Office of the Minister for National Security and Intelligence
Office of the Minister Responsible for the GCSB
Office of the Minister in Charge of the NZSIS

Chair, Cabinet National Security Committee

Intelligence and Security in a Free Society: Report of the first Independent Review of Intelligence and Security in New Zealand

Paper Two: Warranting and Authorisation Framework

Proposal

1. This paper seeks Cabinet policy decisions on the key elements of a unified warranting and authorisation framework and the warranted powers available to the Government Communications Security Bureau (GCSB) and New Zealand Security Intelligence Service (NZSIS).

Executive Summary

2. The Independent Review of Intelligence and Security made a number of recommendations to bring the agencies under a unified warranting and authorisation framework including the establishment of a comprehensive authorisation regime with three tiers and a list of intrusive activities the agencies could be permitted to undertake. They made a number of other recommendations including a more flexible targeting regime and a detailed framework to deal with situations of urgency. Finally, they proposed a comprehensive approval and authorisation framework which includes satisfying the Attorney-General and, in some cases also a judicial commissioner, that an intelligence warrant is necessary and proportionate.

3. The reviewers' recommendations provide a useful basis to develop a comprehensive and unified warranting regime, but do not include a sufficient level of detail for an effective warranting regime.

4. In order to take the reviewers' recommendations forward, the warranting regime would:

   4.1 Identify the objective advanced by the warrant;

   4.2 Describe in plain language a common set of primary powers the agencies require to conduct activities under the warrant; and

   4.3 Give the agencies necessary and reasonable powers to give effect to those primary warranted powers.

5. We propose the government should seek to modernise existing warranted powers that already exist in the agencies' separate legislation to provide a clear legal basis for the activities of the agencies. We also propose to use plain language to describe the primary powers of the agencies which would be shared by both agencies. While the reviewers recommended that both agencies have fully merged powers including

powers to give effect to a warrant, this would amount to a significant expansion of the powers of both agencies. Accordingly, we propose that both agencies shall retain separate powers to give effect to a warrant reflecting their distinct capabilities while enabling them to work together more effectively.

6. We propose Cabinet agree to the reviewers' recommendation to create a three tier authorisation framework with the legislation which includes tier one warrants which target New Zealanders and tier two warrants which target non-New Zealanders. We propose to make it clear that the reviewers' third tier "Ministerial Policy Statements" would only set the parameters for the conduct of lawful activities rather than act as a mechanism for legal authorisation of those activities, and would therefore sit outside the warranting regime.

7. The agencies could exercise the following powers when authorised in an intelligence warrant (only where that activity would be otherwise unlawful):

   7.1 Intercept communications;

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

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

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

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

   7.6 Request a foreign partner to undertake activities that would require a warrant for GCSB or NZSIS to do (noting that neither agency could request a foreign partner to undertake an activity in violation of New Zealand law);

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

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

8. A warrant would not be needed where the agencies are carrying out an otherwise lawful activity, such as receiving information from a third party (notwithstanding paragraph 7.6 above), or carrying out activities with consent.

9. To give effect to those primary powers, the agencies would have a set of powers to give effect that reflect their capabilities. NZSIS would have access to all of these powers, while GCSB would have access to a subset when acting independently. The GCSB operates primarily online and remotely, and would retain its current powers to access information infrastructures and to use its capabilities to intercept communications. The NZSIS operates primarily in the physical world and would retain its current powers to enter premises and other related powers. For the NZSIS, we propose to modernise their powers to align with those in the Search and Surveillance

Act 2012 where appropriate. However, the legislation would also recognise that to respond to modern threats it may be necessary for the powers of both agencies to be used. Accordingly, when operating under a joint warrant, employees of both agencies would have access to the full suite of powers available to both agencies.

10. One risk of a unified framework is that the agencies' powers may be interpreted more narrowly than currently. For the GCSB, which currently has broad and flexible powers such as the ability to access an information infrastructure, it will be important to craft the regime so it does not result in a reduction of powers. There may be some further matters of detail that emerge in the drafting process which might require some amendment to the proposed regime. We propose to give the Minister for National Security and Intelligence and the Minister responsible for the GCSB and in Charge of the NZSIS 'power to act' in respect of any policy decisions necessary through the drafting process.

11. The ability for greater flexibility in the targets of warrants is essential and we support the reviewers' recommendations to allow for warrants targeting a class of entities or an operational purpose where that is necessary and proportionate. This flexibility is vital to targeting threats to national security where the precise identity of a person is unknown (e.g. trying to identify New Zealanders who may be fighting with ISIL in Syria).

12. As discussed in Cabinet paper one, the GCSB has not been able to provide assistance to New Zealand Police in a timely or effective manner under the current assistance function in s 8C of the GCSB Act. There is a difference of view about the legal effect of section 8C which officials are continuing to work through. The GCSB contend the removal of section 14 would remove some of the current obstacles to working with more effectively with New Zealand Police. However, significant operational and potential legal differences would still remain and will need to be resolved to ensure effective assistance. Further work is needed to ensure GCSB assistance to Police is being provided in accordance with Ministers' expectations.

13. The proposed framework strengthens oversight. It would see the Commissioner of Security Warrants replaced with a panel of three judicial commissioners headed by a Chief Commissioner of Intelligence Warrants. Intelligence warrants that target New Zealanders (ie, tier one warrants) would be subject to three important safeguards – a "triple lock". Tier one warrants would be jointly authorised by the Attorney-General and a judicial commissioner, and subject to the review and audit of the Inspector-General.

Background

Summary of the reviewers' recommendations

14. The reviewers have recommended a comprehensive authorisation regime – the starting point is that there must be "some form of authorisation for all of the agencies' activities that involve gathering information about individuals and organisations to ensure that appropriate safeguards apply to everything they do". From this starting point, the reviewers recommend a three-tier system:

    14.1 Warrants (Tier one): required for intelligence collection activities that would otherwise be unlawful for the purpose of targeting a New Zealand citizen or permanent resident. Warrants would be issued by the Attorney-General and a

judicial commissioner. The judicial commissioner would consider the legality of the application;

14.2 Authorisations (Tier two): required for the same types of activities as tier one warrants but where they are not being carried out for the purpose of targeting a New Zealander. Tier two warrants would be issued by the Attorney-General and would not require the involvement of a judicial commissioner;

14.3 Ministerial Policy Statements (Tier three): a policy statement approved by the Minister to provide authorisation for the conduct of lawful activities that involve gathering information about individuals and organisations (e.g. open source collection or physical surveillance in public places).

15. The reviewers propose that warrants (both tiers) would permit the following types of activity where that activity would otherwise be unlawful:

15.1 Interception of communications;

15.2 Acquisition of information held by third parties;

15.3 Accessing information infrastructures;

15.4 Surveillance (including using video, listening and electronic tracking devices); and

15.5 Use of human sources.

16. The reviewers recommend that the basis for issuing a warrant would be outlined in a statutory test; the Attorney-General, and the judicial commissioner in the case of tier one warrants, 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 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 legislation.

17. The reviewers recommend that the Attorney-General should be required to refer warrants 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.

18. The reviewers propose the agencies should be able to obtain warrants or authorisations (i.e. both tiers) aimed at a particular purpose, which would specify the type of information sought and the operational purposes for which it is required. However, they recommend a legislative presumption in favour of targeted warrants, and that purpose-based warrants should only be available if the Attorney-General, and a judicial commissioner in the case of a tier one warrant, are satisfied that a purpose-based approach is necessary and proportionate and could not be reasonably achieved through a targeted warrant.

