Privacy Commissioner
Te Mana Matapono Matatapu

Submission to the Foreign Affairs, Defence and Trade Committee on the New Zealand Intelligence and Security Bill 158-1

1 Key recommendations

1.1 My key recommendations are:

- Apply all of the privacy principles to the intelligence agencies (clause 264)
- The proposed use and disclosure exceptions to privacy principles 10 and 11 should explicitly protect the interests of national security (clause 263)
- Keep the positive definition of "national security" (clause 5) with clarification
- Clarify and strengthen provisions for accessing third party source information (Part 5)
- Strengthen the role of the Privacy Commissioner in oversight and monitoring of direct access to certain databases (Part 5)
- Intelligence warrants should specify whether the nature of activity authorised includes visual surveillance and/or electronic tracking (Part 4)
- Clarify the definition of "private communication" as the basis on which intelligence warrants are required to intercept communications (Part 4)
- Strengthen transparency by expanding the provisions for reporting agencies' activities.

2 Introduction

2.1 The Bill reflects recommendations I have provided previously to support the Hon Sir Michael Cullen and Dame Patsy Reddy's Report of the First Independent Review of Intelligence and Security in New Zealand (the Cullen Reddy review). I was also pleased to make recommendations to Ministers and to support the officials' team in its work to prepare the draft legislation.

2.2 I am pleased to further support the progress of this important legislation and to endorse the approach taken to modernise the regulation of New

Zealand intelligence and security agencies and align agency practice with modern standards for public sector governance and accountability.

2.3 The draft Bill reflects my previously expressed views that the revised legislation governing intelligence and security agencies should:

- be aligned more closely with the framework provided under the information privacy principles of section 6 of the Privacy Act 1993 to bring the practices of intelligence and security agencies in line with the expectations for other public sector bodies that have intelligence functions, subject to specific exceptions
- include explicit safeguards and procedures for privacy intrusive powers including both the warranted and warrantless collection of personal information; and
- strengthen oversight of international information sharing by the intelligence agencies.

2.4 I welcome the extent to which the Bill reflects these recommendations and the strengthening of the oversight provisions. In particular, the Bill reflects my view on the need to amend section 57 of the Privacy Act to provide that the privacy principles should apply more holistically to the intelligence and security agencies.

2.5 However, further improvements to the Bill are needed and there are a number of areas where I consider additional safeguards should be included to ensure the legislation provides adequate privacy safeguards consistent with national security imperatives. I note the aim of the Cullen Reddy report was to ensure that the activities of the intelligence agencies' are reasonable and involve no greater intrusion on individuals' privacy than is necessary and proportionate in the circumstances[1]. I endorse this aim and submit that a number of amendments to the Bill are necessary to fulfil this objective.

2.6 My recommendations aim to help ensure the resulting legislation addresses appropriately the principles of oversight and transparency that are fundamental to the objectives of this Bill. Given the size and complexity of the Bill, for ease of reference for the Committee my submission is structured as follows:

- A summary list of all recommendations

---

1 Report of the First Independent Review of Intelligence and Security in New Zealand Intelligence and Security in a Free Society (29 February 2016) (the "Cullen Reddy report") at [6.3].

- Key recommendations on the main areas of concern
- Important, but more technical comments, which are provided in summary form in the order these appear in the Bill.

3 Summary of Recommendations

Recommendation 1: I recommend that sub clause (g) of the definition of national security be clarified by adding a non-exhaustive list of examples of threats to international security. (paragraph 3.5)

Recommendation 2: I recommend that clause 61 (Matters required to be stated in intelligence warrants) require each intelligence warrant to state what type of surveillance is intended to be undertaken ie electronic surveillance, visual surveillance or both. (paragraph 4.3)

Recommendation 3: I recommend amending the Bill to include both purpose and length limitations in regard to visual surveillance powers. (paragraph 4.6)

Recommendation 4: I recommend that the definition of "private communication" should be amended to delete paragraph (b). (paragraph 4.11)

Recommendation 5: I recommend equivalent provisions to those contained in sections 4A and 4IB of the NZSIS Act, relating to privilege, could usefully be carried over into any new legislation arising from this Bill to provide clarity. (paragraph 4.20)

Recommendation 6: I recommend the Committee clarify whether 'incidentally obtained intelligence' (clause 91) is the same as 'unauthorised intelligence' as defined in Clause 83. (paragraph 4.21)

Recommendation 7: I recommend that section 23 (irrelevant records) of the GCSB Act be carried over into the Bill, to apply to both agencies. (paragraph 4.23)

Recommendation 8: I recommend that subpart 1 of Part 5 of the Bill be removed, or substantively amended. (paragraph 5.11)

Recommendation 9: I recommend that intelligence agency requests for third party information should be expressly covered by the authorisation framework proposed in Parts 4 and 7 of the Bill. (paragraph 5.12)

Recommendation 10: I recommend that requests for certain information types should be subject to tier 1 (or 2) authorisation where New Zealanders have a strong or particular expectation of privacy. (paragraph 5.17). In addition, any requests not specifically covered by tiers 1 or 2 should be subject to a tier 3 ministerial policy statement (paragraph 5.19)

Recommendation 11: I recommend including explicit statutory criteria for intelligence agency requests to third parties, such as those contained in clause 115. (paragraph 5.20)

Recommendation 12: I recommend the rationale for providing direct access to specified databases be carefully reviewed to ensure the provision of access is based on operational need of each intelligence agency. (paragraph 5.21)

Recommendation 13: I recommend additional statutory safeguards on subsequent and ongoing retention, use or disclosure of information obtained d through direct access to databases. (paragraph 5.23)

Recommendation 14: I recommend that clause 105 specify the matters to which the Privacy Commissioner should have regard when being consulted on direct access agreements. (paragraph 5.24)

Recommendation 15: I recommend that direct access agreements (clause 106) specify the process to be followed in the case of any breach of such an agreement, and the frequency of auditing. (paragraph 5.25)

Recommendation 16: I recommend the Bill include criteria for Ministerial reviews of direct access agreements, for example, to consider whether the agreement has operated in an unusual or unforeseen way. (paragraph 5.26)

Recommendation 17: I recommend that provision be made for Ministers to report on the results of their direct access agreement reviews to the Intelligence and Security Committee and ensure that any amendments to the agreement are made. (paragraph 5.27)

Recommendation 18: I recommend that the Bill be amended to ensure that the Privacy Commissioner is able to report to the Intelligence and Security Committee on any matters arising from the Commissioner's consultation roles. (paragraph 5.28)

Recommendation 19: I recommend that the purpose of access to each database be included in Schedule 2 as a third column. (paragraph 5.30)

Recommendation 20: I recommend that consultation on any amendment to Schedule 2 be expanded to include the Inspector-General, Privacy Commissioner and the relevant agency. (paragraph 5.31)

Recommendation 21: I recommend that clause 179 be amended to include annual reporting requirements on the number of permissions granted. (paragraph 5.33)

Recommendation 22: I recommend section 57 of the Privacy Act be repealed entirely. (paragraph 5.38)

Recommendation 23: I recommend that the Privacy Act exceptions proposed in the Bill (clause 263) be amended to state "to avoid a prejudice to 'national security'". (paragraph 5.42)

Recommendation 24: I recommend that, for consistency and to avoid any unwarranted confusion, the Privacy Act should be consequentially amended to clarify the alignment between the two definitions of intelligence and security agency. (Appendix 1, paragraph 6.3)

