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

Chair, National Security Committee

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

Paper Six: Activities of the intelligence agencies – Information sharing and arrangements with foreign partners

Proposal

1. This paper seeks Cabinet policy decisions on the information sharing framework and arrangements with foreign partners, for the Intelligence Services and Oversight Bill (the Bill). It follows the release of the report of the first *Independent Review of Intelligence and Security* (the review) on 9 March 2016.

Executive Summary

2. The review makes a number of recommendations aimed at improving the intelligence and security agencies' (the agencies) access to information held by other government organisations, and at improving transparency and oversight around cooperation and intelligence sharing with foreign partners.

3. The reviewers' recommended changes include (but are not limited to):

    3.1 allowing the agencies to access and retain certain datasets (for example, Customs and Immigration datasets) subject to joint protocols governing access and retention;

    3.2 allowing other organisations to provide information that cannot currently be shared due to a statutory prohibition (for example, tax information) to the agencies, provided there is a warrant in place;

    3.3 expressly allowing the agencies to co-operate and share intelligence with foreign jurisdictions and international organisations, provided this is consistent with the Bill's purposes and the agencies' obligations to act in accordance with New Zealand law;

    3.4 requiring that any future bilateral or multilateral arrangements entered into with foreign jurisdictions and international organisations are referred to the Intelligence and Security Committee (ISC) for noting; and

    3.5 requiring the agencies to develop standard terms for ad hoc intelligence cooperation or sharing, with the draft terms provided to the Inspector-General

of Intelligence and Security (IGIS) for comment and the final terms provided to the ISC for noting.

4. We recommend that Cabinet accept these recommendations, amongst others. In addition, we recommend that officials undertake further work on options for clarifying the law around the information that may be requested by, and shared with, the agencies on an ad hoc basis.

5. The proposed changes would improve the agencies' access to information that they regularly need and would provide more transparency and oversight in terms of New Zealand's arrangements with foreign partners.

Background

6. To achieve its policy aims, the government must be able to share information collected by one of its organisations with other organisations that have a legitimate need to access the information in question. This ability is increasingly important given the drive for improved collaboration between government organisations and the move to provide more public services online.

7. The need to share information extends beyond the public sector, to private sector organisations. There are many legitimate reasons why information gathered by the private sector should be shared with government organisations and especially with the intelligence and security agencies, as discussed below.

8. The need to share information must always be balanced with the obligation to protect the privacy rights of the individuals to which it relates, regardless of the strength of the need to share information. In New Zealand, the Privacy Act 1993 sets out information privacy principles for how public and private sector organisations should collect, use, disclose, store and dispose of personal information. Principle 11 states that organisations (both public and private sector) shall not disclose personal information except in certain circumstances. As discussed below, the Privacy Act 1993 has a limited - and often ambiguous - application to the intelligence and security agencies.

9. In recent years, the government has moved to clarify the law and to enhance the information sharing toolbox available to government organisations. Clear rules about information sharing are beneficial because they:

    9.1 give government organisations legal confidence about their ability to share information, avoiding an organisational culture that discourages information sharing because of a fear of legal repercussions. This in turn reduces the risk that an agency will fail to share information that, to use an extreme example, could have saved lives;

    9.2 break down silos between government organisations, improving collaboration between government organisations and therefore policy outcomes;

    9.3 improve transparency around the ability of government organisations to share information, so that the public can easily understand how their personal information is shared, why, when and with whom;

9.4 reduce transaction costs and the burden on individuals since they do not need to provide the same information more than once to different government organisations; and

9.5 reduce the need for government organisations to use intrusive means to obtain information (which is of particular relevance to the intelligence and security agencies).

10. For example, government organisations are now able to develop approved information sharing agreements (AISAs). AISAs allow government organisations to depart from the privacy principles if there is a clear public policy justification and the privacy implications of doing so are managed appropriately. Examples of information shared under AISAs include:

10.1 passport information collected by the Department of Internal Affairs, which is shared with the Inland Revenue Department to enable it to make contact with overseas based student loan borrowers and liable parents who are in default of their obligations;

10.2 information shared between social, health, education and justice sector organisations to identify vulnerable children, assess their needs and inform the appropriate service response; and

10.3 information from the Inland Revenue Department, which is shared with the New Zealand Police for the purpose of preventing, detecting, investigating, or to use as evidence of, serious crime.

11. The sharing of information with the intelligence and security agencies is therefore not in and of itself a unique phenomenon. Information is shared within government and between the government and the private sector every day, in a range of ways and for a variety of different reasons. Information sharing with the intelligence and security agencies is, however, somewhat different because of the purposes for which information is shared (ie, that of intelligence gathering) and because of the lack of visibility in terms of how that information is collected, used, disclosed and retained.

