue a travel document refer to the definition of "terrorist act" in the Terrorism Suppression Act. We note that definition applies to a relatively narrow set of activities and may not capture all of the situations in which it might be appropriate to prevent a person from travelling to engage in violent extremism. For instance, it may not cover people seeking to travel to engage in training activities with a terrorist organisation. The government may wish to review the grounds for cancelling and refusing to issue travel documents to ensure they remain adequate in the current international environment.

Visual surveillance

8.34 Prior to December 2014, the NZSIS had no authority to carry out visual surveillance on private property. As noted in the Regulatory Impact Statement for the Countering Foreign Terrorist Fighters Legislation Bill, this lack of visual surveillance powers was a significant gap in NZSIS's capabilities.[306] Law enforcement agencies have had the ability to conduct visual surveillance in criminal investigations since 2012.[307] By contrast, the NZSIS was unable to use visual surveillance to monitor people who were training with weapons or planning terrorist attacks.

8.35 The changes to the NZSIS Act in December 2014 have allowed the NZSIS to make better use of technological developments to increase the effectiveness of counter-terrorism investigations. The power has not been used on a regular basis; since its introduction it has only been used

[305] Australian Passports Act 2005, s 22A (inserted by the Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014, schedule 1, cl 20).
[306] Department of Prime Minister and Cabinet *Regulatory Impact Statement: Foreign Terrorist Fighters – targeted review of relevant legislation* (12 November 2014) at [14].
[307] Search and Surveillance Act 2012.

twice. We consider this reflects a proper level of caution both within the NZSIS and at a ministerial level about using intrusive powers.

8.36 We think it is important that the Agencies should, as a general principle, have the ability to make use of modern technologies to perform their functions more efficiently and effectively (while noting that the level of intrusiveness of particular technologies will require assessment on a case-by-case basis). This is particularly so given the small size of the Agencies and the resourcing pressures they face. If technology can allow better use of scarce resources, that should be encouraged.

8.37 Visual surveillance of a private place can entail significant intrusion on an individual's privacy. Like other intrusive powers, it should only be used by intelligence and law enforcement agencies where the threat level is significant and the information required to mitigate or avert it cannot realistically be obtained in a less intrusive way. However, we consider there are situations where its use is justified. We recommend that the legislation should continue to enable visual surveillance by the Agencies in appropriate circumstances.

8.38 Under the temporary provisions introduced in the Countering Foreign Terrorist Fighters Legislation Bill, visual surveillance was dealt with separately from other warranted NZSIS powers and subject to different requirements. It also only applied in a counter-terrorism context. This was largely a product of the targeted, temporary nature of the legislation and the fact that it was passed under urgency.

8.39 As a matter of principle, we see no reason why visual surveillance should be treated differently from other surveillance methods. It should be covered by the same strengthened authorisation regime we have recommended for other intrusive activities. Under this regime the Attorney-General will need to be satisfied that the action is necessary and proportionate, and, where a New Zealander is involved, a judicial commissioner will also need to be satisfied the authorisation is lawful. In addition, the Inspector-General will continue to have oversight of how visual surveillance powers are exercised.

8.40 Although the December 2014 amendments focused on counter-terrorism, visual surveillance could assist the Agencies to perform their intelligence functions in other contexts. For example, it may enable better monitoring of foreign intelligence agents who present a threat to the security of New Zealand. Provided the relevant thresholds for obtaining a tier 1 or tier 2 authorisation are met, we recommend that visual surveillance should be able to be used regardless of the subject matter of the investigation.

8.41 This approach is consistent with the other methods used by the Agencies. For example, there is no restriction on the types of investigations for which listening devices can be used. It is also consistent with the approach taken in the Search and Surveillance Act in relation to Police warrants. The Search and Surveillance Act treats visual surveillance devices in the same way as other surveillance devices, and does not restrict their use to certain types of investigations.

Recommendations

Disruption of travel

103. The maximum three-year cancellation period for travel documents should continue to apply.

104. 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. A judicial commissioner should review the decision and have the ability to overturn it if one of the grounds for judicial review is made out.

105. 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.

Visual surveillance

106. The legislation should continue to enable visual surveillance by the Agencies in appropriate circumstances.

107. Visual surveillance powers should be subject to the new authorisation regime we have proposed and treated the same as other types of surveillance. They should not be restricted to counter-terrorism investigations.

Concluding remarks

We have set out our recommendations in full in the relevant chapters of this report and in Annex C. In concluding, we would like to highlight some key points that we think the government should take into consideration, although they may not all require legislative change.

First, we encourage the Agencies to be as transparent as possible without harming New Zealand's interests. They should make a concerted effort to respond to Official Information Act requests as fully as possible, as well as proactively releasing information to keep the New Zealand public informed about their activities and the reasons for them. The current directors have already made significant progress in publicly explaining the roles of the Agencies and the reasons for them, but further work in this area will continue to improve public understanding over time. As we indicated in Chapter 4, the government should also consider greater engagement with the public about threat levels. This could include releasing some of the National Assessment Bureau's assessments and information about New Zealand's national security priorities.

Second, while we see a continuing need for secret intelligence, we also think there is scope for greater use of open source information. Intrusive intelligence collection methods should only be used as a last resort, where the information required cannot reasonably be obtained in a less intrusive way. We suggest the government consider dedicating more resource to the collection and analysis of open source information.

Third, we have suggested that the government consider strengthening the co-ordination of intelligence collection. While we were not required to look at this under our terms of reference, it became apparent to us that good co-ordination is crucial in order for the Agencies' work to meet the government's needs. A single appropriation and a central co-ordinator would help to achieve more efficient use of resources towards commonly identified priorities and activities.

Finally, a recurring theme throughout our review has been the need for the Agencies to work together and with the broader public sector more effectively. In the modern technological and threat environment, the Agencies will be of little use if they cannot do this. Information from human or electronic sources will usually only provide pieces of a puzzle; they must be combined to provide a full picture. We therefore encourage the Agencies to develop a closer working relationship. While this process has already begun since the co-location of the Agencies, we consider there is much greater scope for co-operation. The recommendations we have made for legislative change would facilitate this.