19. To deal with situations of urgency, the reviewers make a number of useful recommendations, including the ability for applications to be made over the phone, and for the Attorney-General (or another Minister designated by the Prime Minister to act on the Attorney-General's behalf) to issue a warrant alone where there is an imminent threat to the life or safety of any person, or where a delay in seeking a warrant through the ordinary process would be likely to seriously prejudice national security. In only the most urgent cases, a Director of an agency could authorise warranted activity for 24 hours.

20. The reviewers recommend that a panel of three judicial commissioners headed by a Chief Commissioner of Intelligence Warrants replace the current single Commissioner of Security Warrants. They recommend the judicial commissioners could be either retired or sitting judges as the roles would not be full time. The reviewers make no recommendation as to how the judicial commissioners would be appointed, how they would relate to the judiciary, or whether the Chief Commissioner could overrule the decision of a fellow commissioner.

21. When considering a tier one warrant application, the judicial commissioner would need to be satisfied that all the criteria at paragraph 16 above are met. However, the reviewers go on to recommend that legislation clarify that "judicial approval is appropriately focused on legal factors".

Comment

22. Overall, the reviewers' recommendations provide a useful basis to develop a comprehensive and unified warranting regime. There are, however, significant gaps including a lack of detail on the nature of the powers to give effect to a warrant, and how those powers should be divided between the NZSIS and GCSB. The Court of Appeal in *Choudry v Attorney-General* held that intrusive powers need to be spelled out clearly in legislation. In that case, the Court did not accept the NZSIS had any power of entry to private premises in order to effect interception or seizure. As a result, the New Zealand Security Intelligence Service Amendment Act (No 2) was passed in 1999, which included much greater specificity about the powers available to the NZSIS. The warranting framework proposed in this paper provides significantly more detail to the reviewers' proposal about the powers available to the agencies under a warrant.

High-level policy decisions

23. We recommend the Government accept the broad parameters outlined in the reviewers' recommendations. The underlying policy principles underpinning the Government's approach to a new warranting regime should be to:

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

23.2 modernise the powers available to the agencies and to provide a clear legal basis for the activities of the agencies, and the protections and safeguards that apply;

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

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

23.5 make clear that only unlawful activity requires a warrant; and

23.6 remove unnecessary barriers to effective cooperation between agencies.

24. We recommend that Cabinet agree to the reviewers' recommendation to create a three tier authorisation framework, with one change in relation to Ministerial Policy Statements. Ministerial Policy Statements would be an integral part of that framework; it is, however, important to be clear as to their intended legal effect. Lawful activity is by definition lawful and a Ministerial Policy Statement cannot make lawful activity unlawful or unlawful activity lawful. We propose the legislation should make clear that the agencies would retain all powers of a natural person, and that Ministerial Policy Statements should set out the general parameters for the conduct of those lawful activities. One purpose of a Ministerial Policy Statement would be to provide an objective standard against which the Minister and the Inspector-General can assess the propriety of the lawful activities of the agencies.

25. This regime (particularly Ministerial Policy Statements) would only apply to the activities of intelligence agencies, which are subject to Ministerial control and are of keen public interest, and not to law enforcement and regulatory agencies which have their own authorising and oversight mechanisms. This is important given the upcoming review of the Search and Surveillance Act.

Enhancing coordination and collaboration through a unified authorisation regime

26. A unified warranting framework would support work underway to enhance collaboration and coordination in the New Zealand Intelligence Community.

27. Currently, the NZSIS and GCSB operate under separate warranting frameworks. While there are some broad similarities, there are also significant differences. The lack of alignment in the existing frameworks is a significant barrier to effective cooperation, and often leads to multiple applications in respect of the same target(s).

28. The way that the current legislation requires the agencies to operate together is largely based on a 20th century understanding of how intelligence agencies operate, which bears very little resemblance to how modern intelligence agencies must

collaborate to achieve best possible outcomes for New Zealand. In the modern scenario, no single operation should rely on one capability or another, but will instead rely on the composite of skills and capabilities afforded by the two agencies. Legislation must enable the two agencies to maintain their distinct areas of expertise together in a transparent, cleanly authorised, and operationally sensible fashion.

29. To illustrate this point, a terrorist organisation is likely to employ a far higher degree of sophistication in its operational security to obscure its activities. The methods to do this are freely available on the internet. In order to defeat these obfuscation methods, the agencies must deploy a number of different areas of technical and human expertise. Timeliness is often critical, and clarity around what is authorised is essential. This timeliness and clarity is not possible when the operation relies on a patchwork of authorisations under different legal authorities.

30. A unified regime would enable the Attorney-General to consider all the potential tools available to collect intelligence, rather than on an agency-by-agency basis. The proposed regime would allow the two agencies to work more effectively together on joint operations. Joint warrant applications should be a feature of the new framework.

31. Successive reviews of the New Zealand Intelligence Community have emphasised the need to rationalise the development of capabilities in such a way that minimises unnecessary duplication, but reinforces collaboration. The need to minimise duplication has also affected resourcing decisions of other agencies including New Zealand Police and NZDF. The unified warranting regime would be consistent with the intent of these reviews in seeking to remove the unnecessary barriers to cooperation, while retaining appropriate distinctions in the powers to recognise each agency's particular expertise and capabilities.

The three tiers of authorisation

32. As recommended by the reviewers, all intelligence collection activities of the agencies that would otherwise be illegal would require a warrant. As noted, the third tier "Ministerial Policy Statements" would only set parameters for the conduct of lawful activities rather an act as a mechanism for legal authorisation of those activities (and this is a slight departure from what the reviewers proposed).

33. We propose that the warranting regime would include two types of warrant:

    33.1 Warrants (Tier one): required for intelligence collection activities that would otherwise be unlawful and are proposed for the purpose of targeting a New Zealand citizen or permanent resident. Warrants would be issued by the Attorney-General and a judicial commissioner.

    33.2 Warrants (Tier two): required for the same activities as tier one warrants but where those activities are not proposed for the purpose of targeting a New Zealander. These warrants would be issued by the Attorney-General and would not require the involvement of a judicial commissioner. The only significant difference between a tier one warrant and a tier two warrant would be the involvement of a judicial commissioner where New Zealanders are targeted – otherwise the two tiers cover the same types of activities.

33.3 Lawful intelligence activities of the intelligence agencies would be regulated by Ministerial Policy Statements, but would not require legal authorisation under the warranting regime (see Table 1).

Table 1: Modes of authorisation

Otherwise Unlawful Activity – "the warranting regime"	**Lawful Activity**
Tier 1 Warrants: intrusive intelligence collection targeting New Zealanders	Ministerial Policy Statements
Tier 2 Warrants: intrusive intelligence collection not targeting New Zealanders	

34. We propose that the Minister responsible for issuing warrants would be the Attorney-General. The reviewers were of the view that the Attorney-General was best placed to take into account a wide range of factors, including national security considerations as well as legal and human rights considerations. The Minister responsible for the GCSB and in Charge of the NZSIS would issue Ministerial Policy Statements. The reviewers did not see any issue with the Attorney-General also being concurrently Minister responsible for the agencies. This approach is consistent with that adopted in Australia.

The Warranting Regime

35. As noted earlier, the approach recommended by the reviewers has two significant weaknesses: (1) it effectively merges the powers of the NZSIS and GCSB without maintaining any distinction that reflects their different capabilities; and (2) its list of proposed powers excludes core activities of the NZSIS in particular. We propose the following key policy principles for the design of a joint warranting framework:

35.1 The regime must maintain the current powers of both agencies at a minimum – there would not be any reduction in what the agencies are already able to do. In this respect, we are conscious of the risk that the combining the powers of both agencies into a single act may lead to those powers being interpreted more narrowly than is the case now. The legislation would need to be clear that this is not the intention.