State of play: How information is currently shared with the intelligence and security agencies

12. The intelligence and security agencies need to collect a range of information from various sources to perform their statutory functions. Sometimes this extends to collecting information in ways that are ordinarily unlawful (for example, by intercepting communications), but which are permitted under warrant in particular cases. This is the type of 'collection' typically associated with the agencies.

13. In other cases, the agencies may need to access information that is lawfully collected and held by other government organisations (for example, information held by Customs relating to arrivals into the country). The agencies may also need to access information held by private sector organisations; for example, call associated data from telecommunications companies or transaction records from banks.

14. As mentioned above, the Privacy Act 1993 sets out principles for how public and private sector agencies should collect, use, disclose, store and dispose of personal information. Section 57 of the Privacy Act 1993 exempts information collected,

obtained, held, used, or disclosed by, or disclosed to, an intelligence organisation from most of these principles.

15. The reviewers stated that section 57 is generally interpreted as currently allowing the agencies to access personal information held by other organisations but only on a case-by-case basis. As the reviewers noted, this process can be resource intensive and time consuming, especially in relation to datasets that the agencies need to access frequently (such as information about entries to and departures from New Zealand). Further, section 57 is not framed as an empowering statement for the organisation releasing the information, but rather limits the application of the information privacy principles in certain situations.

16. The New Zealand Security Intelligence Service (the NZSIS) currently has statutory functions that it construes as empowering provisions that enable it to carry out its functions. These functions include to:

    16.1 obtain, correlate, evaluate intelligence relevant to security and to communicate any such intelligence to such persons and in such manner, as the Director considers to be in the interests of security (section 4(1)(a));

    16.2 advise any of the following persons on protective measures that are directly or indirectly relevant to security: Ministers, government departments, public authorities and any person who the Director thinks should receive it (section 4(1)(ba)); and

    16.3 conduct inquiries into whether particular individuals should be granted security clearances and to make appropriate recommendations based on those inquiries (section 4(1)(bb).

17. This approach to information gathering and sharing reflects an older style of legislating, with the courts now tending towards requiring specific statutory authority for both information sharing and positive government actions. When another government organisation's governing legislation sets out specific information sharing provisions that do not include the intelligence and security agencies (because, for example, it was anticipated these powers were not needed due to the wider powers under the agencies' own legislation and due to section 57 of the Privacy Act 1993), it raises questions about whether Parliament intended the general powers to remain (including to allow the agency to share the information), or whether 'the field has been covered' by the specific provisions.

18. Section 8E of the Government Communications Security Bureau Act 2003 (the GCSB Act 2003) provides that the Director of the Government Communications Security Bureau (the GCSB) has all the powers that are necessary or desirable for the purpose of performing the functions of the GCSB. The GCSB considers that this provides statutory authority for it to request information from other organisations.

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

Domestic information sharing

20. In light of the possible impacts of information sharing on the privacy of individuals, access to personal information must be justified and the means must be proportionate to the objective sought. Similarly, personal information must be shared in accordance with relevant safeguards and the agencies' compliance with these safeguards independently monitored.

21. It is vital, however, that privacy interests are balanced with the need to share information. Information about individuals posing a threat to New Zealand's national security may be found in different places across government and the private sector. In order for a complete picture to be built, that information must be pieced together by the agencies.

22. For example, certain patterns of behaviour, such as travelling to particular countries, are not necessarily worthy of further investigation in isolation. It is when that behaviour is paired with other causes for suspicion, such as contact with known extremists, that a meaningful intelligence picture can start to be formed. This is particularly relevant in the modern context, where the vast majority of information is stored digitally and spread across multiple datasets.

23. Effective, efficient and responsible sharing of information between the various institutions of government is, therefore, increasingly essential to the government's ability to identify, understand and respond to threats to its national security. As noted in the report of the 9/11 Commission:

> *"Our intelligence and law-enforcement agencies did not manage or share information, or effectively follow leads to keep pace with a nimble enemy. … The US government has access to a vast amount of information. But it has a weak system for processing and using that information. … We need to ensure that our government maximizes their efforts through information sharing … But we stress that these measures need to be accompanied by a commitment to our open society and the principle of review – safeguards that are built into the process and vigorous oversight. We must, after all is said and done, preserve the liberties that we are fighting for."*

24. We propose that the Bill set out a clear and transparent framework for information sharing - one that recognises the fundamental importance of privacy, while facilitating essential cooperation between government organisations. The current framework is not fit for purpose as it provides broad exceptions to the privacy principles for the agencies without clear empowering provisions or parameters for access and disclosure, therefore neither protecting privacy nor facilitating access to information.

25. We therefore recommend that Cabinet agree to the reviewers' recommendations relating to access to datasets (with one exception) and case-by-case access to restricted information. We recommend further work to clarify the law around the agencies' ability to request the disclosure of personal information and the ability of other organisations to disclose personal information to the agencies, during which officials should consider whether additional information privacy principles should apply to the agencies.