The Agencies should also increase their focus on engagement with the broader public sector. Intelligence is only useful to the extent that it can be used by other public authorities and ministers to inform decisions and actions. At times the Agencies will need to work closely with agencies such as Police and the Defence Force to enable this. We have recommended that the Agencies enter into joint protocols with other public authorities they need to work closely with. These protocols would set out mutually agreed guidelines to avoid uncertainty about when and how to engage.

We reiterate our view that the Agencies have made significant progress since Rebecca Kitteridge's review of compliance by the GCSB in 2013, assisted by strengthened oversight by the Inspector-General's office. However, the Agencies are still operating in an environment of some legal uncertainty with legislative powers that are out of date. This makes it difficult for the Agencies to perform their functions effectively, makes the Inspector-General's role more challenging than it might otherwise be and inhibits informed public debate about the appropriate role of the Agencies. We believe the recommendations in this report, if adopted, will go a long way toward addressing these issues.

Annex A: Terms of Reference

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

1. 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;

2. 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:

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

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

5. 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:

6. 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;

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

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

9. previous relevant reviews and progress towards implementing their recommendations;

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

11. 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: Meetings with individuals and organisations

New Zealand

Government agencies and Crown entities

Government Communications Security Bureau

New Zealand Security Intelligence Service

Security Intelligence Group, Department of the Prime Minister and Cabinet

New Zealand Police

Independent Police Conduct Authority

Ministry of Defence

New Zealand Defence Force

Ministry of Foreign Affairs and Trade

Immigration New Zealand

New Zealand Customs Service

State Services Commission

New Zealand Law Commission

Human Rights Commission

Government Chief Information Officer

Oversight bodies

Cheryl Gwyn, Inspector-General of Intelligence and Security

Ben Keith, Deputy Inspector-General of Intelligence and Security

Hon Sir Bruce Robertson, Commissioner of Security Warrants

Members of the Intelligence and Security Committee of Parliament

John Edwards, Privacy Commissioner

Dame Beverly Wakem, Chief Ombudsman

Academics, legal professionals and other interested people and organisations

Amnesty International New Zealand

Spark New Zealand

Vodafone New Zealand

Professor Robert Ayson, Professor of Strategic Studies at Victoria University of Wellington

Dr Jim Rolfe, Director, Centre for Strategic Studies, Victoria University of Wellington

John Ip, Senior Law Lecturer, University of Auckland

Dr Paul Buchanan

Deborah Manning, Barrister

Stuart Grieve QC, Barrister

Sir Maarten Wevers, former Chief Executive of the Department of Prime Minister and Cabinet

Keith Locke, former Green Party MP

Political parties

New Zealand Labour Party

New Zealand First Party

New Zealand ACT Party

New Zealand United Future Party

We also met with other individuals and organisations who wished to remain anonymous.

Australia

Hon Margaret Stone, Inspector-General of Intelligence and Security

Jake Blight, Deputy Inspector-General of Intelligence and Security

Dr Vivienne Thom, former Inspector-General of Intelligence and Security

Office of National Assessments (ONA)

Australian Secret Intelligence Service (ASIS)

Australian Signals Directorate (ASD)

Australian Security Intelligence Organisation (ASIO)

Department of the Prime Minister and Cabinet

Representative of the Parliamentary Joint Committee on Intelligence and Security

New Zealand High Commission in Canberra

Michael L'Estrange, Professor of National Security Policy, Australian National University

Allan Gyngell, National Security College Visiting Fellow, Australian National University

UK

David Anderson QC, Independent Reviewer of Terrorism Legislation

His Excellency Jonathan Sinclair, British High Commissioner to New Zealand

Representatives from the Secret Intelligence Service (SIS or MI6)

Representatives from the Government Communications Headquarters (GCHQ)

USA

Representatives from the Central Intelligence Agency (CIA)

Representatives from the National Security Agency (NSA)

Canada

Linda Goldthorp, Project Director of the Community 2020 review

Annex C: Full list of recommendations

Transparency and accountability

Single Act

1. The objectives, functions and powers of the Agencies and their oversight should be consolidated into a single Act. The purpose of the Act should be to protect New Zealand as a free, open and democratic society.

2. The single Act should require that every action taken towards setting priorities and collecting, analysing, assessing and using intelligence should be done with integrity and in accordance with New Zealand law, including human rights law. The Act should also retain the current legislative requirement that the Agencies conduct their activities free from all political influence.

Integrating the Agencies within the public sector

3. The NZSIS should be established as a public service department and all relevant provisions of the State Sector Act 1988 should apply, subject to specific exemptions or exceptions as appropriate.

4. The NZSIS Director of Security and the Director of GCSB should be appointed (or removed from office for just cause) by the State Services Commissioner. The State Services Commissioner should set the remuneration and terms and conditions of employment and undertake regular performance reviews.

5. The NZSIS should be required to prepare a Code of Conduct based on the principles of the proposed single Act. This could be either a variation of the State Services Commissioner's Standards of Integrity and Conduct or a bespoke Code of Conduct. The Code should be developed in consultation with the State Services Commissioner.

6. The Agencies should continue to consult with the Leader of the Opposition about matters relating to security and the GCSB's intelligence gathering and assistance functions. The Agencies should also, as they see fit, consult with the leader of any other political party in Parliament as defined in the Standing Orders of the House of Representatives about such matters.

Arrangements with foreign partners

7. The legislation should explicitly enable the Agencies to co-operate and share intelligence with foreign jurisdictions and international organisations.

8. There should be a requirement that this co-operation and sharing be consistent with the purposes of the single Act and the Agencies' obligations to act in accordance with New Zealand law, including human rights obligations.

9. Any future bilateral or multilateral arrangements entered into with foreign jurisdictions or international organisations should be referred to the Intelligence and Security Committee ("ISC") to be noted.

10. The Minister responsible for the Agencies should formulate standard terms for *ad hoc* intelligence co-operation or sharing with foreign jurisdictions and international organisations outside of bilateral or multilateral arrangements. The terms should be consistent with the Agencies' obligations to act in accordance with New Zealand law, including human rights obligations, and be referred to the Inspector-General for comment. Once finalised, the standard terms should be referred to the ISC to be noted.

11. For both formal and *ad hoc* intelligence sharing arrangements, 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.