35.2 That plain language is used to describe the primary powers of both agencies in legislation. This makes the effects of their powers clearer, while also providing a common framework to enhance cooperation.

35.3 The regime should preserve an appropriate distinction in agencies' powers to give effect to a warrant consistent with the differences in the nature of their work and capabilities. This would ensure the powers of the agencies are not merged, as this would amount to a significant expansion in powers, particularly for the GCSB.

36. An outline of the proposed warranting regime is attached as an Annex to this paper (page 34).

Identifying the objective of the warrant

37. Cabinet paper one outlines the shared objectives and functions of the agencies. Every warrant would be required to fall within at least one of three identified objectives – to contribute to:

    37.1 the protection of New Zealand's national security (including protecting New Zealand's economic security and assisting to maintain international security, which can affect domestic security);

    37.2 New Zealand's international relations and wellbeing;

    37.3 New Zealand's economic wellbeing.

38. As recommended by the reviewers, every warrant application would also be required to be for the purpose of:

    38.1 the proper performance of one of the agencies' functions (collecting intelligence; protective security; assisting other government agencies);

    38.2 to test, maintain or develop capabilities; and/or

    38.3 to train employees for the purpose of performing the agencies' functions.

Description of the primary powers the agencies can exercise under a warrant

39. Having identified an appropriate objective and function, the agencies would be able to apply for a warrant to exercise one or more of the following powers (only where that activity requiring that power is otherwise unlawful):

    39.1 Intercept communications;

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

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

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

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

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

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

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

40. These are intended to be plain language descriptions of the powers of both agencies and provide transparency as to what the agencies intend to do under a warrant. Both NZSIS and GCSB currently have most of these powers (excluding the new power of intelligence collection through human sources involving unlawful activity). In GCSB's case, these largely fall under its current power to access information infrastructures. The approach recommended in this paper would provide greater clarity and transparency about the powers of the agencies, particularly the GCSB. While these would be shared by both agencies, the differences between the agencies would maintained in how they give effect to these powers – the NZSIS and GCSB will often effect these powers in quite different ways (for example, the NZSIS may conduct surveillance by installing a surveillance device; the GCSB may do so by remotely accessing an information infrastructure).

41. The list above does not precisely correspond to that recommended by the reviewers, which did not include search, seizure, obfuscating and maintaining capabilities, or necessary or desirable acts to protect security and integrity of certain communications and information infrastructures. These activities could have been captured by "accessing an information infrastructure," but that would not have enabled the NZSIS to seize physical items which is an important current power.

42. The list does not include accessing an information infrastructure. This is a significant and important power in the current GCSB Act and enables the GCSB to collect intelligence, provide cybersecurity and information assurance services, and take other measures to protect its capabilities from discovery. Including access to an information infrastructure in the list of powers as proposed by the reviewers would risk this term being interpreted more narrowly. It is a broad term that encompasses many of the powers proposed in this paper(such as seizure, interception, and surveillance). We propose that it be retained as the means by which the GCSB might give effect to a warrant rather than a primary power.

43. The list also amends "acquisition of information held by third parties" to provide greater transparency when the agencies make requests of foreign partners undertake activities where the NZSIS or GCSB would require a warranted power to do so. This approach would ensure transparency in requests of partners, but would not cover general sharing of intelligence with foreign partners. Cabinet paper five deals with information sharing arrangements with other government departments, foreign governments and private sector entities, and these activities would be regulated by a specific provision in the Bill and/or a Ministerial Policy Statement if that activity is otherwise lawful.

44. The reviewers recommended that the agencies should be able to obtain a warrant to "test, develop or maintain capabilities … for the purpose of performing the agencies functions." Para 35.7 is included to give effect to this recommendation and allow the agencies to develop reasonable capabilities to keep their activities covert, or to develop or maintain the ability to collect intelligence in the future. This power is essential to enable the agencies to confront the challenges of modern technology. As with other warrants, any application to undertake this activity would need to satisfy the Attorney-General (and a judicial commissioner in the case of a tier 1 warrant) that it is necessary and proportionate to do so.

45. Acts necessary or desirable to protect security and integrity of certain communications and information infrastructures including identifying and responding to threats and potential threats to those communications and information

infrastructures is defined using GCSB's existing cybersecurity and information assurance function in s 8A of the GCSB Act. This power would be limited to GCSB. The agencies could still exercise the other warranted powers for the purpose of performing the broader protective security function. While the legislation would separately enable the GCSB to provide cyber defence and information assurance purposes without a warrant when it has the consent of an affected entity (see below), the warranting regime preserves the flexibility for the agencies to obtain a warrant where it is not operationally desirable or possible to obtain consent.

46. As noted above, a result of combining GCSB and NZSIS primary powers is that there will be changes in the labels for some of the agencies' current powers. This is because the introduction into statute of a more specific list of powers will change the way the existing, broader, powers that are replicated in the new list are likely to be interpreted. For example, GCSB's ability to take hardware or other physical infrastructure or items that currently falls under "access to information infrastructure" would instead fall under "physical seizure". In the same vein, there are aspects of surveillance that both agencies do, and must be able to continue to do under any new authorisation regime. For example, visual surveillance may be used for operational security purposes at an un-attributable facility.

47. An important change would be the ability to obtain a warrant for certain human intelligence operations. Currently, there is no ability for an NZSIS officer or human source to engage in unlawful activity, even though there are situations where that might be necessary in order to collect intelligence. GCSB officers assisting the NZSIS or conducting similar activities online might require the same power. The reviewers use the example of a human source joining a terrorist group or organisation in order to collect intelligence, such as the intentions or capabilities of that terrorist group. This could happen in the real world or online.

48. In those situations, the operation would need a warrant (and corresponding immunity for the activity would attach) in order for it to be lawful. For operational security reasons, it is not possible to describe in detail the types of activity that might be covered by a human source warrant, but any use of this power would need explicit authorisation in a warrant. Human source collection relying on impersonation (including online impersonation) and not involving other unlawful activity would not require a warrant as that collection would be supported by clearer provisions on the use of cover and associated immunities (addressed in Cabinet paper five).

49. We propose to consolidate the existing definitions of the above powers while drawing on definitions from other places in the statute book.

Agencies would have separate powers to give effect to a warrant

50. We propose to grant to agencies reasonable and necessary powers to give effect to a warrant. It is settled law in New Zealand that the agencies need clear and explicit powers to give effect to a general warranted power (e.g. in 1999, s4E of NZSIS was added to make it clear the NZSIS had a power of entry to private premises to give effect to a warrant). The reviewers do not address this point in any detail other than to note that the agencies should be permitted to undertake "other reasonable activities necessary to give effect to them, such as entry onto private premises in order to install a surveillance device." If this were to apply to both agencies, it would amount to a significant expansion of powers.

51. The previous section identified the primary powers that would be authorised by a warrant. In order to maintain appropriate distinctions between the powers of the agencies, we recommend the agencies have separate powers to give effect to a warrant. The legislation would recognise that the agencies have particular powers reflecting their specialised skills and capabilities. The NZSIS operates primarily in the physical world and usually conducts its activities through direct means (e.g. entering premises; physically accessing a particular phone or device). The GCSB uses its signals intelligence and information assurance capabilities to produce intelligence and protect important information infrastructure and communications primarily by remote means.