26. The agencies regularly provide the product of their intelligence collection and analysis to Ministers, public authorities and others. This is one of their main functions as agreed

by Cabinet [CAB-16-MIN-0142 refers] and as outlined in Cabinet paper one: Overview and key issues. The provision of such intelligence and advice is therefore not considered 'information sharing' for the purpose of this paper.

Access to certain datasets

27. The reviewers proposed that the Bill expressly permit the agencies to access and retain the datasets listed in table 1 below. We note that the reviewers did not expressly address use or disclosure of this information in the context of their specific recommendations; we consider that use and disclosure should be considered alongside access and retention.

28. The lack of provision currently prevents the agencies from directly accessing datasets to which this recommendation applies.

Table 1: Access, use, disclosure and retention of datasets

Dataset	Examples of why access may be needed
Information about border-crossing craft and persons held by the New Zealand Customs Service, and Advanced Passenger Processing data collected by Immigration New Zealand.	– To cross-check information against information about arrivals at the border, to detect the arrival of foreign intelligence officers or other persons of interest (such as suspected terrorists).
Immigration New Zealand databases.	– To allow the GCSB or NZSIS to ascertain if a person is a New Zealander, to determine whether to apply for a tier one or tier two warrant.
Information held in New Zealand Police's National Intelligence Application.	– To allow the agencies to determine the physical safety risk to its field officers posed by certain individuals (who may be under investigation or may be on the periphery of an investigation).
Births, deaths, marriages and relationships, and citizenship registers.	– To allow the agencies to cross-check information to certify identity or associations between persons of interest, or to ascertain nationality.

29. We recommend that Cabinet accept this recommendation with the exception of access to the National Intelligence Application (NIA). Further discussions with the New Zealand Police have led officials to believe there is not a strong case for legislative authority for access to the NIA at this time. Rather, issues of physical security are best handled through the agencies continuing to work closely with the NZ Police as issues arise. The NZ Police is committed to providing the best information to the agencies where legal authority for disclosure exists, along with specialist advice in this area.

30. The reviewers did not expressly address allowing the agencies to access Customs information about border-crossing goods (instead focussing on access to information

about border-crossing craft and persons). However, Customs has clarified that it would be difficult for the agencies to access information about border-crossing craft and persons without simultaneously accessing information about border-crossing goods. Having regard to the scope of the National Intelligence Priorities, we consider that there is a compelling case for allowing the agencies to access this information.

31. To future proof the Bill, we recommend that the datasets be described in a schedule to the Bill and that the schedule may be amended to add, remove or modify any of the entries by Order in Council made by the Governor-General on the advice of the Minister, after consultation with the ISC.

32. We also recommend that the datasets are described generally in the Bill (rather than named), so that the agencies do not lose the ability to directly access a dataset simply because its name, or the way in which information is held, changes.

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

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

35. We consider that requiring the agencies to request this information on a case-by-case basis is not practical, given how often the agencies need to access this information. This is a resource intensive requirement for both the agencies and the organisations providing the requested information.

36. Compared to access on an ad hoc case-by-case request basis, direct access minimises adverse privacy impacts on individuals in appropriate cases. It ensures other organisations are not unnecessarily alerted to the interest of an intelligence agency in a particular individual, which itself has privacy implications for that person. Data matching is also inherently less intrusive because it minimises the number of people that view the information and ensures that only pertinent information is selected for further analysis.

37. Allowing the agencies to easily check that information about an individual is accurate would enable them better to judge whether that the person is of security concern, reducing the risk of surveillance targeting the wrong person. For example, where a person has the same name as a person of security concern, the agencies would be able to easily cross check the information they hold against births, deaths, marriages, and relationship registers or against border crossing information, to ensure they are focusing on the correct person.

38. We also consider that expressly allowing the agencies access to the specified datasets in primary legislation builds transparency, as it makes their powers in this area clear. At present the public does not have any visibility in terms of the agencies' ability to access personal information held by other government organisations.

Joint protocols

39. The reviewers recommend that access and retention to these datasets should be governed by joint protocol agreed between the responsible Minister (or Ministers, should the GCSB and NZSIS have different Ministers) and the Minister responsible for the organisation holding the relevant dataset. We recommend that Cabinet accept this recommendation (and extend it to use and disclosure), as it is essential to ensuring that the agencies' ability to access these datasets is limited, justified and transparent.

40. We recommend that Cabinet agree that a joint protocol should specify the purposes for which the information contained in each dataset can be accessed and retained (as well as used and disclosed).

41. The reviewers recommended that joint protocols should be agreed in consultation with the Privacy Commissioner. We consider that the Privacy Commissioner should be consulted during a joint protocol's development, but that his or her approval should not be required. We note that the Privacy Commissioner is consulted during the development of AISAs and may make a submission on a draft AISA to the organisations developing it (see section 96O of the Privacy Act 1993).