Centralising intelligence assessments

12. The government should consider including the role and functions of the National Assessments Bureau ("NAB") in the single Act. Its function should be to assess and prepare reports relating to New Zealand's national security and economic and international interests, and to provide these reports to the relevant decision-makers.

13. The government should review the current placement of the Combined Threat Assessments Group within the NZSIS and consider whether it might more appropriately be situated within the NAB.

Role of the Inspector-General of Intelligence and Security

14. We recommend section 4 of the Inspector-General of Intelligence and Security Act be replaced with a clear statutory statement on the Inspector-General's role. The purpose of the Inspector-General should be to ensure the Agencies are acting in compliance with their legislative framework, to independently investigate complaints about the Agencies, and to advise the government and the Intelligence and Security Committee of Parliament on matters relating to the oversight of the Agencies.

15. In order to ensure the independence of the Inspector-General, he or she should be appointed by the Governor-General on the recommendation of the House of Representatives and the Inspector-General's Office should be funded through an appropriation that is separate from that of the Agencies.

16. The Inspector-General should be appointed for an initial term of five years to allow sufficient time to build expertise in the technical and specialised work of the Agencies. The current reappointment provision should continue (that is, the ability to be reappointed for one further three-year term).

17. The Minister responsible for the Agencies should receive and comment on (but not approve) the Inspector-General's draft work programme. The legislation should permit the work programme to be made publicly available.

18. Where the Inspector-General undertakes an inquiry at the request of the Intelligence and Security Committee, he or she should report back to the Committee on any findings. The Minister's response to the findings should be made available to the Committee.

19. Where the inquiry is initiated at the Inspector-General's own motion or at the request of the responsible Minister or the Prime Minister, the Inspector-General should be allowed, with the agreement of the responsible Minister or Prime Minister, to present his or her findings to the Intelligence and Security Committee. The current provision allowing the Minister to provide his or her response to the Committee should remain.

20. The category of persons who can complain to the Inspector-General should be extended beyond New Zealand persons. The Inspector-General should have discretion as to whether to inquire into any complaint by a non-New Zealand person. The exercise of this discretion should not be subject to a judicial review challenge.

21. The legislation should clarify that the Inspector-General's review of authorisations is not merely in relation to procedural matters but is a comprehensive look behind the face of the authorisation. This includes reviewing the Agencies' case for an authorisation and how the authorisation was implemented.

22. The current restriction on the Inspector-General inquiring into operationally sensitive matters unless strictly necessary to perform his or her functions should be removed.

23. In order to preserve the independent nature of its role, the Advisory Panel should no longer include the Inspector-General.

24. The legislation should be amended to clarify that the relevant sections of the Protected Disclosures Act apply in the event of a protected disclosure by an employee of the Agencies.

Role of the Intelligence and Security Committee

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

26. The members of the ISC should be nominated by the Prime Minister after consultation with the Leader of the Opposition and subsequently be endorsed by the House of Representatives. The Committee should also elect its own chairperson.

27. The government should consider extending the ISC's examination and review functions to the National Assessments Bureau.

28. The ISC should be authorised to request (but not require) the Inspector-General 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.

29. The government should in general refer proposed legislation relating to intelligence and security matters to an appropriate select committee. It should consider referring specific classified material in the context of proposed legislation to the ISC, which would then report its conclusions to the select committee.

What should the Agencies do?

What should the Agencies' objectives be?

30. The Agencies should have common objectives and should carry out their functions in pursuit of those objectives only. The objectives should be to contribute to:

- the protection of New Zealand's national security, including its economic security and the maintenance of international security (which can indirectly affect domestic security)
- New Zealand's international relations and well-being, and
- New Zealand's economic well-being.

What should the Agencies' functions be?

31. The Agencies should have common functions. These common functions should include:

Collecting intelligence

- Collecting and analysing intelligence in accordance with the government's priorities.
- Providing any intelligence collected and any analysis of the intelligence to:
  - the Minister
  - the National Assessments Bureau for assessment, and
  - any person, office holder, entity or class of persons, office holders or entities (whether in New Zealand or overseas) authorised by the Minister to receive the intelligence.

Protective security

- Co-operating with, advising and assisting public authorities (including overseas authorities) and any other person, office holder, entity or class of persons, office holders or entities authorised by the Minister on protective security matters.
- "Protective security" should be defined to include the Agencies' current functions in relation to the protection of information, people and assets against security threats (for example, cyber security, information assurance and vetting).

Assisting other government agencies

- Co-operating with each other, and with Police and the Defence Force, and assisting those agencies to carry out their functions in accordance with their governing legislation, and

- Co-operating with and assisting any other government agency or entity (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.

32. The Agencies should, as a matter of practice, develop joint operating protocols with other government agencies (for example, between the NZSIS and Police).

Protecting New Zealanders

33. The legislation should clearly set out the circumstances in which the Agencies can direct their activities towards New Zealand citizens and permanent residents, and organisations with their centre of management and control in New Zealand ("New Zealanders").

34. The Agencies should be able to carry out activity for the purpose of targeting New Zealanders where it is necessary in order to protect national security. They should only be able to carry out activities for the wider purposes of contributing to New Zealand's economic and international well-being where those activities target foreign persons and organisations.

35. The government should review the definitions of "foreign person" and "foreign organisation" in order to narrow the circumstances in which they can apply to New Zealanders.

36. The restriction on the GCSB taking any action for the purpose of intercepting New Zealanders' private communications when performing its intelligence function (section 14 of the GCSB Act) should be removed.

37. Instead, protections for New Zealanders should be implemented through a strengthened authorisation framework. If an agency wishes to carry out activity for the purpose of targeting a New Zealander (including those falling within the narrowed definitions of "foreign person" and "foreign organisation"), a warrant approved by both the Attorney-General and a judicial commissioner should be required.

38. Our terms of reference explicitly require us to consider the definition of "private communication" in the GCSB Act. Because we are recommending that section 14 of the Act be removed, the term "private communication" would no longer need to be used or defined in the legislation.

What is national security?

39. "National security" should be defined in legislation. This is because we are recommending a distinction between national security and the Agencies' other objectives for the purpose of defining the situations in which they may direct their activities at New Zealanders.