Recommendation 25: I recommend clause 16 be amended to specify that in order for the good faith immunity for intelligence and security staff to apply, staff should be required to have a reasonable belief that assistance is necessary in order to avoid prejudice to the ability of the agency receiving assistance to perform or exercise a function, duty or power directly related to the purposes or objectives of the Bill. (Appendix 1, paragraph 7.6)

Recommendation 26: I recommend that the Bill be amended to include the ability for the Commissioner to consult with the Inspector-General about any matters that come to his/her attention concerning the intelligence and security agencies. (Appendix 1, paragraph 9.3)

Recommendation 27: I recommend the Bill should be amended to provide that the prohibition on disclosure (clause 176) does not limit agencies who provide assistance to intelligence and security agencies from disclosing to their responsible Minister the fact that they have provided such assistance, and the nature of such assistance. (Appendix 1, paragraph 10.4)

Recommendation 28: I recommend that the Bill be amended to include a specific provision relating to the obligation of confidentiality on agencies supporting intelligence and security agencies (clause 177). (Appendix 1, paragraph 10.7)

Recommendation 29: I recommend the Bill be amended to ensure that the legislation does not introduce an absolute criminal offence that would effectively act as a barrier to transparency reporting (clause 177). (Appendix 1, paragraph 10.11)

Recommendation 30: I recommend there be an obligation on all agencies providing assistance to intelligence and security agencies to report annually, the number of requests received and/or actioned, and the requesting agency, unless the publication of such information would in itself undermine the objectives of the legislation. (Appendix 1, paragraph 10.13)

Recommendation 31: I recommend that the agencies be required to consult me before they enter into, or substantively modify any access information sharing agreement with the New Zealand Customs Service (Schedule 4). (Appendix 1, paragraph 12.2)

Key points

3.1 The Bill proposes a modern day framework for the mutual social objectives of privacy and security. I am pleased to see the Bill moves New Zealand beyond the debate about security OR privacy, and seeks a solution where all of the interests that are important to New Zealanders are recognised and respected. The Bill is an historic opportunity to ensure there is an appropriate system of thresholds, limits, checks and balances to ensure the privacy of individuals is respected and protected while intelligence and security agencies carry out their functions with public trust and confidence.

Definition of National Security

Definition of *National Security*

3.2 The Bill provides a definition of national security. The significance of the definition is that, to obtain certain intelligence warrants under Part 4, an intelligence agency has to satisfy the granter of the warrant that the activity sought to be authorised will contribute to the protection of national security. Aspects of this definition mirror those contained in the definition of security in the current New Zealand Security Intelligence Service Act.

3.3 I am aware that officials and Parliamentary Counsel[2] have proposed that the Act should not contain a definition of national security. Instead, what constitutes a threat to 'national security' would be determined by the Attorney-General and Commissioner of Intelligence Warrants on an ad hoc basis, "allowing it to be adaptive to an ever-changing security environment."[3]

3.4 I support the definition of national security contained in the Bill[4]. I propose an amendment to current sub clause (g) contained in the definition, which states "threats, or potential threats, to international security". In practice this could cover a vast range of things that the public would not consider to fall within the ambit of the intelligence agencies.

---

2 http://www.dpmc.govt.nz/defining-national-security
3 Ibid.
4 See the Privacy Commissioner's submission to the Law Commission's review of national security information in proceedings (8 July 2015) - noting that a generalised approach to defining "national security" can make it difficult to robustly verify that displacing normal rights and assumptions is justified, whereas the advantage of a more granular approach is that it means that the various interests deserving protection can be organised in a hierarchy with greater clarity about the circumstances in which national security "trumps" other interests.

3.5 I **recommend** that this be clarified by adding a non-exhaustive list of examples of threats to international security. This list should include, for example, specific activities such as terrorism or violent extremism, espionage, sabotage, and the proliferation of weapons of mass destruction, or specific obligations, such as international treaty obligations.

3.6 I note that the Global Principles on National Security and the Right to Information (Tshwane Principles), which were developed in conjunction with the United Nation's, include recommendations regarding definitions of national security. Principle 2 of this document states that national security should be defined precisely in national law[5].

3.7 The definition of national security is also relevant to my later comments on the scope of the proposed new exceptions to privacy principles 10 and 11. In my view, these exceptions should be based on avoiding prejudice to national security interests, rather than the functions-based approach that is proposed.

Clarify provisions for the proposed new warranting regime (Part 4)

4 Part 4 - **Authorisations** (clauses 46-96)

Subpart 1—Intelligence warrants

Types of intelligence warrants (clauses 50-52)

4.1 I support the greater clarity and transparency these provisions seek to provide. I am aware that the Inspector-General of Intelligence and Security has been consulted on these provisions and has made comments on this part of the Bill. I defer to her experience with these matters and have therefore refrained from detailed comments on this part of the Bill apart from the following specific comments.

Surveillance

4.2 Clause 63 states what authorised activities an intelligence agency may undertake under an intelligence warrant, including "conducting surveillance" (clause 63 (1)(a)). Surveillance is defined as visual surveillance and electronic tracking.

4.3 Given the intrusive nature of visual surveillance, I **recommend** that clause 61 (Matters required to be stated in intelligence warrants) require more specificity than "particular activity or activities authorised". It should instead require each intelligence warrant to state what type of surveillance

5 This is discussed in the context of restricting access to information using 'national security' justifications.

is intended to be undertaken ie electronic surveillance, visual surveillance or both. This would mean, in part, that decision makers have sufficient information on which to decide whether to impose conditions.

4.4 Under the NZSIS Act visual surveillance powers can only be exercised for counter-terrorism purposes, in accordance with legislative amendments brought under the Countering Terrorist Fighters Legislation Bill. During the debates on this Bill, the Hon. Chris Finlayson noted in regard to visual surveillance:

> "The warrants will be available only for the detection, investigation, or prevention of any actual, potential, or suspected terrorist act or facilitation of a terrorist act. I emphasise those phrases because the limitation was inserted by the select committee and, frankly, I think it is a very good limitation."[6]

4.5 David Shearer further noted:

> "We did not want this bill to be the back door by which the SIS was able to conduct surveillance more generally, so now in the bill it is confined to where there might be terrorist activities and, obviously, still on the basis of a warrant."[7]

4.6 The Intelligence and Security Bill, however, proposes extending the visual surveillance power to <u>all</u> purposes for which warrants can be sought, and also to the Government Communications Security Bureau. I think this is too wide. The power is intrusive and the bill proposes no limitations on this power either by length of warrant or the purpose of said warrant. I **recommend** amending the Bill to include both purpose and length limitations in regard to visual surveillance powers.

4.7 I note that the Committee needs to be satisfied that the extension of powers proposed under this Bill is not only necessary but also that the agency endowed with them has both the resources and the ability to exercise the powers effectively.

Purpose based warrant

4.8 Clause 64 allows for a 'purpose-based warrant' where it is not necessary for the applicant to state the persons or classes of persons to whom the warrant would apply. It is not clear why this provision is necessary. The

---

6 https://www.parliament.nz/en/pb/hansard-debates/rhr/document/51HansD_20141209_00000016/countering-terrorist-fighters-legislation-bill-second

7 https://www.parliament.nz/en/pb/hansard-debates/rhr/document/51HansD_20141125_00000016/countering-terrorist-fighters-legislation-bill-first

Cullen and Reddy report notes the example that a purpose based warrant would allow targeting to "enable interception of communications inside Islamic State ("ISIL")-controlled territory in Syria for the purpose of identifying New Zealanders who are fighting for or otherwise supporting ISIL"[8].

4.9 It appears that the persons falling within the example provided could be covered under the 'class based' warrant provided for in clause 51 (2)(c)(ii). I therefore suggest the Committee consider whether it is necessary to include clause 64.