42. The Commissioner would consider:

    42.1 whether the data is needed for the agencies to discharge their statutory functions;

    42.2 whether only as much information will be retained as is necessary to discharge the statutory function;

    42.3 whether the level of interference with the individual's 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;

    42.4 whether the protocol sets out appropriate procedures for the access, use, retention, disclosure, and deletion of the dataset; and

    42.5 any other privacy implications of the proposed access.

43. This consultation requirement allows the agencies and Ministers to use the Privacy Commissioner's considerable expertise to develop robust protocols that appropriately balance the need to access information with the privacy rights of the people to whom the information relates. It also builds in an element of independent input.

44. In addition to the reviewers' recommendations, we recommend that the IGIS should also be consulted during the development of a joint protocol. This is consistent with the approach taken to the GCSB policy on personal information (section 25A of the GCSB Act 2003), where both the Privacy Commissioner and IGIS must be consulted.

45. We also agree with the reviewers' recommendations:

45.1 that the responsible Ministers[1] review each protocol every three years, specifically the operational and legal justification for the continued access, use, disclosure, and retention of the dataset;

45.2 that the IGIS should monitor the agencies' compliance with each protocol; and

45.3 that 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, including appropriate training for staff and processes to ensure that users only access the datasets where justified.

46. We also recommend that each three yearly review is undertaken in consultation with the Privacy Commissioner and the IGIS.

47. To build transparency, we recommend that the parties to a joint protocol each publish a summary of the joint protocol on their websites once it is agreed and following the completion of each three yearly review (ensuring that publication occurs in a manner compliant with requirements of security). We note that the Official Information Act 1982 would apply to joint protocols in the usual manner.

48. Each of these recommendations will help to ensure that the continued access is justified, transparent, secure, and subject to executive and independent oversight.

Commencement of the Bill's provisions allowing access to datasets

49. A lack of easy access to the Customs and Immigration datasets and the Department of Internal Affairs registers presents severe operational difficulties for the agencies.[2] Given the nature of these datasets, if access is not automated (ie, if direct access is not provided for) then the value of access is nullified, because the information cannot be gained with any currency, the fact of the search may give away classified information, and the data may not be received or utilised in a way necessary for matching or cross-checking.

50. We therefore recommend that Cabinet agree to bring the sections allowing the agencies access to these datasets into force the day after Royal Assent. In line with ensuring appropriate oversight, we also recommend that the provisions requiring joint protocols to be developed are also brought into force at this time.

A parallel mechanism for access in new Customs legislation

51. In September 2015 Cabinet agreed to develop new customs and excise legislation to replace the Customs and Excise Act 1996 [EGI-15-MIN-0066 refers]. In relation to information disclosure, it agreed to:

51.1 allow Customs to disclose information it holds for a range of purposes, including 'national security';

[1] By 'responsible Ministers' we mean the Minister Responsible for the GCSB / the Minister in Charge of the NZSIS and the Minister responsible for the organisation that is the statutory custodian of the information.
[2] In 2014 the Customs and Excise Act 1996 was amended to give the NZ Police and the NZSIS direct access to Customs data, but for counter-terrorism purposes only.

51.2 allow disclosure to occur to organisations falling within the definition of 'department' in section 2 of the Public Finance Act 1989 (this captures the GCSB and the NZSIS);

51.3 only allow disclosure of biometric information, passenger name records and intelligence generated by Customs, for certain purposes - including national security;

51.4 allow Customs and the receiving organisation to enter into a written 'information disclosure arrangement' where a request is for regular or ongoing disclosure of information, following consultation with the Privacy Commissioner; and

51.5 provide for direct access to Customs' information databases for certain purposes (including national security), subject to an information disclosure arrangement.

52. This new legislation would therefore create another avenue for the agencies to access Customs information, in addition to that recommended by the reviewers. We consider that having two parallel schemes for access on the statute book is undesirable. We also consider that the scheme proposed by the reviewers is more appropriate for the GCSB and NZSIS given the nature of their work. Having all of the agencies' dataset access arrangements in one place and subject to enhanced oversight arrangements will also achieve a higher level of transparency and accountability. In addition, we note that:

52.1 joint protocols – which will be similar to information disclosure arrangements - will be agreed at a ministerial level (compared to at an organisation level), which is appropriate given the nature of the agencies' work;

52.2 there will be more independent input into a joint protocol's development than into an information disclosure arrangement's development, since both the Privacy Commissioner and the IGIS will be consulted (compared to the Privacy Commissioner alone); and

52.3 there will be independent oversight of compliance with joint protocols, provided by the IGIS.