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

53. Both agencies would be able to:

    53.1 access (instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of, including any audio or visual capability) an information infrastructure;

    53.2 install, use, maintain or remove an interception device;

    53.3 extract and use any electricity; and

    53.4 install, maintain, use or remove an audio or visual surveillance device to maintain the operational security of a warranted activity;

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

    54.1 install, use, maintain or remove a visual surveillance device;

    54.2 install, use, maintain or remove a tracking device;

    54.3 break open or interfere with any vehicle or other thing;

    54.4 enter any place, vehicle or other thing authorised by the warrant;

    54.5 take photographs, sound and video recordings, and drawings of a place vehicle or other thing searched, and of any thing found in or on that place vehicle or other thing;

    54.6 Use any force in respect of any place vehicle or thing that is reasonable for the purposes of carrying out a search or seizure;

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

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

55. The specific powers would be supported by the following general ancillary powers:

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

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

56. The first general ancillary power is currently in section 4E of the NZSIS Act. The second general ancillary power is not currently included in either the GCSB Act or the NZSIS Act. However, it is an ancillary power widely used in other jurisdictions (see for example section 25(4)(e) of the Australian Security Intelligence Organisation Act). The agencies should be able to take reasonable steps in order that intelligence operations remain covert (e.g. reasonable steps to prevent foreign agents from detecting that New Zealand intelligence agencies are monitoring their activities).

57. The restrictions on the GCSB are consistent with their current powers. While the NZSIS list has expanded significantly, this reflects to a substantial degree the age of its primary legislation. The passage of the Search and Surveillance Act 2012 set a new standard for those types of powers, and it is appropriate to align those powers accordingly. The inclusion of accessing an information infrastructure at this level recognises that this is the primary tool of the GCSB to give effect to the primary powers. It would also capture NZSIS current ability to maintain and monitor electronic devices. Given the importance of accessing an information infrastructure to the GCSB, it may be necessary to include a provision for the avoidance of doubt to ensure that this term is interpreted in such a way that preserves the current scope of that power.

58. While the GCSB would not have the largely physical powers available to the NZSIS (such as entry to premises), if the Attorney-General (and judicial commissioner in the case of a tier one warrant) were to approve a joint intelligence warrant (see below), employees of both agencies would be able to access the full suite of powers available to both agencies. For example, the GCSB is not able to enter private premises without consent to install an interception device. However, under a joint warrant with the NZSIS, we propose that the legislation would allow GCSB staff to do so jointly with the NZSIS (see below on cooperation).

59. We propose to retain current arrangements allowing persons and organisations to assist in the execution of a warrant. Both agencies would be able to continue to rely on section 24 of the Telecommunications (Interception Capability and Security) Act which imposes an obligation a network operator or service provider to assist to give effect to a warrant.

60. There may be matters of detail that emerge in the drafting process which may require some amendment to the proposed regime. We propose to give the Minister for National Security and Intelligence and the Minister responsible for the GCSB and in Charge of the NZSIS 'power to act' in respect of any policy decisions necessary through the drafting process.

Subjects of Warrants

61. To respond to a more complex range of threats, the warranting regime requires a degree of flexibility in terms of its targeting. The reviewers propose the agencies will be able to get targeted warrants (including classes of targets) and purpose-based warrants.

62. Targeted warrants would be required to specify the subject of the warrant – for example, the person whose communications may be intercepted, the information infrastructure to be accessed, or the thing to be seized. This would include particular classes of these things, as currently set out in the GCSB Act but not the NZSIS Act. We also recommend that, as proposed by the reviewers, the agencies should be able to obtain warrants aimed at a particular purpose. The application would specify the type of information sought and the operational reasons requiring its collection. This approach would be particularly useful for the purpose of accessing information infrastructure to identify threats to New Zealand posed by a terrorist group.

63. Purpose-based warrants would need to be sufficiently limited to be Bill of Rights Act consistent. In part, this would be achieved through the application of the warrant criteria by the Attorney-General and/or judicial commissioner which require them to be satisfied that a warrant is both necessary and proportionate.

<table>
<tr><td colspan="3">Warrants may be directed in the following ways:</td></tr>
<tr><td colspan="2">Targeted warrants</td><td>Purpose-based warrants*</td></tr>
<tr><td colspan="2">Targeted warrants would be required to specify the subject of the warrant (e.g. the person whose communications may be intercepted, the information infrastructure to be accessed, or the thing to be seized).

Target warrants could also be directed at a class of persons or things.</td><td>The application would specify the type of information sought and the operational reasons requiring its collection. This approach would be particularly useful for the purpose of conducting activities to identify threats to New Zealand.</td></tr>
<tr><td>Example (Targeted): a known ISIL recruiter based in Syria.</td><td>Example (Class): persons and information infrastructures (computers and phones) engaged in an illegal, unreported and unregulated (IUU) fishing operation.</td><td>Example (Purpose): a warrant for the purpose of identifying New Zealanders fighting with ISIL in Syria.</td></tr>
<tr><td colspan="3">* When applying for a purpose-based warrant, the application will need to demonstrate why the result could not be reasonably achieved through a targeted warrant.</td></tr>
</table>

64. In line with the recommendations of the reviewers, we propose that the legislation should require a purpose-based warrant to demonstrate why the objective of the warrant could not be reasonably achieved through a targeted warrant. Given the differences in the warranting regime outlined by the reviewers and the detailed framework proposed in this paper, we propose tier one warrants would be limited in the following ways:

64.1 Installation of surveillance devices could only be authorised where the application identified a specific target;

64.2 Access to an information infrastructure would require the warrant application to identify the specific information infrastructure (or class of information infrastructures) to be accessed;

Review warrants and incidentally obtained intelligence

65. The reviewers address the issue of incidentally obtained intelligence about a New Zealander by introducing a new type of warrant called a "review warrant", which we recommend Cabinet agree to. Where the agencies wish to use incidentally obtained intelligence about a New Zealander collected under a tier two warrant, they would need to apply for a tier one warrant authorising the use of intrusive powers against New Zealanders.

66. Unless a review warrant is obtained or one of the grounds for disclosing incidentally obtained intelligence to a public authority is met, the intelligence could not be retained.

Removal warrants

67. Where a device is installed, it may be necessary in some circumstances to seek a warrant to remove that device (for example, if the NZSIS installed a device in a premise and the target of warrants no longer resided at that address). I propose to retain (with appropriate modifications for the new regime) section 4I of the NZSIS Act in relation to removal warrants and apply it both agencies so that the agencies can remove devices where it would no longer be appropriate for a device to be installed.

Criteria for issuing a warrant

68. Before issuing a warrant, the Attorney-General (and the judicial commissioner in the case of tier one warrants) would need to be satisfied that:

68.1 The proposed activity is necessary either:

68.1.1 For the proper performance of one of the agency's functions;

68.1.2 To test, maintain or develop capabilities; or

68.1.3 To train employees for the purpose of performing the agency's functions.

68.2 The proposed activity is proportionate to the purpose for which the authorisation is sought;

68.3 The outcome sought cannot reasonably be achieved by less intrusive means;

68.4 There are satisfactory arrangements in place to ensure nothing will be done in reliance on the warrant beyond what is reasonable and necessary for the proper performance of a function of the agencies; and

68.5 There are satisfactory arrangements in place to ensure that information is only obtained, retained, used and disclosed in accordance with legislation.

69. The purpose of this test is to ensure that an intelligence warrant is only issued when it is necessary and proportionate to do so, and that any consequences of an intelligence warrant would be managed appropriately. The final two criteria should be able to be standardised in many cases as they relate to the internal policies and information management of the agencies. However, they are retained as part of the regime to ensure the Attorney-General and judicial commissioner can impose or require additional arrangements or conditions in particular cases.