40. The definition should be broad in order to reflect the wide-ranging and rapidly changing nature of threats to New Zealand's status as a free, open and democratic society. It should be defined as follows:

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 or safety of New Zealanders overseas
- threats, or potential threats, that may cause serious harm to the life, 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 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.

How should the Agencies operate?

A comprehensive authorisation regime

41. The legislation should require some form of authorisation for all of the Agencies' intelligence and security activities that involve gathering information about individuals and organisations, to ensure that appropriate safeguards apply to everything they do.

42. There should be a three-tiered approach to authorisation of the Agencies' activities, with higher levels of scrutiny applying to activity that targets a New Zealand citizen or permanent resident, or an organisation that has its centre of management and control in New Zealand ("New Zealander").

Tier 1 authorisation – warrant approved by the Attorney-General and a judicial commissioner

43. The highest level of authorisation would be a warrant approved by the Attorney-General and a judicial commissioner ("tier 1 authorisation"). A tier 1 authorisation should be required for any activity that would otherwise be unlawful that is for the purpose of targeting a New Zealander.

44. Warrants should be able to permit the following types of activity:

- interception of communications, including metadata
- acquisition of information held by third parties (such as telecommunications companies, internet service providers, banks and government agencies – who would be required to comply where reasonably practicable – and foreign intelligence agencies)
- accessing an information infrastructure
- surveillance (including using video, listening and electronic tracking devices, and physical surveillance)
- use of human sources.

45. Both the Attorney-General and judicial commissioner would need to be satisfied that the statutory criteria for issuing a tier 1 authorisation are met. The Attorney-General would also take into account broader national interest considerations and would have discretion to decline to issue an authorisation even if the criteria are met. The judicial commissioner would consider the legality of the application, including consistency with human rights laws.

46. The Attorney-General could, as is currently the case, be the Minister responsible for the Agencies as well, and this should not prevent him or her from approving authorisations. In fact, we see considerable benefit in the same person having this dual role.

47. As an additional safeguard, the legislation should provide for review warrants (issued through the same process as other tier 1 authorisations). A specific review warrant would be required if the Agencies wish to analyse incidentally obtained intelligence for the purpose of an operation or investigation targeting a New Zealander.

48. Any incidentally obtained intelligence should be destroyed unless a review warrant is obtained or one of the grounds for disclosing incidentally obtained information to public authorities is met.

Tier 2 authorisations – warrant approved by the Attorney-General

49. The second tier of authorisation would be a warrant issued by the Attorney-General ("tier 2 authorisation"). Tier 2 authorisations would be required for the same types of activity as tier 1 authorisations, but where it is not for the purpose of targeting a New Zealander.

Tier 3 authorisations – policy statement approved by the responsible Minister

50. The lowest level of authorisation would be a policy statement approved by the Minister responsible for the Agencies after being referred to the Inspector-General for comment ("tier 3 authorisation").

51. Tier 3 authorisations should apply to the Agencies' intelligence and security activities that involve gathering information about individuals and organisations but are lawful without a warrant or authorisation (for example, open source intelligence collection, surveillance in public places or access to information infrastructures with consent).

52. A tier 1 or 2 authorisation should not ordinarily be required for activity that is permitted under the general law. However, the Minister should be able to specify in a tier 3 authorisation that a higher level of authorisation must be sought for particular activities, for example because of the level of risk or intrusion on privacy associated with the activity.

53. Each tier 3 authorisation should set out what information or activity it applies to, the purposes for which that information can be collected or activity carried out, the methods that can be used and any protections that need to be put in place (for example, privacy protections).

54. Tier 3 authorisations should apply for a maximum of three years before requiring renewal.

Basis for granting tier 1 and 2 authorisations

55. Before issuing a tier 1 or 2 authorisation, the legislation should require the Attorney-General, and the judicial commissioner in the case of tier 1 authorisations, to be satisfied that:

- the proposed activity is necessary either:
  - for the proper performance of one of the agency's functions, or
  - to test, maintain or develop capabilities or 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 authorisation 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 the Act.

56. The Attorney-General should be required to refer applications for tier 1 and tier 2 authorisations to the Minister of Foreign Affairs for comment if the proposed activity is likely to have implications for New Zealand's foreign policy or international relations.

Other matters relating to tier 1 and 2 authorisations

57. Tier 1 and 2 authorisations should be valid for up to 12 months, as is currently the case.

58. Instead of identifying a particular person, place or thing as the target, some tier 1 and tier 2 authorisations should be able to specify the type of information sought and the operational purposes for which it is required.

59. However, the legislation should contain a presumption in favour of targeted authorisations. The Attorney-General, and the judicial commissioner in the case of tier 1 authorisations, should only be able to issue a purpose-based authorisation where satisfied it is necessary and proportionate in the circumstances, and that the outcome sought could not reasonably be achieved through the use of a targeted authorisation.

60. The ability to obtain purpose-based authorisations should apply to the following types of authorisations:

- tier 1 and 2 authorisations to intercept communications, including metadata
- tier 1 and 2 authorisations to acquire information held by third parties (including foreign partners)
- tier 2 authorisations to access an information infrastructure
- tier 2 authorisations to carry out surveillance.

61. In relation to the remaining types of authorisations:

- tier 1 and 2 authorisations permitting the use of human sources should be required to identify the source and the information they are seeking to obtain
- tier 1 authorisations allowing surveillance should be required to identify the specific target (by identity, place or selector such as a phone number)
- tier 1 authorisations to access information infrastructures should be required to specify the information infrastructure or class of information infrastructures targeted.

62. Where an individual is required to be identified in an authorisation, the legislation should allow this to occur through a description (such as a job title or code name) where the individual cannot be identified by name, or to allow for role succession.

63. The legislation should also allow authorisations and warrants to be amended or revoked.

Records and reporting on authorisations

64. The Agencies should be required to keep a register of all authorisations issued (tiers 1, 2 and 3). The register should be made available to the Inspector-General, the Minister responsible for the Agencies, the Attorney-General and the judicial commissioners.

65. The Agencies' annual reports should include reporting on the outcome of tier 1 and tier 2 authorisations (including review warrants). This would allow the Inspector-General to monitor whether necessity and proportionality is being accurately judged at the point when authorisations are issued.