53. We understand that the new Customs legislation is currently being drafted and that the aim is for it to be introduced in September 2016 and passed by the 2017 General Election. In contrast, the Intelligence Services and Oversight Bill must be passed by 31 March 2017 - meaning that the agencies will get access to Customs' datasets under this Bill much earlier than they would under Customs' new legislation, which is highly desirable from an operational perspective.

54. We therefore recommend that Cabinet agree that the agencies are not able to use the disclosure framework in the new legislation replacing the Customs and Excise Act 1996, and that officials from those agencies and Customs work with the Parliamentary Counsel Office to determine how best to incorporate that exclusion into legislation.

Access on a case-by-case basis to restricted information

55. Some information held by other government organisations is needed by the agencies less frequently and only in specific investigations, meaning that direct access to this information is unnecessary and unlikely to be a proportionate response. We agree with the reviewers that allowing the agencies to obtain this information on a case-by-case basis is more appropriate in these situations.

56. However, as noted above, the section 57 exemption contained in the Privacy Act 1993 does not allow other organisations to share information where there is a statutory restriction on sharing that information. We agree with the reviewers' view that there is some information in this category that the agencies should be able to access.

57. We therefore recommend that Cabinet agree to the reviewers' recommendation to allow the agencies to access the following information about identified individuals or organisations by request on a case-by-case basis pursuant to a tier one or two warrant (depending on the nationality of the person to whom the warrant relates).

Table 2: Access to restricted information allowed under warrant

Information	Reason why access may be needed
Tax information held by the Inland Revenue Department.	– To understand a person's financial situation in order to inform an assessment of the threat they may pose to national security (eg, through the financing of terrorism).
Driver licence photographs held by the New Zealand Transport Agency.	– To support operational activity by confirming the identities of individuals of security concern.
National Student Identification Numbers linked information.	– To determine whether persons of interest are taking courses of security concern.

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

59. The rationale for accessing NSIN linked tertiary education records is that the tertiary study that someone has undertaken may contribute to understanding the security risks associated with that individual.

60. We therefore recommend including amendments in the Bill requiring the organisations holding the information listed above to provide the relevant information to the GCSB or NZSIS upon request, provided that the GCSB or NZSIS hold a warrant in relation to that information. In relation to tax information, this may require an amendment to the

Tax Administration Act 1994 to override tax secrecy and require the Commissioner to comply with the warrant.

61. We think that a sound case exists for this limited overriding of these statutory prohibitions (including the secrecy obligation in tax legislation[3]). A tier one warrant is a high threshold and may only be obtained where the reviewers' narrowly cast threshold of national security is met. In the case of both tier one and tier two warrants, the Attorney-General will need to be satisfied, amongst other things, that the information is necessary for the proper performance of one of the agencies' functions, and that it is proportionate to that purpose.

62. We note that all warrants would be subject to review by the IGIS under his or her existing functions.

Ongoing work to clarify the application of the Privacy Act 1993

63. We are aware there are outstanding questions around disclosure of information, which have not been able to be resolved in the time allowed for the development of this Cabinet paper.

64. The agencies are eager to have an empowering statement that expressly allows them to request information in accordance with their functions. We also note there are questions about the ability of other organisations to disclose information to the agencies in light of section 57 of the Privacy Act 1993, particularly where another legislative scheme relating to disclosure of information is at play (as discussed above). In addition, we consider it may be appropriate for the agencies to be subject to more information privacy principles than is currently the case. We set out these issues in more detail below.

Agency requests for disclosure of information

65. The agencies regularly ask other organisations to disclose information to them. Since they are asking for information (rather than compelling disclosure), an express power is not technically required (particularly since the NZSIS has a wide statutory function in section 4A of its Act, which it reads as an empowering provision to obtain, evaluate and communicate information).

66. To create transparency around the agencies' powers we consider officials should consider including an empowering provision in the Bill, as part of the ongoing work proposed below. We envisage such a provision would allow the agencies to ask for information on an ad hoc case-by-case basis, with requests being limited to information necessary for the agencies to perform their functions.

[3] Tax secrecy exists to promote tax compliance by protecting information provided to the Inland Revenue Department and as a balance to its significant information gathering powers. Exceptions to tax secrecy exist in some limited circumstances where it is considered appropriate to do so. Provision of information to GCSB and NZSIS to fulfil their statutory functions under a tier one or tier two warrant is considered appropriate.

Disclosure of information to the agencies

67. As discussed above, there is a question about whether section 57 empowers an organisation to share information with the agencies, particularly where that organisation is subject to a more specific legislative scheme for information sharing. Section 57 is not framed as an empowering statement, but rather limits the application of the information privacy principles in certain situations. It also serves to limit the jurisdiction of the Privacy Commissioner in terms of complaints relating to breaches of the information privacy principles.