Definition of private communication – threshold for warrant authorisation needs to be clarified

4.10 The definition of a "private communication" has a pivotal role as the threshold for when an interception warrant must be obtained in order for an intelligence agency to collect communications content and data.

4.11 I **recommend** that the definition of "private communication" should be amended to delete paragraph (b). Any communication objectively intended to be private (under paragraph (a)) should require a warrant for its interception. Paragraph (b) casts uncertainty on that basic premise by discounting any communication as "private" where it might potentially be intercepted.

4.12 The definition used in the Bill is outdated in the modern communications environment and its adoption in the intelligence context is problematic. It raises questions about which communications platforms can be relied on as secure, and those platforms that are commonly used but that may have vulnerabilities to interception in certain circumstances. For example, is the intent that communications over unencrypted platforms can be intercepted without a warrant because of the risk such platforms can be hacked?

4.13 Subject to the overriding objective assessment of whether the parties intended privacy (covered by paragraph (a)), communications platforms should be covered by the authorisation framework, rather than rationing the use of the warrant procedure based on the technical attributes of the communications platform.

4.14 This is consistent with the Cullen Reddy review that recommended putting in place clearer and more consistent protections for New Zealanders through the authorisation framework. The reviewers concluded that a

8 https://www.parliament.nz/resource/en-nz/51DBHOH_PAP68536_1/64eeb7436d6fd817fb382a2005988c74dabd21fe

definition of "private communication" would not be needed in the new legislation.

4.15 In my view, continuing to use the definition of "private communication" in the intelligence context is a missed opportunity to resolve the residual concerns about the lack of clarity about when a communication is protected as presumptively private and therefore requires a warrant authorisation to be intercepted or collected by the intelligence agencies.

4.16 In my view, this core definition should be amended to plainly state the circumstances in which the interception of private communications requires a warrant. This is necessary to improve public trust and confidence and assurance about the privacy protections that New Zealanders are entitled to, and to avoid any unintended chilling effect on freedom of expression.

4.17 I note that many submitters to the Cullen Reddy review did not consider intrusions on individuals' privacy by the state, for example through the interception of communications and metadata, to be justified.[9] While the reviewers accepted the case for surveillance powers, their objective was to provide the public with greater assurance by establishing a clearer, more comprehensive legislative framework with strong safeguards and oversight in place for all of the agencies intelligence and security activities.[10]

4.18 The modernisation of the definition of "private communication", and confirmation that a warrant authorisation is generally required for communications interception, is an important step in realising this objective.

Privileged communications

4.19 The provision for the protection of privileged communications under clause 67, is not as strong as the protections currently included in the NZSIS Act. Section 4A and 4IB of the NZSIS Act address the issue of intelligence warrants and visual surveillance warrants. Sections 4A(3)(d) and 4IB(3)(d) state that:

> "any communication sought to be intercepted or seized under the proposed warrant is not privileged in proceedings in a court of law under—(i) section 58 or 59 of the Evidence Act 2006; or (ii) any rule of law that confers privilege on communications of a professional nature between a lawyer and his or her client".

4.20 These sections confer a higher burden of proof on the NZSIS to ensure they are not collecting privileged material. I **recommend** equivalent provisions

9 Cullen Reddy report at [1.32].
10 Cullen Reddy report at [1.31].

could usefully be carried over into any new legislation arising from this Bill to provide clarity.

Subpart 3 - Incidentally-obtained intelligence (clause 91)

Retention

4.21 Clause 91 states that an intelligence agency may retain any 'incidentally obtained intelligence'. The Committee should clarify whether this is the same as 'unauthorised intelligence' as defined in Clause 83.

4.22 Clause 91 also does not include what is currently provided for under section 23 of the GCSB Act – that is irrelevant records. Section 23 of the GCSB imposes an obligation on the GCSB to destroy as soon as practicable after the interception, the communication, or any part of the communication, including any copies of it or records (whether written or otherwise), except in accordance with the permissions for retention under section 25 (which covers incidentally obtained intelligence).

4.23 The positive obligation contained in section 23 for the GSCB to destroy irrelevant records could usefully be carried over in any legislation resulting from this Bill – in line with the obligations contained in Principle 9 of the Privacy Act that an agency should not keep personal information for longer than necessary. I therefore recommend that section 23 be carried over into the Bill to apply to both agencies.

Clarify and strengthen procedures for accessing third party information (Part 5)

5 Part 5 - Accessing information held by other agencies (clauses 97- 118)

Subpart 1—Request and disclosure of information (clauses 99-101)

5.1 This part of the Bill is new and sets out provisions for the intelligence agencies to ask for information held by any person, including public and private sector agencies, and for those agencies to disclose to intelligence and security agencies the information sought.

5.2 Under existing law, there is no explicit authority for these requests. The intelligence agencies operate under the assumption that the authority to make information requests is implicit. I am not aware of any realistic challenge to this assumption however and I understand the intent of subpart 1 is to provide explicit legislative clarity that:

- the intelligence agencies may seek information from third party sources; and

- those agencies receiving requests from the intelligence agencies can respond to them.

It appears that the intent is to confirm that requests can relate to both personal and non-personal information.

5.3 Sub-part 1 provides that it's purpose is:

- To recognise the existing ability of the intelligence agencies to request information from third party sources (including public and private sector) (clause 99(a)(i))

- To recognise the existing ability of any agency receiving a request to disclose information in response (clause 99(a)(ii))

- Not to confer any legal right or obligation on an agency (clause 99(b)).

5.4 The two operative clauses then provide for intelligence agency requests (clause 100) and responses to those requests (clause 101).

Recommended repeal or substantial amendment of sub-part 1

5.5 It is my considered view that the approach taken in sub-part 1 is unnecessary and will add additional complexity. I **recommend** that sub-part 1 should be removed from the Bill, or substantially amended.

5.6 Sub-part 1 is unnecessary in light of:

- Other provisions of the Bill that clearly set out the functions, duties and powers of the intelligence agencies, such as the function of collecting and analysing intelligence; and

- the proposed reform to section 57 of the Privacy Act (clause 264) to bring agency disclosures to the intelligence agencies within the scope of the privacy principles.

5.7 The proposed application of the Privacy Act will affirm that agencies receiving requests can respond to them where the request falls within the relevant exception to the disclosure principle (IPP 11). The risk that a request from an intelligence agency could be considered ultra vires appears remote and therefore the policy rationale for including an explicit enabling provision does not appear to be strong. If it is to be included, it needs to clearly set out:

- the rights, responsibilities and authority of the intelligence agencies in making requests and

- the rights, responsibilities and authority of the agencies responding to such requests.

5.8 The approach proposed in the Bill will require an agency dealing with an intelligence agency request for information to navigate two Acts in formulating a response. The approach is unwieldy and adds unnecessary complexity to the process as the relationship between the two statutes is unclear in a number of respects..

5.9 I note the stated objective of promoting effective, clear and easy to understand legislation.[11] However, sub-part 1 does not meet this objective. It fails to clearly convey the voluntary nature of these requests for information and that agencies receiving a request have the discretion to refuse them.

5.10 Sub-part 1 mixes a general purpose of not conferring a legal right or obligation on an agency with a detailed list of overrides to disclosure. Overrides of the nature set out in clause 100(3) are generally needed where a disclosure is mandatory rather than voluntary. The result is a lack of clarity as to the intent and effect of the sub-part, or clear guidance for agencies responding to intelligence agency requests.