Judicial commissioner

66. A panel of at least three judicial commissioners should be introduced, headed by a Chief Commissioner of Intelligence Warrants (in place of the current single Commissioner of Security Warrants). At least one judicial commissioner should be available at all times to ensure that applications for tier 1 authorisations can be dealt with promptly.

67. The judicial commissioners should either be retired judges, as the current Commissioner is, or sitting judges, as the role will not be full time. This will expand the pool of potential candidates. Having sitting judges as commissioners would enable them to be designated to sit on national security-related cases as well.

Authorisation in urgent situations

68. 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 (or another minister designated to act on his or her behalf). "Urgent" means where:

- there is an imminent threat to the life or safety of any person, or
- the delay associated with obtaining a tier 1 authorisation through the ordinary process is likely to seriously prejudice national security.

69. 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 and consider it in the ordinary way.

70. If the Commissioner or Attorney-General declines to confirm the authorisation, any intelligence collected under the interim authorisation should be destroyed unless one of the grounds for retaining and disclosing incidentally obtained intelligence is met.

71. In urgent situations a tier 1 authorisation (including an interim authorisation) or a tier 2 authorisation could be granted by the Attorney-General or designated minister orally – for example, over the phone – provided the director of the agency certifies the approval has been given.

72. The Prime Minister should be required to designate a minister to have a standing power to act on behalf of the Attorney-General in the event that the Attorney-General cannot be contacted.

73. The Prime Minister should also be required to designate a minister to act on behalf of the Minister of Foreign Affairs when he or she is unavailable, for the purpose of providing comment on tier 1 and tier 2 authorisation applications.

74. As a last resort, the legislation should provide for a Director authorisation. Such an authorisation could only be given where obtaining an interim authorisation or a tier 2 authorisation from the Attorney-General or designated minister would cause delay to such an extent that the purpose of obtaining it would be defeated (for example, because the threat to a person's life or safety is likely to eventuate before the authorisation could be obtained).

75. Where an urgent Director authorisation is granted, the Director should notify the Attorney-General (and, for activity requiring a tier 1 authorisation, the Chief Commissioner of Intelligence Warrants) without delay and provide a full application within 24 hours.

76. Any interim or oral authorisations and supporting documentation should be referred to the Inspector-General as soon as practicable.

77. Each agency should be required to state in its annual report how many times the urgent authorisation processes were used in the reporting year.

Cover for operations and employees

78. The legislation should explicitly provide for the Agencies to obtain, create and use any identification information necessary for the purpose of maintaining the secret nature of their authorised activities. This should include the ability to create cover for anyone authorised to undertake activity for the Agencies.

79. "Identity information" should include anything that could be used to establish identity – such as credit cards and shell companies in additional to traditional forms of identification (such as passports and driver licences).

80. The Agencies should also have the ability to obtain, create and use identification information necessary to keep the identity of their employees confidential.

81. The use of these powers should be covered by a tier 3 authorisation (policy statement) to ensure they are exercised only where necessary and proportionate.

82. There should be corresponding immunities from civil and criminal liability for reasonable acts done in good faith to create or maintain cover as part of an authorised operation or to keep the fact of a person's employment with the NZSIS or GCSB secret.

83. These powers and immunities should be incorporated through general provisions in the legislation governing the Agencies, rather than by inserting specific exceptions in other legislation as is currently the case.

Immunities

84. The same immunities should apply to both agencies, in line with our recommendations that the Agencies share functions and an authorisation regime.

85. Immunities should also apply to anyone required to assist the Agencies, such as telecommunications companies, or to human sources or agents acting at the Agencies' request or direction.

86. The legislation should provide that no person should be subject to criminal liability for acts carried out in good faith and in a reasonable manner that are necessary to give effect to a tier 1 or tier 2 authorisation.

87. Employees of the Agencies should also have immunity from criminal liability for acts carried out in good faith, in a reasonable manner and in accordance with the purposes of the Act to obtain a tier 1 or tier 2 authorisation.

88. The immunities for employees of the Agencies should also extend to any relevant minor offences or infringements that may need to be committed in the course of investigations carried out under a tier 3 authorisation (such as breaches of road user rules).

89. Employees of the Agencies and any person acting at the request or direction of the Agencies should be protected from civil liability for acts or omissions in good faith in the pursuance or intended pursuance of the Agencies' duties, functions or powers. This is the same protection as is provided to public sector employees under the State Sector Act 1988.

90. Where the GCSB or NZSIS is assisting another agency to perform its functions, any immunities that apply to the agency being assisted should also apply to the GCSB and/or NZSIS.

Accessing and using information

91. The legislation should provide that the Agencies may only examine and use information intercepted or collected for the purpose of performing one or more of their functions, or where one of the grounds for retaining and disclosing incidentally obtained intelligence is met.

92. A tier 3 authorisation (policy statement) should establish procedures to ensure compliance with this requirement, including procedures to determine when intelligence obtained under one of the Agencies' functions can be used for the purpose of fulfilling another function. Compliance with the policy statement should be monitored by the Inspector-General as part of his or her existing functions.

93. The current GCSB legislative provisions on the retention, destruction and disclosure of incidentally obtained information (ss 23 and 25 of the current GCSB Act) should be retained and extended to the NZSIS.

Access to datasets

94. The legislation should enable the Agencies to access and retain the following electronic datasets:

- Customs information about border-crossing craft and persons
- Immigration databases, including Advanced Passenger Processing data
- information held in Police's National Intelligence Application
- births, deaths, marriages and relationships registers and citizenship registers.

95. The Justice and Electoral Select Committee should be invited to consider whether access by the Agencies to an electronic copy of the electoral roll would be appropriate.

96. Access to and retention of datasets should be subject to a joint protocol agreed between the Minister responsible for the NZSIS or GCSB and the Minister responsible for the relevant agency holding the information. The joint protocol should identify the types and scope of information that will be shared, and for what purposes the Agencies will use it.

97. The protocol should be agreed in consultation with the Privacy Commissioner, who would consider whether the access is both necessary to perform a statutory function of the Agencies and proportionate to the objective.