68. Some organisations currently provide information to the GCSB or NZSIS, both in response to a request from an agency and proactively (for example, when they come across some information they consider the GCSB or NZSIS should know about). We note that some organisations would prefer a positive power for them to share the information (whether in response to a request or proactively). We consider that options for addressing these issues should be provided to Ministers shortly, as recommended below.

Information privacy principles

69. The agencies regularly require access to personal information held by other organisations. Disclosure of such information usually occurs because of the section 57 exemption, which states: *Nothing in principles 1 to 5 or principles 8 to 11 applies in relation to information collected, obtained, held, used, or disclosed by, or disclosed to, an intelligence organisation.*

70. We recommend that further consideration be given to whether there are additional information privacy principles that the agencies should be subject to, noting that this must be able to be done without prejudicing the security or defence of New Zealand, or the international relations of the government of New Zealand. We recommend that officials further consider this issue over the coming weeks and make recommendations to Ministers, as outlined below.

Ministerial power to act

71. It is crucial to the agencies' operations that any changes to address these issues are clear, workable, and coherent. We therefore recommend that Cabinet:

    71.1. direct officials to provide advice to the Minister for National Security and Intelligence, the Minister of Justice and the Minister Responsible for the GCSB and In Charge of the NZSIS/the Attorney-General by 13 May 2016 about:

        71.1.1. including an empowering statement in the Bill allowing the agencies to request information from other organisations;

        71.1.2. options for clarifying the law around disclosure of information to the agencies; and

        71.1.3. whether to make the agencies subject to more information privacy principles than is currently the case, as well as options for doing so in a manner that is not prejudicial to the security or

defence of New Zealand, or the international relations of the government of New Zealand.

71.2. authorise the Minister for National Security and Intelligence, the Minister of Justice and the Minister Responsible for the GCSB/In Charge of the NZSIS/the Attorney-General to take decisions following officials' advice and to authorise the issuing of drafting instructions in relation to any such decisions, as necessary.

72. We recommend that Cabinet direct officials to develop the advice referred to above in consultation with the Privacy Commissioner.

Arrangements with foreign partners

73. The value to New Zealand of our international intelligence sharing and cooperation arrangements is significant. It may include exchanges of technology, skills and expertise, and intelligence products, amongst other things. In the current climate of global and transnational threats, it is in New Zealand's interest to foster these international relationships where they benefit New Zealand, particularly with the five eyes partnerships but also increasingly with non-traditional partners.

74. The reviewers recognised the importance of these relationships and the degree of cooperation and sharing that may occur within them. They proposed a series of recommendations to ensure that appropriate mechanisms are in place to oversee these relationships - to allow for a greater degree of transparency and oversight of these activities.

75. The reviewers recommended that the Bill explicitly enable the agencies to cooperate and share intelligence with foreign jurisdictions and international organisations. This will be generally allowed under the agencies' functions as agreed by Cabinet [CAB-16-MIN-0142 refers]. However, we agree that it should also be expressly permitted under a provision devoted to arrangements with foreign partners.

76. The reviewers recommended that the Bill make it clear that this cooperation and sharing must be consistent with the Bill's purposes, as well as with the agencies' obligations to act in accordance with New Zealand law (which is consistent with the way the agencies currently operate). We agree that this requirement should be made clear in the Bill.

77. To build greater transparency, we recommend that Cabinet agree with the recommendation that future bilateral or multilateral arrangements entered into with foreign jurisdictions or international organisations should be referred to the ISC, for noting.

78. Foreign policy objectives should be considered in the development and framing of sharing arrangements with foreign partners. We expect that the Ministry for Foreign Affairs and Trade will be consulted on any proposal to enter into an arrangement with a foreign jurisdiction or international organisation.

79. Sharing information with foreign entities outside traditional partnerships is essential to New Zealand's ability to protect its national security. However, when information is shared outside of well-established partnerships, it is no longer supported by the long-

standing intelligence sharing principles and practices which underpin the cooperation with that nation.

80. We therefore recommend that the Bill require the agencies to formulate standard terms for ad hoc intelligence cooperation or sharing, with the draft terms being forwarded to the IGIS for comment and the final version provided to the ISC for noting. These terms would establish consistent principles, standards and practices to ensure that New Zealand complies with its human rights obligations set out in domestic law.

81. The reviewers also recommended the government consider including restrictions on the circumstances in which information collected by the agencies about New Zealanders may be shared with foreign jurisdictions and international organisations. We agree that there will be some circumstances in which intelligence – regardless of the nationality of the person to whom it relates – should not be shared. A strong example is where there are legitimate concerns that the information may be used to punish someone in a manner inconsistent with human rights standards.