5.11 Overall, I am not persuaded that the provisions are needed and if retained they will need substantial amendments including:

- Explicitly confirming the voluntary nature of information requests made by the intelligence agencies;
- Explicitly confirming that the Privacy Act takes precedence over the Bill provisions in relation to personal information requests and disclosures. It is critical that the legislation clearly sign-post the application of the Privacy Act to intelligence agency requests for personal information;
- Explicitly confirming that where there is a specified procedure for gathering intelligence, that procedure should be used in preference to the requests power;
- Explicitly limiting the use of the request power by one intelligence agency to request information from the other intelligence agency and providing a form of specific authorisation and oversight for requests between the intelligence agencies;
- Explicitly confirming that the requests power is intended to apply to ad hoc requests for information rather than routine ongoing arrangements;[12]

11 Cabinet Paper One at [22.4].
12 See Cabinet Paper Five at [65] and fact sheet 13.

- Explicitly confirming whether or not any rights or obligations are conferred on the intelligence agencies (clause 99(b) indicates no right or obligation is intended to be conferred on an "agency" and whether this term includes an "intelligence agency"). If it's not intended to confer legal rights or obligations on an intelligence agency, this undermines the case for including sub-part 1. But if it is intended to confer legal rights and obligations on an intelligence agency then these need to be described.

- Amendments to the overrides to disclosure in clause 101(3) (if retained):

    - Clause 101(3)(a)(i) should read "imposes a prohibition or restriction in relation to the disclosure of information or regulates the manner in which personal information may be obtained or made available (for example, in relation to personal information, information privacy principle 11 in section 6 of the Privacy Act 1993);"

    - Clarifying clause 101(3)(b) as the intent of these provisions is unclear. For example, does it refer to contractual terms and conditions between a disclosing agency and its customers that restricts the agency's ability to comply with a request, or to information subject to commercial confidentiality or to some other kind of agreement or confidentiality obligation?

Bringing information requests within the authorisation framework

5.12 I **recommend** that intelligence agency requests for third party information should be expressly covered by the authorisation framework proposed in Parts 4 and 7 of the Bill. The gathering of intelligence from co-operating third parties is a form of surveillance that should attract additional oversight and authorisation.

5.13 This recommendation is consistent with the aim of the Cullen Reddy recommendations that the new legislation should establish a comprehensive and consistent authorisation regime that requires some form of authorisation for all of the intelligence agencies' intelligence collection and protective security activities that involve gathering information about individuals and organisations, proportionate to the level of intrusion involved.[13]

5.14 The Cullen Reddy review explicitly contemplated that tier 1 and 2 authorisations could permit the acquisition of information held by third

13 Cullen Reddy report at [6.27].

parties such as telecommunication companies, internet service providers, banks and government agencies.[14]

5.15 However the Bill provides the intelligence agencies with the choice of seeking an intelligence warrant to seize information or one or more classes of information, or to request the information on a voluntary basis. (The Bill does not contain a production order power that exists in the law enforcement context.)

5.16 Where a third party is willing to provide the information sought on a voluntary basis, the Bill does not require any prior specific authorisation for that request or subsequent collection of information. While it is proposed that the disclosure would be subject to the Privacy Act, this would not control or scrutinise the type or amount of information that could be disclosed or the frequency of requests, so long as the disclosure falls within the proposed disclosure exception and is considered necessary for the performance of any of the intelligence agency's functions.

5.17 I **recommend** that requests for certain information types should be subject to a tier 1 (or 2) authorisation where New Zealanders have a strong or particular expectation of privacy. For example, in my view, New Zealanders would expect that intelligence agency requests for banking, communications or health information, or information held by certain government agencies, would be subject to a warrant authorisation.

5.18 Although this approach would make compliance with the request compulsory on the part of the agency holding the information sought, rather than voluntary, in my view, the process protections of a warrant process provide greater assurance to the public than a negotiated process of request and release without explicit oversight.

5.19 In addition, any requests not specifically covered by tier 1 or tier 2 should be subject to tier 3. Cabinet Paper Two proposed that these requests would be subject to the tier 3 ministerial policy statement, including: [15]

- requests to telecommunications providers for communications data
- the provision of cyber security and information assurance services by consent
- requests for information from any other agency of the Crown and the private sector.

However, these activities are not currently included in the mandatory matters to be covered by ministerial policy statements in clauses 165 and

14 Cullen Reddy report at [6.45], [6.57].
15 Cabinet Paper Two at [100].

166 of the Bill. I recommend that this gap should be addressed so that the collection of personal information by voluntary request is verified as necessary and proportionate.

5.20 In addition, I **recommend** including explicit statutory criteria for intelligence agency requests to third parties such as those contained in clause 115, including:

- proportionality of the privacy impact and
- the lack of other available means of obtaining the information.

Subpart 2—Direct access to database information (clauses 102-109, Schedule 2)

5.21 I welcome the direct access agreement provisions in clauses 102-109 of the Bill. These new agreements provide for greater transparency and accountability than the current law. However I query whether a sufficient case has been made to provide direct access to each specified database to both intelligence agencies. Does the GCSB require access to these databases as well as the NZSIS? I **recommend** the rationale be carefully reviewed to ensure the provision of access is based on operational need.

5.22 It is important to note that the form of direct access proposed is not limited to one-time access but extends to the copying of the information (including by forensic techniques such as previewing and cloning). The definition of "access" in clause 97 means information can not only be searched, but also retained, re-used and re-checked by the intelligence agencies on an ongoing basis.

5.23 I therefore **recommend** additional statutory safeguards on subsequent and ongoing retention, use or disclosure of this information, in accordance with the principle that information collected for one purpose should not be used for another. (See also clauses 82 and 83 of the Bill, which limit the use unauthorised intelligence.)

5.24 I welcome the provisions for consultation on direct access agreements (clause 105). This could usefully be strengthened by the inclusion of more detail about the matters to which the Privacy Commissioner should have regard (such as the privacy implications of the proposed agreement). Cabinet Paper Five set out a number of matters the Privacy Commissioner would consider - these factors have not been included in the Bill. I **recommend** that at a minimum, the Privacy Commissioner should consider the privacy implications of the proposed agreement or any variation.

5.25 Clause 106 sets out the content of direct access agreements. I **recommend** the agreements also specify the process to be followed in the case of any breach of such an agreement, and the frequency of auditing (for example, annually).

5.26 Ministers are to review direct access agreements every three years and consult with the Inspector-General and the Privacy Commissioner (clause 108). I **recommend** the Bill include criteria for these reviews, for example, to consider whether the agreement has operated in an unusual or unforeseen way:

- has failed to facilitate the purpose to which it relates,
- impinges unreasonably on the privacy of individuals, or
- has operated in a manner such that the costs of access under the agreement outweigh the benefits.

(Section 96X of the Privacy Act provides a useful precedent.)

5.27 Further, I **recommend** that provision be made for Ministers to:

- report on the results of the review to the Intelligence and Security Committee; and
- ensure that any necessary amendments are made to the agreement to address any material issues arising from a review.

5.28 I also **recommend** the Bill be amended to ensure that I am able to report to the Intelligence and Security Committee any matters arising from my consultation roles in relation to the direct access agreements and their review.

Schedule 2

5.29 The databases that may be accessed are listed in Schedule 2 of the Bill, which may be amended by Order in Council on the recommendation of the Minister after consultation with the Intelligence and Security Committee.