98. The Minister responsible for the Agencies should review the protocols every three years.

99. The Agencies should be required to ensure the information they obtain is held on secure IT systems and that a range of internal compliance and audit mechanisms are in place. This would include appropriate and regular training for staff on their professional and legal responsibilities and processes to ensure staff always justify their activity on the system.

100. The Inspector-General should monitor the Agencies' compliance with each protocol.

Access on a case-by-case basis

101. The legislation should provide for access to the following information about individuals on a case-by-case basis:

- tax information held by the Inland Revenue Department
- driver licence photographs held by the New Zealand Transport Agency
- National Student Identification Numbers held by the Ministry of Education.

102. Access should be in accordance with a tier 2 authorisation if the information relates to a foreign person or organisation, or a tier 1 authorisation if it relates to a New Zealand citizen, permanent resident or organisation.

Countering foreign terrorist fighters

Disruption of travel

103. The maximum three-year cancellation period for travel documents should continue to apply.

104. 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. A judicial commissioner should review the decision and have the ability to overturn it if one of the grounds for judicial review is made out.

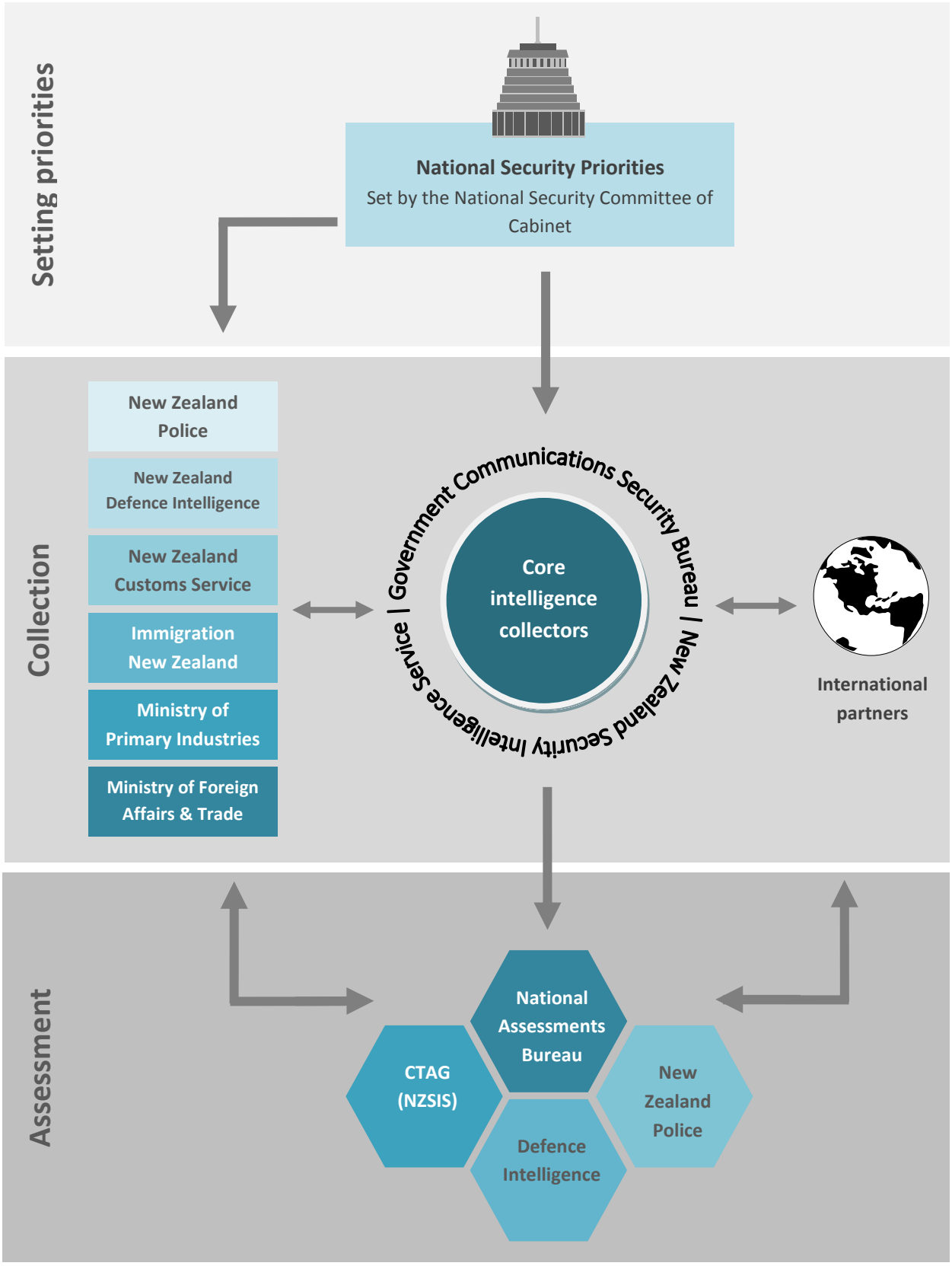
105. The ability to suspend a travel document for a maximum of 10 working days should be retained, to prevent a person from leaving the country while the process for cancelling their travel document is progressed.

Visual surveillance

106. The legislation should continue to enable visual surveillance by the Agencies in appropriate circumstances.

107. Visual surveillance powers should be subject to the new authorisation regime we have proposed and treated the same as other types of surveillance. They should not be restricted to counter-terrorism investigations.

Annex D: New Zealand's Intelligence System



Annex E: Outline of proposed single Act

Part 1 – Preliminary provisions

This Part should include:

- a purpose statement (to protect New Zealand as a free, open and democratic society)
- an interpretation section defining key terms such as national security, surveillance, interception, incidentally obtained information, foreign person and foreign organisation.

Part 2 – Intelligence and security agencies

This Part should include:

- the principles applying to the Agencies' performance of their functions
- the objectives of the Agencies
- the functions of the Agencies and the National Assessments Bureau
- provisions relating to the Agencies' status as public service departments.