82. Cabinet has agreed that one of the shared functions of the agencies will be to share intelligence and analysis with anyone whom the Minister authorises to receive the information [CAB-16-MIN-0142 refers]. We recommend that the Bill therefore include a statement that the Minister should only authorise the sharing of information with foreign jurisdictions or international organisations in accordance with New Zealand law, particularly in accordance with the human rights recognised by New Zealand law, except to the extent that they are, in relation to national security, modified by an enactment.

Incidentally obtained intelligence

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

84. We therefore recommend carrying over and extending section 25 of the GCSB Act 2003 so that it applies to both agencies. Section 25 states that the relevant Director can only retain incidentally obtained intelligence where that intelligence is relevant to:

    84.1. preventing or detecting a serious crime;

    84.2. preventing or avoiding the loss of human life on the high seas;

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

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

85. Section 25 of the GCSB Act 2003 also provides that the relevant Director can only communicate that intelligence to:

85.1. any employee of the New Zealand Police;

85.2. any member of the New Zealand Defence Force;

85.3. the Director of the GCSB or the NZSIS, whichever is relevant; or

85.4. any public authority (whether in New Zealand or overseas) that the Director thinks fit to receive the information.

86. We note that this approach makes the agencies' powers in this area clear and accessible, further building transparency.

Access to an electronic copy of the electoral roll

87. The reviewers recommended that 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. We recommend that Cabinet invite us to refer this issue to the Justice and Electoral Select Committee once the Bill has been introduced, for its consideration.

Recommendations

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

1. **note** that the report of the first *Independent Review of Intelligence and Security* (the review) recommends a number of changes relating to access by the intelligence and security agencies (the agencies) to information held by other organisations, and to arrangements with foreign partners;

2. **note** that most of the recommended changes, if accepted, will be included in the proposed Intelligence Services and Oversight Bill (the Bill);

Access to certain datasets

3. **note** that the agencies regularly need to access information held by other organisations, in order to perform their functions under the Bill;

4. **note** that the agencies' need to access information held by other organisations must be balanced with the obligation to protect the privacy interests of the people to whom the information relates;

5. **agree** that the Bill should give the agencies the ability to directly access, use, disclose, and retain the following datasets:

    5.1. information about border-crossing craft, persons and goods held by the New Zealand Customs Service;

    5.2. Advanced Passenger Processing data collected by Immigration New Zealand;

    5.3. Immigration New Zealand datasets; and

    5.4. births, deaths, marriages and relationships, and citizenship registers;

6. **reject** the reviewers' recommendation that the Bill should give the agencies the ability to access and retain the NZ Police's National Intelligence Application;

7. **agree** that these datasets be described in a schedule to the Bill and that the schedule may be amended to add, remove or modify any of the entries, by Order in Council made by the Governor-General on the advice of the Minister, after consultation with the ISC;

8. **direct** the agencies to work with each organisation holding a relevant dataset to ensure as direct access as possible that meets the agencies' operational needs while minimising resourcing demands on the disclosing organisation;

9. **agree** that access to, and use, disclosure, and retention of, a dataset must be subject to a joint protocol agreed between the agency's Minister and the Minister responsible for the organisation that holds the relevant dataset;

10. **agree** that a joint protocol should specify the purposes for which the information contained in each dataset can be accessed and retained (as well as used and disclosed);

11. **agree** that the Privacy Commissioner should be consulted during a joint protocol's development;

12. **agree** that, as part of consultation, the Privacy Commissioner should consider:

    12.1. whether the data is needed for the agency to discharge its statutory function;

    12.2. whether only as much information will be retained as is necessary to discharge its statutory function;

    12.3. whether the level of interference with the individual's 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;

    12.4. whether the protocol sets out appropriate procedures for the access, use, retention, disclosure and (where applicable) deletion of the dataset; and

    12.5. any other privacy implications of the proposed access;

13. **agree** that the Inspector-General of Intelligence and Security (IGIS) should be consulted during a joint protocol's development;

14. **agree** that the responsible Ministers should review each joint protocol every three years, with a particular focus on the operational and legal justification for continued access, use, disclosure and retention of the dataset;

15. **agree** that each three yearly review of a joint protocol is undertaken in consultation with the Privacy Commissioner and the IGIS;

16. **agree** that the IGIS should monitor the agencies' compliance with a joint protocol;

17. **agree** that the agencies must ensure that the information they obtain is held on secure IT systems and that a range of internal compliance and audit mechanisms are in place,

including appropriate training for staff and processes to ensure that users only access the datasets when justified;

18. **agree** that the parties to a joint protocol must each publish a summary of the joint protocol on their websites once it is agreed and following the completion of each three yearly review (ensuring that the publication occurs in a manner compliant with requirements of security);

19. **agree** to bring all provisions in the Bill relating to access to the specified datasets into force the day after the Bill receives Royal Assent (including the provisions relating to joint protocols);