5.30 I **recommend** that the purpose of access to each database, for example, identity or status verification or other data matching purpose, be included in Schedule 2 as a third column. I note that Cabinet Paper Five anticipated that an access agreement would specify the purpose of access.[16] This is consistent with comparable Schedule-based information access provisions such as Schedule 5 of the Privacy Act 1993, Schedule 4 of the Citizenship Act 1977 and Schedule 1A of the Births, Deaths, Marriages and Relationships Registration Act 1995.

5.31 I also **recommend** that consultation on any amendment to Schedule 2 be expanded to include the Inspector-General, the Privacy Commissioner and

16 Cabinet Paper Five at [40].

the relevant agency providing access to ensure the appropriate limitations can be identified.

5.32 In relation to clause 109 and the amendment of Schedule 2 by Order in Council, I note that Orders in Council made under Part 9A of the Privacy Act are expressly designated as a legislative and disallowable instrument for purposes of the Legislation Act 2012 (s 96M). I suggest that it may be worth similarly clarifying the status of Orders in Council under clause 109 of the Bill.

Subpart 3—Access to restricted information (clauses 110-118)

5.33 This part sets out the provisions for access to restricted information. To strengthen transparency of the operation of this part of the Bill, I **recommend** that clause 179 be amended to include annual reporting requirements on the number of permissions granted.

Clarify and strengthen amendments to the Privacy Act

Amendments to the Privacy Act— (clauses 262-264)

Reform of section 57 of the Privacy Act (clause 264)

5.34 I welcome the proposed reform of section 57 of the Privacy Act and the application of additional privacy principles to the intelligence agencies (principles 1, 4(a), 5, 8, 9, 10 and 11, in addition to principles 6, 7 and 12 that currently apply).

5.35 The Bill currently narrows the exemption of the agencies to only principles 2, 3 and 4(b). In my view, this is a considerable advance on the current law. Nevertheless, in my submission to the Cullen Reddy review, I recommended removing section 57 entirely and applying all of the privacy principles to the intelligence agencies, with appropriately tailored exceptions. I did so because I consider that the intelligence gathering nature of the work of these agencies was not unique, and could be accommodated within the flexibility of the Privacy Act framework.

5.36 Other public sector agencies frequently engage in intelligence gathering activities (including the Police, Customs and the New Zealand Defence Force), rely on human sources and are considered with activity that carries potential for serious harm to the nation or which have a strong interest in protecting sensitive channels of information from international sources (the Ministry of Foreign Affairs and Trade, New Zealand Customs, the New Zealand Defence Force or the Police, in particular).

5.37 These other agencies carry out their work within the general legislative framework and public sector accountability frameworks which the Bill proposes will now apply to the intelligence agencies. The evidence shows that it is possible to normalise the application of Privacy Act principles to a

wide diversity of agencies, including those with intelligence gathering functions. These agencies do not report difficulties in the application of principles 2, 3 and 4(b) in practice.

5.38 I therefore see no reason for section 57 to continue and believe that the intelligence agencies should be subject to the same Privacy Act obligations as other agencies (subject to tailored exceptions). I **recommend** section 57 be repealed entirely as no clear or compelling case has been made to continue the exemption.

5.39 In fact there is a strong case for the privacy principles to apply to the intelligence agencies, given the nature of their functions and powers. While it is accepted that the nature of intelligence gathering is inherently intrusive, the privacy principles (in particular principle 4(b)) serve to ensure that any intrusion is proportionate in the particular circumstances, rather than to prohibit intrusive surveillance per se.

5.40 Principle 4(b) provides that personal information shall not be collected by an agency:

> By means that, in the circumstances of the case –
>
> (i) are unfair; or
>
> (ii) intrude to an unreasonable extent upon the personal affairs of the individual concerned.

5.41 There is an internal balancing of interests within Principle 4(b), which provides that the collection must not be unfair or intrude unreasonably "in the circumstances of the case". This provides a practical means of taking into account the gravity of the particular matter under investigation, such as threats to national security. In considering whether any collection of personal information by means such as listening devices was unreasonably intrusive, the nature and gravity of the reason for collection would generally offer justification for the intrusion. However there will be outer limits that principle 4(b) usefully reinforces, for example, the collection of personal information for vetting purposes should not use means that are more intrusive than necessary for that particular function.

New intelligence related exceptions to privacy principles 10 and 11 (clause 263)

5.42 I **recommend** that Privacy Act exception proposed in the Bill be amended to provide that:

Principle 10(da)

> that the use of the information for that other purpose is necessary to avoid prejudice to "national security" (as defined in clause 5 of the New Zealand Intelligence and Security Bill)

Principle 11(fa)

> that the disclosure of the information is necessary to avoid prejudice to "national security" (as defined in clause 5 of the New Zealand Intelligence and Security Bill) .

5.43 The Bill currently proposes additional exceptions for privacy principles 10 and 11 and will allow use or disclosure where the agency that holds the information is satisfied that is "necessary to enable an intelligence and security agency to perform any of its statutory functions".

5.44 While I support adding a specific new "intelligence and security" exception, I consider the threshold proposed is the wrong approach. The exception should protect against prejudice to national security interests (as defined in clause 5 of the Bill) rather than being linked to performance of the agencies' functions generally. In my view, a functions based exception is too broad.

5.45 The current exceptions in the Privacy Act principles are generally set to a threshold of harm – either to an individual or the public at large – or for a specific public purpose. For example, Principle 10 imposes limits on the use of personal information obtained for one purpose being used for another unless doing otherwise "is necessary to avoid a prejudice to the maintenance of the law" or for "the enforcement of a law imposing a pecuniary penalty" or "to prevent or lessen a serious threat to public health or public safety".

5.46 These thresholds focus on the harm that is being avoided, or which may flow with adverse consequences, if the information is not used. Principle 11, which relates to disclosure of information, has similar thresholds.

5.47 In contrast, the proposed threshold in the Bill would allow any use or disclosure broadly necessary for the agencies' "functions", regardless of the strength of the national security interest. In my view, a better approach that is more consistent with the Privacy Act framework, and is appropriately targeted and proportionate, would be for the new exception to align with the harm based standard. Such an approach would also be simpler for agencies that are considering requests, than a standard which relates to various functions elsewhere in the Bill.

5.48 It should also be noted that with the proposed reform of section 57 and the application of more of the privacy principles to the intelligence agencies, other Principle 11 exceptions will become relevant to disclosures to and by the intelligence agencies including:

- Avoiding prejudice to the maintenance of the law;
- Preventing or lessening a serious threat to public health or safety;

- Preventing or lessening a serious threat to the life or health of an individual;

- The disclosure is directly related to the purpose for which it was obtained.

This means that there will be a range of justifications for disclosure available, in addition to the new disclosure exception.

EU adequacy considerations

5.49 It is important to note the international implications of New Zealand's domestic legislation relating to the intelligence agencies, including the privacy dimension. In particular, one consideration in designing the new intelligence-related exceptions to the privacy principles, is the potential impact on New Zealand's adequacy status.

5.50 New Zealand's privacy framework has been assessed as being adequate under European Union (EU) law. In 2012, the European Commission formally ruled that New Zealand's privacy laws provided adequate protection under European data protection standards. This is significant for New Zealand's trade relationship as it means that personal information can be sent to New Zealand from Europe without European companies having to take additional measures. Importantly, it removes the barrier to EU entities transacting business with New Zealand that involves the personal data of EU citizens.