Part 3 – Authorisations

This Part should include:

- a requirement that the Agencies only undertake activity authorised under the Act
- the three-tiered authorisation framework for the Agencies' activities
- the processes for obtaining authorisation, including the criteria that must be met
- the arrangements for authorisations in urgent situations
- provisions relating to the execution of authorisations (such as the ability to require assistance from third parties)
- provisions enabling the use of cover / assumed identities and requiring a policy statement to be issued to regulate their use
- immunities applying to employees of the Agencies and persons assisting them.

Part 4 – Access to, retention and use of information

This Part should include:

- provisions allowing the Agencies to access specified information held by government departments in accordance with joint ministerial protocols (for datasets) or authorisations (for information requests).
- a requirement that the Agencies destroy incidentally obtained intelligence unless a review warrant is obtained or it is relevant to the grounds set out in the current s 25 of the GCSB Act (such as detection of serious crime).

Part 5 – Administration

This part should include:

- any necessary provisions relating to the directors and employees of the Agencies
- annual reporting requirements
- an obligation on the directors to keep a register of authorisations.

Part 6 – Commissioners of Intelligence Warrants

This part should include:

- provisions relating to the appointment of a Chief Commissioner and at least two other Commissioners
- the functions of the Commissioners.

Part 7 – Inspector-General of Intelligence and Security

This part should include:

- provisions relating to the appointment and independence of the Inspector-General and Deputy Inspector-General
- the functions of the Inspector-General
- the powers and proceedings of the Inspector-General
- the reporting procedures of the Inspector-General
- the appointment and functions of the advisory panel.

Part 8 – Intelligence and Security Committee

This part should include:

- the appointment of the Committee
- the powers and functions of the Committee including the power to request reports from the Inspector-General
- the proceedings of the Committee
- the requirements and any limitations with respect to reporting by the Committee
- limitations on any person appointed by or appearing before the Committee.

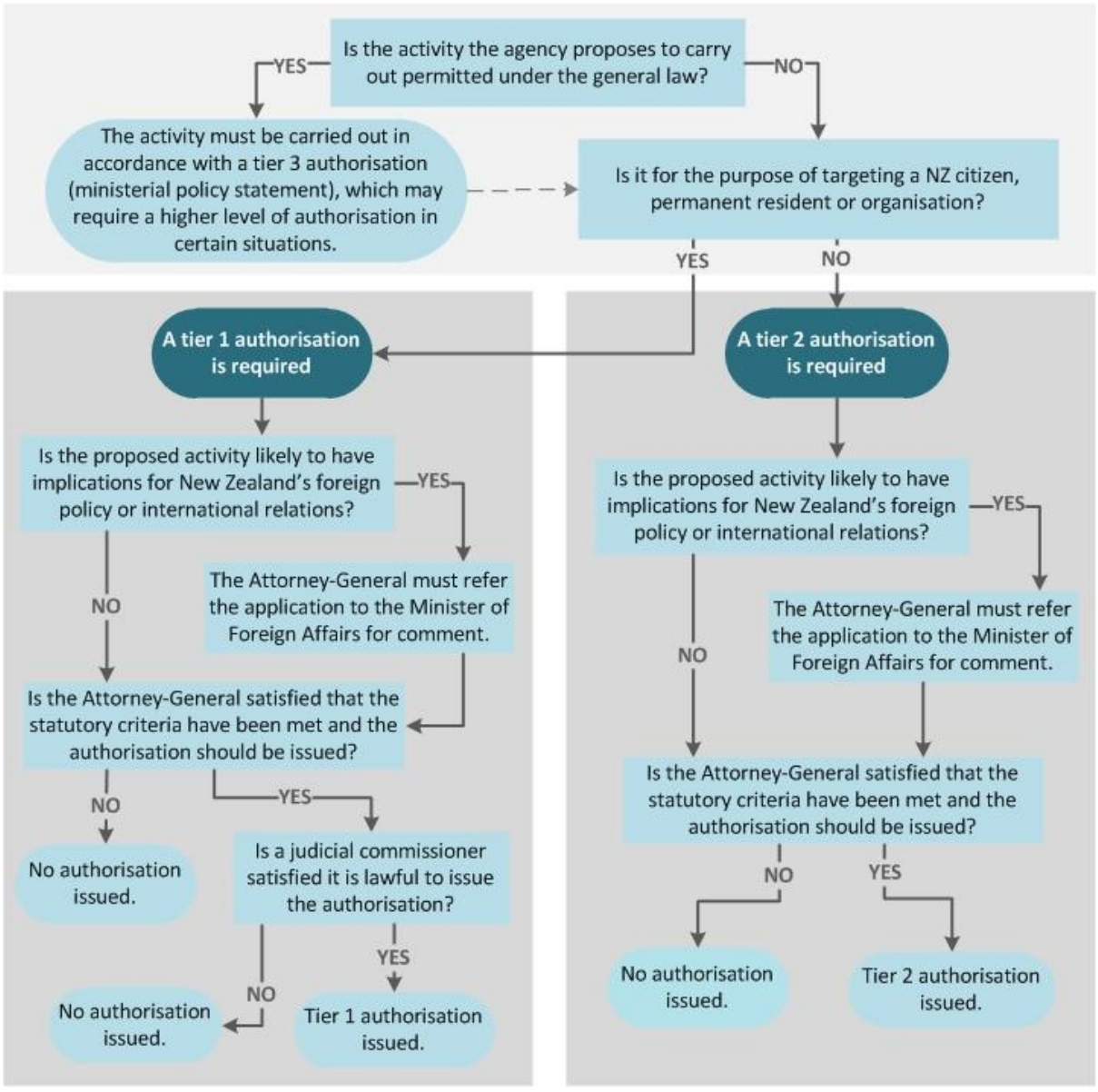
Part 9 – Periodic Reviews

This part should incorporate the current provisions of the Intelligence and Security Committee Act in relation to periodic reviews.

Part 10 – Offences

This part should carry over and amalgamate the offences in the existing legislation (for example, unauthorised disclosure of information).

Annex F: Proposed authorisation framework



Before issuing a tier 1 or 2 authorisation, the Attorney-General and / or a judicial commissioner must be satisfied that...

- The proposed activity is necessary for the proper performance of a function; to test, maintain or develop capabilities; or to train employees.
- 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 beyond what is reasonable and necessary for the proper performance of a function.
- There are satisfactory arrangements in place to ensure information is only obtained, retained, used and disclosed in accordance with the legislation.