20. **note** that Cabinet has previously agreed to changes to the Customs and Excise Act 1996 that enable disclosure of information from Customs to organisations falling within the definition of 'department' in section 2 of the Public Finance Act 1989, which captures the GCSB and the NZSIS [EGI-15-MIN-0066 refers];

21. **agree** that the NZSIS and the GCSB are not able to use the disclosure framework in the new legislation replacing the Customs and Excise Act 1996, and that officials from those agencies and Customs work with the Parliamentary Counsel Office to determine how best to incorporate that exclusion into legislation;

Access on a case-by-case basis to restricted information

22. **agree** to give the agencies access to the following information about identified individuals or organisations by request on a case-by-case basis pursuant to a tier one or tier two warrant issued under the new legislation:

    22.1. tax information held by the Inland Revenue Department;

    22.2. driver licence photographs held by the New Zealand Transport Agency; and

    22.3. National Student Identification Numbers linked information;

23. **agree** that access to National Student Identification Numbers linked information should only be available for adults and young people in relation to tertiary education, not for children in the early education, primary or secondary schooling systems;

Ongoing work to clarify the application of the Privacy Act 1993

24. **note** that it may be desirable to include an empowering statement in the Bill expressly permitting the agencies to request other organisations to disclose information to them, with requests being limited to information necessary for the agencies to perform their functions;

25. **note** that there are outstanding questions about the ability of other organisations to disclose information on an ad hoc basis to the agencies in light of section 57 of the Privacy Act 1993, particularly where another legislative scheme relating to the disclosure of information exists;

26. **note** that it may be appropriate for the agencies to be subject to more information privacy principles under the Privacy Act 1993 than is currently the case, providing that

this could be done without prejudicing the security or defence of New Zealand, or the international relations of the government of New Zealand;

27. **direct** officials to provide advice (developed in consultation with the Privacy Commissioner) to the Minister for National Security and Intelligence, the Minister of Justice and the Minister Responsible for the GCSB and In Charge of the NZSIS/the Attorney-General by 13 May 2016 about:

    27.1. including an empowering statement in the Bill allowing the agencies to request other organisations to disclose information to them;

    27.2. options for clarifying the law around disclosure of information to the agencies; and

    27.3. whether to make the agencies subject to more information privacy principles than is currently the case, as well as options for doing so in a manner that is not prejudicial to the security or defence of New Zealand, or the international relations of the government of New Zealand;

28. **authorise** the Minister for National Security and Intelligence, the Minister of Justice and the Minister Responsible for the GCSB/In Charge of the NZSIS/the Attorney-General to take decisions following officials' advice on the matters in recommendation 27 and to authorise the issuing of drafting instructions in relation to any such decisions, as necessary;

Arrangements with foreign partners

29. **agree** to include a statement in the Bill expressly allowing the agencies to cooperate and share intelligence with foreign jurisdictions and international organisations, provided that such cooperation and sharing is consistent with the Bill's purposes and the agencies' obligations to act in accordance with New Zealand law;

30. **agree** that any future and multilateral arrangements relating to cooperation and sharing of intelligence entered into with foreign jurisdictions or international organisations should be referred to the Intelligence and Security Committee (ISC) for noting;

31. **note** that the Ministry of Foreign Affairs and Trade should be consulted on any proposal to enter into an arrangement with a foreign jurisdiction or international organisation relating to cooperation and sharing of intelligence;

32. **agree** that the Bill should require the agencies to formulate standard terms for ad hoc cooperation and intelligence sharing, which must be forwarded to the IGIS for comment and the final version referred to the ISC for noting;

33. **agree** that the Bill should include a statement that the responsible Minister should only authorise the sharing of intelligence and analysis with foreign jurisdictions or international organisations in accordance with New Zealand law and all human rights standards recognised by New Zealand law, except to the extent that they are, in relation to national security, modified by an enactment;

Incidentally obtained intelligence

34. **agree** that the Director of the GCSB/NZSIS should only be able to retain incidentally obtained intelligence where that intelligence is relevant to:

    34.1. preventing or detecting a serious crime

    34.2. preventing or avoiding the loss of human life on the high seas

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

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

35. **agree** that the Director of the GCSB/NZSIS should only be able to communicate intelligence falling within one of the categories outlined in recommendation 34 to:

    35.1. any employee of the New Zealand Police;

    35.2. any member of the New Zealand Defence Force;

    35.3. the Director of the GCSB or the NZSIS, whichever is relevant; or

    35.4. any public authority (whether in New Zealand or overseas) that the Director thinks fit to receive the information.

Access to an electronic copy of the electoral roll

36. **note** that the reviewers recommended that 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; and

37. **invite** the Minister for National Security and Intelligence and the Minister Responsible for the GCSB and In Charge of the NZSIS to refer the question of whether access by the agencies to access an electronic copy of the electoral roll would be appropriate, to the Justice and Electoral Select Committee once the Bill has been introduced, for consideration.

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