5.51 Such findings of adequacy are rare and hard-won. Only 5 countries outside Europe have obtained this advantage.[17] The Privacy Commissioner provides periodic update reports to the European Commission on developments in New Zealand privacy law.[18] My concern is to ensure that New Zealand's adequacy finding is not put at risk of re-examination, in light of the international focus on intelligence agency access to personal data resulting from the Snowden leaks. [19]

---

17 Argentina, Canada, Israel, and Uruguay.
18 https://privacy.org.nz/blog/update-on-nzs-adequacy-under-the-eu-data-protection-directive/
19 Following the Snowden revelations, the European Parliament passed a resolution that included recommendations to review New Zealand and Canada's data adequacy findings in light of their participation in the five eyes programme. See also the recent Yahoo developments reported by Reuters "Yahoo email prompts European ire" (5 October 2016) http://www.reuters.com/article/us-yahoo-nsa-ireland; and in the New York Times "Yahoo said to have aided US Email Surveillance by Adapting Spam Filter" (5 October 2016) http://www.nytimes.com/2016/10/06/technology/yahoo-email-tech-companies-government-investigations.html.

5.52 Another relevant development is the Schrems decision in which the Court of Justice of the European Union declared the European Commission's 2000 Decision on EU-US Safe Harbour invalid.[20] In doing so, the Court noted that "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life."

5.53 The Court also found that nothing prevented data protection authorities from examining claims that questioned the EU's adequacy findings. The effect is that in the event of such a complaint, data protection authorities must now examine the adequacy decision of third countries - such as New Zealand - with 'all due diligence'.[21]

5.54 I therefore **recommend** further tailoring of the new exceptions to the privacy principles 10 and 11 as outlined above, to avoid the exceptions being interpreted as over-broad and open-ended with the result that New Zealand's EU adequacy status is put at risk.

Transparency

5.55 I support greater transparency, including reporting by the intelligence agencies on the use of their powers. While the trade-off between transparency and national security remains complex, there are ways such as reporting aggregated intelligence information in ways that allow the public to have greater insight into the extent and use of intelligence powers without harming national security. Where I see opportunities to strengthen the transparency provisions in the Bill I have included some suggested amendments in the appendix attached.

20 *Maximillian Schrems v Data Protection Commissioner,* case C-362/14 (October 2015).
21 See Brent Tuttle "On the adequacy of an adequacy decision post-Schrems" (1 June 2016) available at: https://iapp.org/news/a/on-the-adequacy-of-an-adequacy-decision-post-schrems/

Appendix 1 - Further recommendations for amendment to the Bill

6 Part 1 - Preliminary provisions (clauses 3-8)

Purpose of the Act

6.1 The purposes of the Act are framed generally and have broad application. This accords with the recommendations of the Cullen Reddy review and the approach of modernising accountability and transparency of the intelligence agencies. I note that clause 3(1)(c), which refers to ensuring the functions of the agencies are performed "in accordance with New Zealand law and all human rights obligations recognised by new Zealand law", includes the Privacy Act.

Definition of *intelligence and security agency*

6.2 Clause 4 of the Bill (Interpretation) defines an intelligence and security agency as meaning:

(a) the New Zealand Security Intelligence Service (NZSIS) and/or, the :

(b) the Government Communications Security Bureau (GCSB).

6.3 In contrast, section 2 of the Privacy Act defines these two agencies simply as "intelligence organisations". Currently, Schedule 4 of the Bill does not include a consequential amendment to address this inconsistency. I therefore **recommend** that, for consistency and to avoid any unwarranted confusion, the Privacy Act should be consequentially amended to clarify the alignment between the two definitions.

7 Part 2 - Intelligence and security agencies (clauses 9-23)

Objectives, Functions and Limits (clauses 11-23)

7.1 The Bill brings together existing provisions. The Bill purports to separate the two functions of the agencies by specifying, in clause 15, that the GCSB has specific functions in relation to information security. Clause 15 provides that in carrying out any activity to provide information assurance and cybersecurity activities, the GCSB does not require an authorisation under Part 4 of the Bill if the activity is lawful or undertaken with the consent of the public authority or agency in question.

7.2 This is a new provision and appears to apply where the GSCB has the consent of the relevant agency. Clause 15(4) provides that any information obtained in performing functions under the clause "may only be used in the performance or exercise of a function, duty or power under section 14 unless an authorised activity under Part 4."

7.3 I support that general limitation on the use of information for purposes outside those for which it was obtained, unless expressly authorised. (I note clause 17(2)(c) is also consistent with that approach,)

Clause 16 (Co-operation with other entities to facilitate their functions)

7.4 Clause 16 of the Bill provides that it is a function of intelligence and security agencies to cooperate with each other. The good faith immunity for intelligence and security officials in sub-clause 16(4) provides that an employee is immune from criminal liability for any act done for that section if "(a) the employee reasonably believed that the act was necessary to provide the assistance and (b) the act was carried out in a reasonable manner".

7.5 What constitutes 'a reasonable manner' would seem open to interpretation. There is also currently no defined threshold for necessity in terms of assessing the requirement for any assistance provided. I consider it would be helpful for agencies, and would provide greater assurance in the intended operation of the legislation, if it included a clearer threshold for when such immunity would attach to the actions of intelligence and security staff.

7.6 I **recommend** the provision be amended to specify that in order for the good faith immunity for intelligence and security staff to apply, staff should be required to have a reasonable belief that assistance is necessary in order to avoid prejudice to the ability of the agency receiving assistance to perform or exercise a function, duty or power directly related to the purposes or objectives of the Bill.

7.7 Such specifications would both meet an appropriate necessity test and would ensure the assistance provided was necessary to directly progress the aim of this legislation and not as a means to simply facilitate any wider and unrelated objectives of the assisting agencies.

8 Part 3 - Covert activities of intelligence and security agencies

Subpart 1 - Assumed identities (clauses 24-34)

Clause 29 (Assistance to acquire, use, and maintain assumed identity)

8.1 Clause 29 addresses the circumstances in which an agency may grant a request (received under clause 28) from an intelligence or security agency for assistance to acquire, use or maintain an assumed identity. Sub-clause 29(1)(b) requires the agency to be satisfied that "reasonable protections are or will be in place for the purpose of ensuring that, as far as practicable, the authorised person will use the assumed identity appropriately".

8.2 The Director-General must approve the use of assumed identities (clause 26) and must have regard to every relevant ministerial policy statement that has been issued that relates to the acquiring, use and maintenance of assumed identities (sub-clause 26(4)). Given these specifications, it is unclear where an agency receiving a request for assistance would have reasonable cause for believing a receiving agency subsequent use would be 'appropriate'.

8.3 However, if it is envisaged that an agency who is not satisfied the "reasonable protections" noted above are or will be in place may refuse to grant a request or action a direction, I consider it would be appropriate to explicitly specify that such a response can be taken if the decision to refuse to grant a request is made in good faith and with reasonable care.

Clause 32 (Restrictions on access to information about process for obtaining assistance etc)

8.4 Clause 32 provides that an agency must not permit any person to access a request made, a direction given, or any other information within its possession or control relating to the process for obtaining or giving the assistance or compliance with the direction.

8.5 While these provisions indicate a general obligation on agencies to provide security protections for information received or generated in this context, the current text does not clearly detail the objective of any such protection.

8.6 The Bill provides adequately for the protection of information relating to assumed identities held by the intelligence and security agencies. It does not include any explicit requirement for an issuing agency to ensure they themselves have provided reasonable protection in terms of the information they receive from an intelligence and security agency, or which they generate in the course of responding to an issuance direction or request.

8.7 Principle 5 of the Privacy Act will apply to both to intelligence and security agencies, and to any agency providing assistance and will require them to ensure that any information they hold is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss and unauthorised access, use, modification, or disclosure. However, for assurance, and for the avoidance of doubt, I consider it would be beneficial if the Bill was amended to stress that obligation. This could be achieved by inclusion of an explicit provision, or through a cross-reference to the Privacy Act.