Annex G: Glossary of terms

Combined Threat Assessment Group (CTAG)	An interdepartmental assessment unit located within the NZSIS. CTAG assesses terrorist threats to New Zealand and New Zealanders and provides advice on the domestic threat level. It includes representatives from the New Zealand Police, GCSB, New Zealand Defence Intelligence and Aviation Security Service.
Counter-intelligence	Intelligence activities concerned with identifying and mitigating threats to security from foreign governments or individuals engaged in espionage, sabotage, subversion or terrorism.
Department of Prime Minister and Cabinet (DPMC)	Provides advice to support the effective conduct of executive government by the Prime Minister, the Governor-General and members of the Cabinet. Includes the Security and Intelligence Group, which provides leadership and co-ordination of national security strategy and policy, intelligence requirements, priority setting and risk management.
Espionage	The practice of spying to obtain information about the plans and activities of a foreign government or private organisation. (Note: in New Zealand espionage is a criminal offence under s 78 of the Crimes Act 1961, which contains its own more specific definition).
Five Eyes	An intelligence-sharing arrangement between New Zealand, Australia, the UK, Canada, and the USA.
Foreign Terrorist Fighters (FTFs)	United Nations Security Council Resolution 2178 defines foreign terrorist fighters as "individuals who travel to a state other than their states of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict."

Government Communications Security Bureau (GCSB)	The GCSB is New Zealand's signals intelligence agency. Its functions are to: • provide information assurance and cyber security services to the New Zealand government and critical infrastructure organisations • collect foreign intelligence and provide it to government decision-makers • co-operate with and provide assistance to New Zealand Police, New Zealand Defence Force and the New Zealand Security Intelligence Service.
Human intelligence (HUMINT)	Information gathered from human (rather than electronic) sources, including through interpersonal contact.
Inspector-General of Intelligence and Security (Inspector-General)	Provides independent external oversight and review of the intelligence and security agencies. Responsible for reviewing issues of legality, efficacy and efficiency, and human rights and privacy compliance. In particular, the Inspector-General: • assists the Minister responsible for the intelligence and security agencies to ensure the activities of each agency comply with the law • ensures that complaints relating to intelligence and security agencies are independently investigated.
Intelligence and Security Committee (ISC)	A statutory committee established under the Intelligence and Security Committee Act 1996. Includes the Prime Minister, Leader of the Opposition, and other members nominated by them and confirmed by the House. The ISC examines the policy, administration and expenditure of the GCSB and NZSIS, considers both agencies' annual reports and conducts an annual financial review of the Agencies' performance. It also considers Bills or other matters relating to the Agencies referred to it by Parliament, and any matters referred by the Prime Minister due to their security or intelligence implications.
Islamic State in Iraq and the Levant (ISIL, ISIS or Islamic State)	ISIL is a predominantly Sunni jihadist group originating from al-Qaeda in Iraq. Its stated aim is to create a single, transnational Islamic state based on Shariah law. The United Nations has designated it to be a terrorist organisation. ISIL is based in Iraq and Syria but also operates in eastern Libya, the Sinai Peninsula of Egypt and other areas of the Middle East, North Africa, and South Asia.

Metadata	Metadata is data about data. It includes data created when forms of electronic communication are made – for example, the time and date of a phone call or email, the email addresses or phone numbers of the parties, and the cell towers or Internet Protocol addresses the communication was sent and received from. It does not include the content of communications, such as the body of an email.
National Assessments Bureau (NAB)	Part of the Security and Intelligence Group in DPMC. Produces intelligence assessments on events and developments bearing on New Zealand's interests to inform government decision making.
National Intelligence and Security Advisor (NISA)	A new position we suggest the government consider establishing to oversee and co-ordinate the New Zealand Intelligence Community (NZIC). The NISA would be the principal adviser to the government on matters of intelligence and security. He or she would also oversee and direct the implementation of a single NZIC appropriation and ensure the activities of the NZIC are aligned with the government's priorities.
National Security Committee of Cabinet (NSC)	NSC is the key decision-making body of executive government in respect of security, intelligence and crisis management. It oversees the New Zealand Intelligence Community. It is chaired by the Prime Minister and has standing authority to make decisions without reference to full Cabinet when urgent action is needed, or where operational or security considerations require it.
New Zealand Intelligence Community (NZIC)	Three agencies form the core of the NZIC: the Government Communications Security Bureau, New Zealand Security Intelligence Service and National Assessments Bureau. A range of other government agencies also have intelligence units but are seen as sitting outside the core NZIC – for example, the New Zealand Defence Force, New Zealand Police, New Zealand Customs Service and Immigration New Zealand.
New Zealand Security Intelligence Service (NZSIS)	NZSIS is New Zealand's human intelligence agency. Its functions include: • investigating threats to New Zealand's security • collecting foreign intelligence relevant to security, and • providing a range of protective security advice and services to the government.

Officials' Committee for Domestic and External Security Co-ordination (ODESC)	A forum of central government chief executives with security responsibilities, chaired by the chief executive of DPMC. Assists the government with setting national security direction.
Open source intelligence (OSINT)	Information from sources that are generally available, including information obtained from the media (for example, newspapers, radio, television), professional and academic records (for example, papers, conferences, professional associations) and public data (for example, government reports, demographics, hearings, speeches).
Sabotage	Damaging, destroying or interfering with the operation of equipment or property with the intention of prejudicing the security or defence of a country. (Note: in New Zealand sabotage is a criminal offence under s 79 of the Crimes Act 1961, which contains its own more specific definition).
Security and Intelligence Group (SIG) of the Department of Prime Minister and Cabinet	Provides leadership and co-ordination of national security strategy and policy, intelligence requirements, priority setting and risk management. Also leads development of cyber security policy and co-ordinates relationships with foreign partners. Includes the National Assessments Bureau (NAB), which provides all-source intelligence assessments to inform government decision-making.
Signals Intelligence (SIGINT)	Intelligence-gathering by interception of signals, whether communications between people or from electronic signals not directly used in communication.
Subversion	Attempts to overthrow a legally constituted Government by force or undermine the authority of the state by unlawful means.