Role of the Minister of Foreign Affairs in relation to an intelligence warrant

70. Intelligence activities can have implications for New Zealand's international relations or foreign policy. It is therefore appropriate for the Minister of Foreign Affairs to be consulted on intelligence warrant applications where those implications are likely to occur. This requires careful consideration of the appropriateness of the proposed intelligence activities, while maintaining an appropriate distance from operational decisions so as to not undermine his or her ability to conduct New Zealand's international relations.

71. The reviewers recommend that the Attorney-General should be required to refer warrants to the Minister of Foreign Affairs for comment where the proposed activity is likely to have implications for New Zealand's foreign policy or international relations. We recommend that Cabinet agree, but we propose the standard should be "consultation" rather than comment.

72. The reviewers note they would expect the Attorney-General and Minister of Foreign Affairs to agree on a process for determining when a requirement to consult the Minister would be triggered. We propose a joint protocol be developed prior to commencement of the legislation between the Attorney-General and Minister of Foreign Affairs to ensure this process works in an effective and timely manner.

Urgency: interim authorisations and urgent director authorisations

73. As the reviewers note, both agencies encounter situations where it is necessary to progress a warrant application urgently. While this occurs most frequently in counter-terrorism and counter-espionage operations, urgency may be required in other contexts. Temporary provisions in the NZSIS Act passed in 2014 as part of the foreign terrorist fighters legislation enabled the Director of Security to authorise warranted activities for up to 24 hours. In practice, the NZSIS has rarely used these provisions.

74. The reviewers have, however, made a number of useful and practical suggestions to enhance the responsiveness of the intelligence warranting process. These include:

    74.1 Requiring the Prime Minister to designate a Minister to have a standing power to act on behalf of the Attorney-General in the event the Attorney-General cannot be contacted;

    74.2 Requiring the Prime Minister to designate a Minister to act on behalf of the Minister of Foreign Affairs when he or she is unavailable;

    74.3 Making provision for warrants to be issued orally in exceptional circumstances (e.g. over the phone); and

74.4 Having multiple judicial commissioners, with one always available.

75. We support these recommendations as they help to reduce the risk that an inability to contact the appropriate Minister or judicial commissioner becomes a single point of failure in the warranting process. These steps would help to improve the overall responsiveness of the regime and ensure proper oversight, even in situations requiring an urgent response.

76. However, the Bill should provide for special warranting procedures in situations of urgency, as defined by the reviewers:

76.1 Where there is an imminent threat to the life or safety of any person; or

76.2 Where the delay associated with obtaining a warrant through the ordinary process is likely to materially prejudice national security.

77. In urgent situations, we propose that the Attorney-General could alone authorise tier one warranted activity to occur (an "interim authorisation"). In such cases, the Attorney-General would have to notify the Chief Commissioner of Intelligence Warrants immediately. The Chief Commissioner could direct that the warranted activity cease at any time.

78. In these cases, the agencies would have to submit a full tier one warrant application within 48 hours. If the Attorney-General or judicial commissioner then declined to confirm the warrant, any intelligence would need to be destroyed (unless one of the grounds for retaining and disclosing incidentally obtained intelligence is satisfied). The reviewers note that 48 hours is consistent with the Search and Surveillance Act 2012, which allows police to conduct warrantless surveillance for 48 hours in urgent situations.

79. We expect the above procedure to be sufficient for almost all situations. However, there may be some particularly serious situations where immediate action is required, and a Director should be able to make an urgent authorisation (an "urgent Director authorisation"). An urgent Director authorisation would only be available where even an interim authorisation is likely to cause delay to such an extent that the purpose of obtaining a warrant would be defeated. Where an urgent Director authorisation is granted, the Director should notify the Attorney-General (and the Chief Commissioner of Intelligence Warrants in respect of activity requiring a tier one warrant) without delay and provide a full application within 24 hours.

80. The Minister of Foreign Affairs would be required to be consulted when the urgent authorisation is confirmed. However, the protocol between the Attorney-General and the Minister of Foreign Affairs should address the nature and extent of any process to seek earlier input from the Minister of Foreign Affairs in situations of urgency.

81. All urgent authorisations would need to be referred to the Inspector-General for review as soon as practicable, and the agencies would be required to report in their Annual Report the number of times interim authorisations or urgent Director authorisations were used during the reporting year.

Assistance and Cooperation

NZSIS and GCSB cooperation

82. I recommend the regime allow for the submission of joint warrant applications. The approach in the preceding section of this paper was to maintain appropriate distinctions in the agencies' powers to give effect to warrants. Accordingly, joint warrant applications are necessary to ensure the agencies can operate effectively together.

83. Joint GCSB and NZSIS applications would ensure that the Attorney-General (and judicial commissioner in respect of tier one warrants) has full visibility of the intelligence activity against a particular target or targets. It would also encourage the agencies to consider each other's capabilities to ensure that an intelligence operation is conducted in a coordinated manner, and would make best use of each agency's specialist disciplines.

84. Operating under a joint warrant with the same powers provides the clearest legal footing for this kind of joint activity as it does not require a patchwork application of discrete powers and assistance mechanisms as between GCSB and NZSIS. The patchwork approach is particularly problematic where one agency is relying only on the other's statutory power because the agency with the statutory power requires the assistance of the other agency to carry it out. The ability to operate under a joint warrant recognises that when the agencies work together they are drawing on their combined capabilities to achieve the same objective.

85. When operating under a joint warrant, we recommend the agencies would be able make use of the full suite of intelligence collection powers (including through the use of powers available to only one agency). For example, the GCSB would be able to enter a premises without consent to install a device under a joint warrant with the NZSIS.

86. The removal of section 14 of the GCSB Act as proposed by Cabinet paper one would significantly improve the ability of the agencies to work together to protect New Zealand's national security.

Agency cooperation with Police and NZDF

87. The effect of the reviewers' recommendation is to retain the status quo for cooperation with New Zealand Police and NZDF. The agencies would be able to assist the New Zealand Police and NZDF in the performance of their functions. The reviewers made it clear that they did not wish to expand the powers of those other agencies through cooperation with the intelligence agencies.

88. We understand that current arrangements are working well for NZDF, but there are several issues that need to be addressed to ensure that New Zealand Police have appropriate access to the agencies' skills and technical capabilities.

Issues with GCSB Cooperation with Police

89. As discussed in Cabinet paper one, the GCSB has not always been able to provide assistance to New Zealand Police in a timely or effective manner under the current assistance function in s 8C of the GCSB Act. There is a difference of view about the

legal effect of section 8C which officials are continuing to work through. The GCSB contend the removal of section 14 would remove some of the current obstacles to working with more effectively with New Zealand Police. However, significant operational and potential legal differences would still remain and will need to be resolved to ensure effective assistance. Further work is needed to ensure GCSB assistance to Police is being provided in accordance with Ministers' expectations.

90. We note that Cabinet paper one has recommended the agencies should develop joint operating protocols with other agencies such as New Zealand Police. Officials from GCSB and New Zealand Police are currently working to resolve current operational and potential legal obstacles. It is essential that any obstacles are resolved. We propose Cabinet direct officials from DPMC, New Zealand Police and the GCSB to report to the Minister for National Security and Intelligence, the Minister of Police and the Minister responsible for the GCSB by 31 May 2016 on how to ensure effective cooperation under the new framework, including under a GCSB / New Zealand Police protocol. If further policy decisions are required to ensure the new regime works smoothly, we propose that those Ministers are given power to act to take those policy decisions.

Role of judicial commissioners

91. We propose to establish a panel of judicial commissioners. The particular institutional arrangements relating to the appointment, qualifications and administrative arrangements for judicial commissioners will be addressed in Cabinet paper 4. We do not propose to have sitting judges appointed as judicial commissioners (this will be discussed in detail in paper 4).