Clause 34 (Immunity of authorised persons)

8.8 Sub-clause 34(1) provides that an authorised person is protected from civil and criminal liability, however it may arise, for any act that the authorised person does, or omits to do in good faith and with reasonable care.

8.9 I consider that prescribing a clear obligation on agencies to "take such steps as are reasonable", as recommended in the section above, would also help to define what actions or omissions might be considered 'reasonable' in terms of any determination of liability or immunity from liability.

9 Part 6 - Oversight of intelligence and security agencies (clauses 119)

Subpart 1 - Inspector-General of Intelligence and Security (clauses 120-153)

Appointment, functions and powers of Inspector-General (clauses 120-126)

Cooperation

9.1 Clause 124 carries over the provisions in the current Intelligence and Security Act allowing the Inspector-General to consult about any matter relating to his/her functions with the Privacy Commissioner and others (this could include consultation about complaints).

9.2 The current provision in the Privacy Act (Section 72B) allows for the Privacy Commissioner to consult with the Inspector-General regarding whether to refer, either in whole or in part, a complaint made to the Commissioner. However, Section 72B does not allow for a more general consultation such as in circumstances where the Commissioner has initiated an inquiry, or for consultation on a substantive rather than a specific issue.

9.3 As the Bill proposes to give the Privacy Commissioner a more substantive role in regard to the intelligence and security agencies, I **recommend** that the Bill be amended to include the ability for the Commissioner to consult with the Inspector-General about any matters that come to his/her attention concerning the intelligence and security agencies. Similar to the intention of the current complaints consultation provision, this more general consultation provision would help to ensure that there is no unnecessary duplication.

9.4 There may also be circumstances where either an inquiry or a complaint relates equally to the functions of the Commissioner and of the Inspector-General. I therefore propose that the Committee consider inclusion of a provision for joint inquiries.

10 Part 7 – Miscellaneous provisions

Security records (clauses 175-176)

10.1 Clause 176 (Disclosure of information relating to activities of intelligence and security agency) protects against disclosure of information relating to the activities of an intelligence and security agency.

10.2 Sub-clause 176(1) prevents disclosure by specified intelligence and security staff of information relating to the activities of an intelligence and security agency "other than in the performance of their functions or duties". Sub-clause 176(2) provides explicitly that the prohibition on disclosure does not limit the disclosure of information concerning the activities of an intelligence and security agency to the Minister responsible to the Minister responsible for that agency.

10.3 There does not appear to be any provision here or elsewhere in the Bill covering reporting of activities of other agencies that may undertake work to support the work of an intelligence and security agency (for example, agencies providing assistance in establishing or maintaining an assumed identity). In particular, the Bill does not appear to take account of the need for such agencies to report their activities to their respective responsible Ministers so as to comply with their accountability obligations. Nor does it address the public reporting of their activities for assurance and transparency purposes.

10.4 I **recommend** the Bill should be amended to provide that the prohibition on disclosure does not limit agencies who provide assistance to intelligence and security agencies from disclosing to their responsible Minister the fact that they have provided such assistance, and the nature of such assistance.

Confidentiality (clause 177)

10.5 Clause 177 (Duty of confidentiality) places an obligation of confidentiality on specified staff of intelligence and security agencies and makes it an offence to make a record of or use or disclose information that comes into their knowledge in the performance or exercise of their functions, duties or powers, unless authorised by a Minister responsible for an intelligence and security agencies.

10.6 As noted above, clause 32 requires that an agency receiving an assistance request or direction must not permit any person to access a request made, a direction given, or any other information within its possession or control relating to the process for obtaining or giving the assistance or compliance with the direction. However, the Bill does not contain any express obligation on staff of such agencies acting to assist an intelligence and security agency to maintain confidentiality equivalent to that applying to intelligence and security agency staff under clause 177.

10.7 I therefore **recommend** that the Bill be amended to include a specific provision relating to the obligation of confidentiality on agencies supporting intelligence and security agencies. Such a provision could provide a basis on which agencies would be able to take advantage of civil and criminal liability immunity, but should be designed to take into

account the recommendations made here regarding the need for transparency reporting.

10.8 'Transparency reporting' is public reporting by private sector agencies about the information requested by and disclosed to government agencies, usually for law enforcement or national security purposes. The benefits of transparency reporting include, not only increasing the visibility of information gathering by government agencies to increase consumer trust and help oversight bodies monitor trends in information gathering, but also to encourage companies to adopt good processes for handling requests, particularly those that are broad or ill-defined. Over the past several years, considerable work has been carried out internationally to increase transparency concerning the scale and scope of access to commercial data for law enforcement and national security purposes.

10.9 The key challenges for maximising the benefits of transparency reporting are comparability (how to compare transparency reports of different companies); and coverage (the scope of information covered by transparency reports and the number of companies producing them). In 2015 my Office conducted the first of what we hope will be regular surveys of agency responses to such requests to establish a benchmark against which we could evaluate both requesting and responding agency practice. Given the benefits of transparency reporting for individual privacy, I consider that it is important that agencies be continued to be able to provide information to inform this important accountability measure.

10.10 It should be possible to develop appropriate reporting bands so that the public can see the frequency of requests by the intelligence agencies and where they are directed, without creating an undue operational risk. This serves public trust, confidence and accountability.

10.11 I therefore **recommend** the Bill be amended to ensure that the legislation does not introduce an absolute criminal offence that would effectively act as a barrier to transparency reporting. Provision should be made to enable agencies to report aggregated data and activity summaries in a manner that supports transparency reporting while not prejudicing the work of the intelligence and security agencies concerned.

Security clearance information (clause 178)

10.12 Clause 178 (Use of Intelligence provided for security clearance assessment) prescribes the purposes for which information obtained by or disclosed to the New Zealand Security Intelligence Service for the purpose of a security clearance assessment may be used. The permitted uses specified under sub-clause (1) include the security assessment itself, any other security clearance assessment, and counter-intelligence (both terms being defined under sub-clause 178(3)).

10.13 Sub-clause 178(2) states that the prescribed limits apply despite anything in information privacy principle 10 in section 6 of the Privacy Act.

10.14 I consider the proposed over-ride of principle 10 of the Privacy Act appropriately confines the purposes for which such information can be used and I have no additional recommendations in this regard.

Annual reports (clause 179)

10.15 Clause 179 (Annual Reports of intelligence and security agencies) requires the Director-General of each intelligence and security agency to report annually on the activities of the agency during the year. However, the Bill does not explicitly refer to an obligation on agencies assisting intelligence and security agencies (for example, by issuing or maintaining assumed identities) to report on directions that may have been given or requests received in that regard. It is therefore not clear whether, and if so, how, this information can be reported by the other non-intelligence and security agencies.

10.16 I consider it would improve the transparency of the legislation's implementation and provide for greater public assurance if the Bill was amended to include a specific provision relating to the reporting of activities undertaken by other agencies in support of intelligence and security work. Such a provision could include a requirement that any such reports of activities taken to support intelligence and security agencies should be in a form that describes the quantum of requests, but does not disclose any information about the quality of such requests or directions that would prejudice the protections against disclosure provided for elsewhere in the Act (for example, as noted above in terms of clause 32 which protects against disclosure of information relating to the process for obtaining or giving the assistance or compliance with a direction).

10.17 For transparency, I **recommend** at least there should be an obligation on all agencies providing assistance to intelligence and security agencies to report annually, in their respective Annual Reports, the number of requests received and/or actioned, and the requesting agency, unless the publication of such information would in itself undermine the objectives of the legislation.