92. The reviewers recommend clarifying the legislation in such a way that the judicial commissioner "would consider the legality of the application." They also note that they see their recommendation as continuing the current practice, and refer to the evidence of the Commissioner of Security Warrants before United Kingdom Joint Committee considering the Draft Investigatory Powers Bill. It is therefore not clear whether the reviewers are proposing that judicial commissioners be restricted only to matters of law.

93. We do not consider it appropriate to reduce the level of judicial involvement in warrants, and therefore propose that Attorney-General and judicial commissioner jointly issue tier one warrants.

Safeguards: The "Triple-lock" for tier one warrants

94. Intelligence warrants that target New Zealanders would be subject to three important safeguards – a "triple lock". Tier one warrants would be authorised by the Attorney-General, approved by a judicial commissioner, and subject to the review and audit of the Inspector-General (a "triple-lock").

95. Table 3: The 'triple lock'

The "Triple-lock" to protect New Zealanders The Attorney-General, Judicial Commissioner and Inspector-General		
Executive Oversight	**Judicial Commissioners**	**Inspector-General**

Attorney-General: needs to be satisfied that a proposed warrant is necessary for national security or foreign intelligence purposes. As the senior law officer, balances security needs with human rights and rule of law considerations.	Judicial commissioners: independent persons required to approve any intelligence warrant that targets New Zealanders. Commissioners would apply their significant judicial experience, ensuring robust scrutiny is applied to intelligence warrants.	The Inspector-General would review and audit the material supporting the application for a warrant and its execution, to ensure its execution is lawful and proper.

96. The "triple-lock" incorporates executive, judicial, and the Inspector-General's oversight and includes the key elements of prior authorisation and in-depth post-facto review. The United Kingdom Independent Reviewer of Terrorism Legislation, David Anderson QC, highlighted the strengths of New Zealand's oversight system, particularly the role of the Commissioner of Security Warrants and the "broad mandate and strong investigatory function" of the Inspector-General. We are confident the proposed system of oversight, particularly in relation to the issuing of warrants will continue to be world leading.

Ministerial Policy Statements

97. We recommend that Cabinet agree to the reviewers' recommendation for the establishment of Ministerial Policy Statements, but with more detail on their precise legal effect (as above at paragraphs 24-25). These statements would be approved by the responsible Minister after being referred to the Inspector-General for comment. There may be some tension for the Inspector-General providing comment on Ministerial Policy Statements, and then reviewing the agencies' compliance with those statements. We are of the view this tension can be managed appropriately and consider it important for Ministerial Policy Statements to be developed with the benefit of comments from the Inspector-General. This is also why we support the proposal for comment only, rather than consultation.

98. Ministerial Policy Statements would be issued for lawful activities carried out in the performance of the agencies' functions. Each statement should be required to set out:

    98.1 The type of activity it applies to;

    98.2 The purposes for which that information can be collected or the activity carried out;

    98.3 Any internal approvals required before collecting that information or carrying out an activity;

    98.4 Any limitations of methods that can be used; and

    98.5 Any protections that need to be put in place (e.g. privacy protections).

99. As discussed above at paragraphs 24-25, Ministerial Policy Statements would not affect the lawfulness or otherwise of an activity, but would be a mechanism to enable the responsible Minister to regulate the lawful activities of the agencies. For example,

physical surveillance in a public place is a lawful activity, but the Minister should set out the general parameters within which the agencies undertake that activity. The lack of a Ministerial Policy Statement would not invalidate otherwise lawful actions.

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

- surveillance in a public place;
- obtaining and using publicly available information;
- requests to telecommunications providers for communications data;
- provision of cyber security and information assurance services by consent;
- use of cover as a means to support intelligence collection or obfuscate activities;
- information sharing with foreign partners (will be discussed in Cabinet paper 5);
- requests for information from other any agency of the Crown and the private sector; and
- lawful human intelligence collection.

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

Special case of cyber security and information assurance by consent

102. The reviewers suggest that provision of cyber security and information assurance services by the GCSB should not require a warrant where those services are provided with the consent of the affected entity (e.g. the CORTEX programme). We recommend this proposal be accepted.

103. The GCSB's success in defending New Zealand's critical information infrastructures is a product of the speed with which it is able to detect and respond to an incident. Globally, it takes organisations an average of 200 days to detect that they have been compromised by a hostile actor. In contrast, the length of time it takes for a security compromise to occur is a matter of seconds (for example, if a user opens a malicious email attachment or clicks on a malicious link). The exfiltration, destruction or modification of sensitive and valuable data and the theft of secrets and intellectual property can then occur in a matter of seconds.

104. To provide effective protection, the GCSB needs to be able to respond quickly to cyberattacks. The requirement to get a warrant for activity conducted with the consent of the affected entity is unduly burdensome and leads to critical delays. Even when not time-critical, the services provided are well suited to a consent-based regime. We recommend the government give express recognition in the Bill that cyber security and information assurance services with consent do not require a warrant as they are a lawful activity and may be covered by a Ministerial Policy Statement. The legislation should not exclude the possibility of cyber security and information assurance services and other activities being provided without consent in some circumstances – in such cases the GCSB would need to seek an appropriate warrant.

105. To provide appropriate safeguards, information obtained by consent may only be used for the purpose of cyber security and information assurance unless an appropriate warrant is also obtained. For the avoidance of doubt, GCSB would still retain the ability (under current section 8A(c) of the GCSB Act) to report on intelligence obtained in the course of conducting cyber defensive services.

Miscellaneous warranting issues

106. We propose Cabinet accept the following recommendations of the Reviewers:

106.1 Allow warrants to be amended or revoked;

106.2 Require the agencies to keep a register of all warrants and Ministerial Policy Statements, and make that register available to the Inspector-General, the Minister responsible for the agencies, the Attorney-General and the judicial commissioners;

106.3 Require the agencies to report on the outcome (including whether the application was approved or declined) of tier one and tier two warrants in their annual reports;

106.4 extend s15C of the GCSB Act to both agencies (which provides protections for privileged material as defined in sections 54, 56, 58 and 59 of the Evidence Act 2006);

107. Some issues arising in this paper will be considered in the next suite of Cabinet papers, including:

107.1 Cover: the agencies' ability to obtain, create and use any identification information necessary for the purpose of carrying out their activities and maintaining the secret nature of those activities will be dealt with in Cabinet paper 5;

107.2 Immunities: The immunities available to the agencies (including persons or entities assisting the agencies) will be covered in Cabinet paper 5.

107.3 Information-sharing: the ability and limits on the agencies to obtain and share information domestically and internationally will also be covered in Cabinet paper 5.

Recommendations

The Minister for National Security and Intelligence and the Minister Responsible for the GCSB and in Charge of the NZSIS recommend that the Committee:

1. **note** that the Independent Review of the Intelligence Security recommended the following:

    1.1 the establishment of a comprehensive authorisation regime with three tiers:

        1.1.1 Tier one: required for intelligence collection activities that would otherwise be unlawful for the purpose of targeting a New Zealand citizen or permanent resident;

        1.1.2 Tier two: required for the same types of activities as tier one warrants but where they are not being carried out for the purpose of targeting a New Zealander;

        1.1.3 Tier three: a policy statement approved by the Minister to provide authorisation for the conduct of lawful activities that involve gathering information about individuals and organisations.

    1.2 the agencies be permitted to conduct the following activities where that activity would be otherwise unlawful:

        1.2.1 Interception of communications;

        1.2.2 Acquisition of information held by third parties;

        1.2.3 Accessing information infrastructures;

        1.2.4 Surveillance (including using video, listening and electronic tracking devices); and

        1.2.5 Use of human sources.

    1.3 the basis for issuing a warrant would be outlined in a statutory test where the Attorney-General, and the judicial commissioner in the case of tier one warrants, would need to be satisfied that:

        1.3.1 The proposed activity is necessary either:

            1.3.1.1 For the proper performance of one of the agency's functions; or

            1.3.1.2 To test, maintain or develop capabilities or train employees for the purpose of performing the agency's functions;

        1.3.2 The proposed activity is proportionate to the purpose for which the authorisation is sought;

        1.3.3 The outcome sought cannot reasonably be achieved by less intrusive means;

1.3.4 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

1.3.5 There are satisfactory arrangements in place to ensure that information is only obtained, retained, used and disclosed in accordance with legislation;

1.4 the Attorney-General should be required to refer warrants 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;

1.5 the agencies should be able to obtain warrants (both tiers) aimed at a particular purpose, which would specify the type of information sought and the operational purposes for which it is required;

1.6 a detailed framework to deal with a range of urgent situations;

1.7 a panel of three judicial commissioners headed by a Chief Commissioner of Intelligence Warrants replace the current single Commissioner of Security Warrants;

2. **agree** the reviewers' recommendations provide a useful basis to develop a comprehensive and unified warranting regime;

3. **note** that the regime proposed by the reviewers does not include sufficient detail for an effective warranting regime;

4. **note** that fully merging the powers of both agencies as suggested by the reviewers would amount to a significant expansion in the powers of the agencies, particularly the GCSB;

5. **agree** the underlying policy principles underpinning the Government's approach to a new warranting regime should be to :

5.1 simplify the legislation to make it easier for the agencies and the public to understand what the agencies' powers are, and under what circumstances they can be exercised.;

5.2 modernise the warranted powers available to the agencies and to provide a clear legal basis for the activities of the agencies, and the protections that apply;

5.3 consolidate and harmonise the existing powers of both agencies under a single, framework, whereby similar activities are authorised in the same way;

5.4 maintain appropriate distinctions between the powers of NZSIS and GCSB powers to give effect to a warrant to reflect their different capabilities, within the context of a unified framework that facilitates greater coordination and collaboration;

5.5 make clear that only unlawful activity requires a warrant; and

5.6 remove unnecessary barriers to effective cooperation between agencies.

6. **note** a unified warranting framework would support work underway to enhance collaboration and coordination in the New Zealand Intelligence Community;

7. **note** the proposed unified warranting regime would be consistent with the intent of capability reviews in seeking to remove the unnecessary barriers to cooperation, while retaining appropriate distinctions in the powers to recognise each agency's particular expertise and capabilities;

8. **agree** to the reviewers' recommendation to create a three tier authorisation framework with the legislation making it clear that the reviewers' third tier "Ministerial Policy Statements" would set the parameters for the conduct of lawful activities rather an act as a mechanism for legal authorisation of those activities;

9. **agree** the warranting regime would include two types of warrant:

    9.1 Warrants (Tier one): required for intelligence collection activities that would otherwise be unlawful and are proposed for the purpose of targeting a New Zealand citizen or permanent resident. Warrants would be issued by the Attorney-General and a judicial commissioner;

    9.2 Warrants (Tier two): required for the same activities as tier one warrants but where those activities are not proposed for the purpose of targeting a New Zealander. These warrants would be issued by the Attorney-General and would not require the involvement of a judicial commissioner;

10. **note** the agencies would retain all the powers of a natural person;

11. **agree** that lawful intelligence activities of the intelligence agencies could be regulated by Ministerial Policy Statements, but would not require formal legal authorisation under the warranting regime;

12. **note** the this regime would only apply to the activities of intelligence agencies, which are subject to Ministerial control and are of keen public interest, and not to law enforcement and regulatory agencies which have their own authorising and oversight mechanisms;

13. **agree** the Minister responsible for issuing warrants under the proposed regime would be the Attorney-General;

14. **note** that this would not preclude the Minister responsible for the agencies being at the same time the Attorney-General as is the case currently;

The proposed warranting regime

15. **agree** that the warranting regime must maintain the current powers of both agencies;

16. **note** that Cabinet paper one outlines the shared objectives and functions of the agencies;

17. **agree** that the agencies should have a shared set of powers described in plain language that could be authorised under a warrant;

18. **agree** that the agencies would be able to apply for a warrant to exercise one or more of the following powers (only where it is otherwise unlawful):

18.1 Intercept communications;

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

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

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

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

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

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

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

19. **note** the creation of a warrant to cover the collection of intelligence from human sources is proposed for the first time;

20. **agree** that the agencies would have separate powers to give effect to a warrant;

21. **note** that the powers to give effect in the NZSIS Act require significant modernisation to bring them in line with those in the Search and Surveillance Act (with necessary and appropriate modifications for an intelligence and security agency);

22. **agree** the full suite of powers to give effect to a warrant would only be available to NZSIS as this aligns with its current capabilities, and only an appropriate subset of those powers would be available to GCSB in recognition of its different role and capabilities;

23. **agree** that both agencies would be able to exercise the following powers to give effect to a warrant:

23.1 access (instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of, including any audio or visual capability) an information infrastructure;

23.2 install, use, maintain or remove an interception device;

23.3 extract and use any electricity; and

23.4 install, maintain, use or remove an audio or visual surveillance device to maintain the operational security of a warranted activity;

24. **agree** that the NZSIS only would be able to exercise the following powers to give effect to a warrant unless the agencies were operating under a joint warrant, when they would be available to both agencies:

    24.1 install, use, maintain or remove a visual surveillance device;

    24.2 install, use, maintain or remove a tracking device;

    24.3 break open or interfere with any vehicle or other thing;

    24.4 enter any place, vehicle or other thing authorised by the warrant;

    24.5 take photographs, sound and video recordings, and drawings of a place vehicle or other thing searched, and of any thing found in or on that place vehicle or other thing;

    24.6 Use any force in respect of any place vehicle or thing that is reasonable for the purposes of carrying out a search or seizure;

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

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

25. **agree** that the powers to give effect would be supported by the following general ancillary powers:

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

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

26. **note** the central of role of accessing information infrastructures to the intelligence collection capabilities of GCSB;

27. **agree** if necessary to include in legislation a provision maintaining its current scope for the avoidance of doubt;

28. **agree** that the warranting regime requires a degree of flexibility in terms of its targeting in order to respond to a more complex range of threats;

29. **agree** that warrants of both agencies should also be able to be directed towards a particular class of targets;

30. **agree** that warrants of both agencies should be able to rely on a description of the particular targets where the precise identity of the target is unknown;

31. **agree** the agencies should be able to obtain warrants aimed at a particular purpose where the warrant application would specify the type of information sought and the operational reasons requiring its collection;

32. **note** that purpose-based warrants would need to be sufficiently limited to be Bill of Rights Act consistent;

33. **agree** that the legislation should include a legislative presumption in favour of targeted warrants;

34. **agree** that tier one warrants (including purpose-based warrants) would be limited in the following ways:

    34.1 Installation of surveillance devices could only be authorised where the application identified a specific target;

    34.2 Access to an information infrastructure would require the warrant application to identify the specific information infrastructure (or class of information infrastructures) to be accessed;

35. **agree** to establishment of a "review warrant" which would enable the agencies to use incidentally obtained intelligence about a New Zealander collected under a tier two warrant, by applying for a tier one warrant;

36. **agree** that in those circumstances the intelligence could not be retained unless a review warrant is obtained or one of the grounds for disclosing incidentally obtained intelligence to a public authority is met;

37. **agree** that the agencies would be able to obtain a removal warrant (similar to section 4I of the NZSIS Act) to remove previously installed surveillance or interception devices;