11 Part 8 - Repeals and amendments

11.1 Part 8 of the Bill includes a number of amendments to other legislation, some of which have implications for privacy in that they involve changes to the current provisions relating to the handling of personal information. Schedule 4 includes some additional consequential amendments to other legislation.

11.2 My comments relate to the proposed amendments to three of these Acts, namely: the Education Act 1989, the Immigration Act 2009, the Passports Act 1992, and the Privacy Act 1993, and the Customs and Excise Act 1996 and Tax Administration Act 1994.

Amendment to Education Act 1989 (clauses 209-210)

11.3 Part 30 of the Education Act authorises the use by authorised users of national student numbers (NSNs) for specific purposes, in order to facilitate the accurate use and transfer, by authorised users, of information relating to individual students.

11.4 Section 344 of the Act (Use of national student numbers) provides that the Secretary (the chief executive of the Ministry of Education) may authorise or require an authorised user to use national student numbers only for specific prescribed purposes. Section 346 of the Act (Offences) provides that an authorised user commits an offence, and is liable on conviction to a fine not exceeding $15,000, who uses or discloses a person's national student number otherwise than in accordance with the authorisations under section 344 that apply to that user.

11.5 Clause 210 amends section 346 to expand the exception on the restrictions on use of the NSN to include use or disclosure required under section 177 of the Act which requires agencies to provide the Director-General of an intelligence and security agency access to specified restricted information.

11.6 I consider this is a necessary and appropriately confined over-ride of the current restriction in the Act on the use of the NSN for non-prescribed purposes. The proposed amendment will enable the NSN to be used by intelligence and security agencies where it is necessary to support their functions, duties and powers.

Amendments to Passports Act 1992 (clauses 233-261)

11.7 Clauses 233-261: introduces a new section 27GA to the Passports Act 1992 which provides for the Minister to take action (including: to refuse to issue, recall, cancel, or retain New Zealand travel document on grounds of national or international security. To take such action they must have reasonable cause to believe the person is a danger to the security of New Zealand because the person intends to engage in, or facilitate a specified act (including, for example, undertake a terrorist act) and that:

- the person is a danger to the security of a country other than New Zealand
- the taking of that action will prevent or effectively impede the ability of the person to do either of the activities specified

- the danger to the security of that country cannot be effectively averted other than by taking an action specified.

11.8 I consider these are appropriately high-set thresholds and ensure that adverse action will only be taken in this context where it is a proportionate response to an identified risk. I further consider the requirement for the individual concerned to be notified and the options for Ministerial decisions to be reviewed (as provided for in the proposed new sections 27GC and 27GF) are necessary safeguards to ensure those affected by the new intrusive power are appropriate informed and have the opportunity to request a review of any such decision.

Amendment to Tax Administration Act 1994 (clauses 278-279)

11.9 Section 81 of the Tax Administration Act 1994 (Officers to maintain secrecy) requires that all Inland Revenue staff must maintain, and must assist in maintaining, the secrecy of all matters relating to the legislation described in subsection (1C) of that section, and the officer must not communicate any such matter, except for the purpose of carrying into effect that legislation or as otherwise provided for as explicit exclusions prescribed in the Act.

11.10 Clause 279 of the Bill amends section 81 to include an additional exception to the obligation of secrecy to allow the Director-General of an intelligence and security agency or an employee authorised by the Director-General for that purpose, to access information where permission to access restricted information has been granted in accordance with sections 113 or 114 of the NZSIS Act.

11.11 I consider the proposed amendment to section 81 is a necessary and appropriately constrained additional exclusion to the secrecy rules under section 81 that will enable Inland Revenue staff to disclose tax payer information to duly authorised intelligence and security agency staff where it is necessary to support their prescribed functions, duties and powers.

12 Schedule 4 - Consequential amendments

Amendments to the Customs and Excise Act 1996

12.1 The proposed new section 280M of the Customs and Excise Act 1996 provides for the Police to access information held by the New Zealand Customs. New section 280M(3) requires that before allowing access to a database in accordance with subsection 280M(2), the chief executive of New Zealand Customs must enter into a written agreement with the Commissioner of Police.

12.2 We consider this is a valuable control on access to the Customs-held information. However, for assurance and transparency, and to ensure any

such agreement appropriately addresses any potential privacy concerns, I **recommend** that the agencies be required to consult me before they enter into, or substantively modify any such agreement.

national law. (Categories of information whose withholding may be necessary to protect a legitimate national security interest are set forth in Principle 9.) A national security interest is not legitimate if its real purpose or primary impact is to protect an interest unrelated to national security, such as protection of government or officials from embarrassment or exposure of wrongdoing; concealment of information about human rights violations, any other violation of law, or the functioning of public institutions; strengthening or perpetuating a particular political interest, party, or ideology; or suppression of lawful protests.

"**National security**" is not defined in these Principles. Principle 2 includes a recommendation that "national security" should be defined precisely in national law, in a manner consistent with the needs of a democratic society.

"**Public authorities**" include all bodies within the executive, legislative, and judicial branches at all levels of government, constitutional and statutory authorities, including security sector authorities; and non-state bodies that are owned or controlled by government or that serve as agents of the government. "Public authorities" also include private or other entities that perform public functions or services or operate with substantial public funds or benefits, but only in regard to the performance of those functions, provision of services, or use of public funds or benefits.

"**Public personnel**" or "**public servant**" refers to current and former public employees, contractors, and sub-contractors of public authorities, including in the security sector. "Public personnel" or "public servant" also include persons employed by non-state bodies that are owned or controlled by the government or that serve as agents of the government; and employees of private or other entities that perform public functions or services or operate with substantial public funds or benefits, but only in regard to the performance of those functions, provision of services, or use of public funds or benefits.

"**Sanction**," when used as a noun, refers to any form of penalty or detriment, including criminal, civil and administrative measures. When used as a verb, "sanction" means to bring into effect such form of penalty or detriment.

"**Security sector**" is defined to encompass: (i) security providers, including but not limited to the armed forces, police and other law enforcement bodies, paramilitary forces, and intelligence and security services (both military and civilian); and (ii) all executive bodies, departments, and ministries responsible for the coordination, control, and oversight of security providers.

Public authorities also have an affirmative obligation to publish proactively certain information of public interest.

Principle 2: Application of these Principles

(a) These Principles apply to the exercise of the right of access to information as identified in Principle 1 where the government asserts or confirms that the release of such information could cause harm to national security.

(b) Given that national security is one of the weightiest public grounds for restricting information, when public authorities assert other public grounds for restricting access—including international relations, public order, public health and safety, law enforcement, future provision of free and open advice, effective policy formulation, and economic interests of the state—they must at least meet the standards for imposing restrictions on the right of access to information set forth in these Principles as relevant.

(c) It is good practice for national security, where used to limit the right to information, to be defined precisely in a country's legal framework in a manner consistent with a democratic society.

Principle 3: Requirements for Restricting the Right to Information on National Security Grounds

No restriction on the right to information on national security grounds may be imposed unless the government can demonstrate that: (1) the restriction (a) is prescribed by law and (b) is necessary in a democratic society (c) to protect a legitimate national security interest; and (2) the law provides for adequate safeguards against abuse, including prompt, full, accessible, and effective scrutiny of the validity of the restriction by an independent oversight authority and full review by the courts.

(a) *Prescribed by law.* The law must be accessible, unambiguous, drawn narrowly and with precision so as to enable individuals to understand what information may be withheld, what should be disclosed, and what actions concerning the information are subject to sanction.