38. **agree** that in order to issue a warrant, the Attorney-General (and the judicial commissioner in the case of tier one warrants) would need to be satisfied that:

    38.1 The proposed activity is necessary either:

        38.1.1 For the proper performance of one of the agency's functions;

        38.1.2 To test, maintain or develop capabilities; or

        38.1.3 To train employees for the purpose of performing the agency's functions;

    38.2 The proposed activity is proportionate to the purpose for which the authorisation is sought;

    38.3 The outcome sought cannot reasonably be achieved by less intrusive means;

    38.4 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

    38.5 There are satisfactory arrangements in place to ensure that information is only obtained, retained, used and disclosed in accordance with legislation;

39. **agree** that the Attorney-General should be required to refer warrant applications to the Minister of Foreign Affairs for consultation on foreign policy and international relations implications;

40. **agree** that the Attorney-General and Minister of Foreign Affairs develop a joint protocol prior to commencement of the legislation to ensure the consultation process works in an effective and timely manner;

41. **agree** to the following to address situations of urgency:

    41.1 require the Prime Minister to designate a Minister to have a standing power to act on behalf of the Attorney-General in the event the Attorney-General cannot be contacted;

    41.2 require the Prime Minister to designate a Minister to act on behalf of the Minister of Foreign Affairs when he or she is unavailable;

    41.3 make provision for warrants to be issued orally in exceptional circumstances (e.g. over the phone); and

    41.4 have multiple judicial commissioners;

42. **agree** that the Attorney-General could alone authorise tier one warranted activity to occur (an "interim authorisation") where:

    42.1 Where there is an imminent threat to the life or safety of any person; or

    42.2 Where the delay associated with obtaining a warrant through the ordinary process is likely to seriously prejudice national security;

43. **note** there may be some particularly serious situations where even an interim authorisation is likely to cause delay to such an extent that the purpose of obtaining a warrant would be defeated;

44. **agree** that in only those circumstances a Director should be able to make an urgent authorisation (an "urgent Director authorisation");

45. **agree** that where an urgent Director authorisation is granted, the Director should notify the Attorney-General (and the Chief Commissioner of Intelligence Warrants in respect of activity requiring a tier one warrant) without delay and provide a full application within 24 hours;

46. **agree** that all urgent authorisations would need to be referred to the Inspector-General for review as soon as practicable, and the agencies would be required to report in their Annual Report the number of times interim authorisations or urgent Director authorisations were used during the reporting year;

47. **agree** that the legislation should allow for the submission of joint warrant applications;

48. **agree** that under a joint warrant, the agencies could be authorised to use the full suite of powers (including through the use of powers to give effect available to only one agency);

49. **note** that in practice, the GCSB has not been able to provide assistance to New Zealand Police in a timely or effective manner;

50. **note** that there are ongoing discussions between New Zealand Police and GCSB aiming to resolve potential issues that may be preventing effective cooperation;

51. **direct** officials from DPMC, New Zealand Police and the GCSB to report to the Minister for National Security and Intelligence, the Minister of Police and the Minister Responsible for the GCSB by 31 May 2016 on how to ensure effective cooperation under the new framework, including under a GCSB / New Zealand Police protocol;

52. **note** that there may be some further matters of detail that emerge in the drafting process which might require some amendment to the proposed warranting regime;

53. **agree** to grant the Minister for National Security and Intelligence and the Minister responsible for the GCSB and in Charge of the NZSIS 'power to act' in respect of any necessary policy decisions relating to the warranting regime that may emerge through the drafting process;

Role of judicial commissioners

54. **note** the institutional arrangements relating to the appointment and administrative arrangements for judicial commissioners will be addressed in Cabinet paper 4;

55. **note** sitting judges would not be appointed as judicial commissioners;

56. **note** reviewers recommend limiting the role of the judicial commissioner to consideration of legal factors;

57. **agree** that the legislation should not limit the role of judicial commissioners;

58. **agree** that the Attorney-General and judicial commissioner jointly issue tier one warrants;

Safeguards: The "Triple-lock" for tier one warrants

59. **agree** that Intelligence warrants that target New Zealanders would be subject to three important safeguards – a "triple lock", as Tier one warrants would be:

    59.1 authorised by the Attorney-General;

    59.2 approved by a judicial commissioner; and

    59.3 subject to the review and audit of the Inspector-General;

Ministerial Policy Statements

60. **agree** to the reviewers' recommendation for the establishment of Ministerial Policy Statements;

61. **agree** Ministerial policy statements would be approved by the responsible Minister after being referred to the Inspector-General for comment;

62. **note** Ministerial Policy Statements would be issued for lawful activities carried out in the performance of the agencies' functions;

63. **agree** that the lack of a Ministerial Policy Statement would not invalidate otherwise lawful actions carried out by the agencies;

64. **agree** each Ministerial Policy Statement should be required to set out the following (if applicable):

    64.1 the type of information or collection activity it applies to;

    64.2 the purposes for which that information can be collected or the activity carried out;

    64.3 any internal approvals required before collecting that information or carrying out an activity;

    64.4 any limitations of methods that can be used; and

    64.5 any protections that need to be put in place (e.g. privacy protections).

65. **note** Ministerial Policy Statements would be an important component of the proposed new regime and would enhance oversight and compliance, as they would provide an objective standard against which the propriety of the agencies' lawful activities can be assessed;

Special case of cyber security and information assurance by consent

66. **note** the reviewer's recommendation that the provision of cyber security and information assurance services by the GCSB should not require a warrant where those services are provided with the consent of the affected entity (e.g. The CORTEX programme);

67. **agree** to include in legislation a provision that makes clear that cyber security and information assurance with consent do not require a warrant as they are a lawful activity and may be covered by a Ministerial Policy Statement;

68. **agree** that cyber defence services by consent would be subject to the following safe-guards:

    68.1 information obtained by consent may only be used for the purpose of cyber defence unless an appropriate warrant is also obtained;

Miscellaneous warranting issues

69. **agree** that legislation address the following miscellaneous issues:

    69.1 allow warrants to be amended or revoked;

    69.2 require the agencies to keep a register of all warrants and Ministerial Policy Statements, and make that register available to the Inspector-General, the Minister responsible for the agencies, the Attorney-General and the judicial commissioners;

69.3 require the agencies to report on the outcome of tier one and tier two warrants in their annual reports;

69.4 extend s15C of the GCSB Act to both agencies to protect the privileged communications of New Zealanders;

70. **note** that some issues arising in this paper will be considered in Cabinet paper five:

70.1 Cover: the agencies' ability to obtain, create and use any identification information necessary for the purpose of maintaining the secret nature of their activities will be dealt with in Cabinet paper 5;

70.2 Immunities: The immunities available to the agencies (including persons or entities assisting the agencies) will be covered in Cabinet paper 5;

70.3 Information-sharing: the ability and limits on the agencies to obtain and share information domestically and internationally will also be covered in Cabinet paper 5.

Authorised for lodgement

Rt Hon John Key
Minister for National Security and Intelligence

Hon Christopher Finlayson
Minister Responsible for the GCSB
Minister in Charge of the NZSIS

ANNEX: SHARED WARRANTING FRAMEWORK FOR NZSIS & GCSB

WARRANT FOR THE PURPOSE OF (para 38)

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

Functions (set out in full in para 38 of paper one)

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

SHARED WARRANTABLE POWERS (para 39)

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

GCSB only

SEPARATE POWERS TO GIVE EFFECT (paras 53 and 54)

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

- Access to information infrastructure

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

SHARED, GENERAL ANCILLARY POWERS (para 55)

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