OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

6 October 2016

Submission on the New Zealand Intelligence and Security Bill

To the Foreign Affairs, Defence and Trade Committee

1. This submission is from the Inspector-General of Intelligence and Security. I wish to appear before the committee with Ben Keith, Deputy Inspector-General of Intelligence and Security, to speak to my submission.

2. My interest is in whether the legislation:

   2.1. fully and clearly spells out the powers of the intelligence and security agencies, the purpose of those powers and the controls on them, including that they are sought and exercised proportionately and that any expansion of powers or removal of conditions is justified;

   2.2. includes necessary accountability and oversight mechanisms; and

   2.3. is otherwise consistent with fundamental rights and freedoms.

3. To that end, my comments follow. They primarily concern new provisions that seem overly broad, or lacking safeguards, and some provisions that are carried over from the current Acts but omit or weaken the conditions that apply. My understanding is that the Bill is intended to be no less stringent, and in parts stronger, in its governance of the significant powers conferred on the agencies.

4. My comments are set out, as far as possible, in the order in which the relevant clauses occur in the Bill. Matters relating to multiple clauses are covered first, followed by comments on specific clauses.

Authorisations (Part 4 of the Bill)

Ministerial role

5. As proposed in the report of the First Independent Review of Intelligence and Security[1] (the Review), the Bill would make the Attorney-General (with, at times, the Commissioner of Intelligence Warrants) responsible for authorising intelligence warrants (cl 53). While it is not specifically stated, that proposal may have been intended to emphasise the legal character of the warrant process and/or effect a separation between the Minister(s) responsible for the agencies and the warrant issuer.

---

[1] Hon Sir Michael Cullen and Dame Patsy Reddy *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand* (29 February 2016).

6. I suggest there are good reasons for warrant approvals to remain with the responsible Minister, whether or not that Minister is also the Attorney-General:

   6.1. First, the consideration of warrant applications is a very effective channel for keeping the responsible Minister apprised of the day-to-day business of the agencies.

   6.2. Second, ministerial authorisation of warrants has an important function in signalling executive responsibility and accountability for use of the unique powers of the agencies. I think that function is properly expressed in authorisation by the responsible Minister. It is also appropriate that the responsible Minister may, where appropriate, be subject to oversight and direction by the Prime Minister and/or Cabinet.

   6.3. The distinguishing characteristic of the post of Attorney-General is the law officer role. In my view that is not the key ministerial role in warranting: instead, the issuing Minister should look to his or her advisers and, where required, to the Attorney-General and Solicitor-General to ensure the lawfulness of his or her actions, particularly consistency with the Bill of Rights Act 1990. For the most sensitive class of warrants, a specific and independent legal review function is filled by the Commissioner.

Proportionality and necessity

7. The intelligence-gathering powers conferred by the Bill constitute the most extensive and potentially most intrusive powers available to any state agency. They are generally used covertly, potentially over a considerable period and without the subject ever being notified. Where the powers are used for covert intelligence-gathering regarding foreign governments, or otherwise have implications for foreign policy or international relations, they have significant implications for the national interest.

8. For those reasons the decision-makers who issue intelligence warrants must determine that every exercise of such powers is both necessary and proportionate. This is recognised in the Bill in cl 57, which states criteria for issuing a warrant including "the proposed activity is proportionate to the purpose for which it is to be carried out" (cl 57(b)) and "the purpose of the warrant cannot reasonably be achieved by less intrusive means" (cl 57(c)).

9. To assess proportionality and necessity, however, the decision-makers must be able to identify the particular information sought and satisfy themselves that:

   9.1. the proposed exercise of the warranted powers is necessary to seek particular intelligence;

   9.2. the consequences of that exercise, including the intrusion into the privacy of the intended subject(s) and any other party, and any risk to the national interest, are justified by the utility of the particular information sought; and

   9.3. the exercise of the warranted powers is subject to any restrictions, safeguards and other conditions required to ensure that the agency's actions and their consequences go no further than is necessary and justifiable.

10. The Bill does not provide for these requirements in comprehensive and clear terms, compared to the current Acts, other surveillance and interception warrant provisions in New Zealand law, or

intelligence and security legislation in other jurisdictions. Although the Bill does impose some similar obligations on the intelligence and security agencies, what is required is a clearer duty on the warrant issuers to consider and impose specific and effective safeguards.

Comparison with existing legislation

11. First, the proportionality test in cl 57(b) is expressed in much broader terms than the current legislation:

    11.1. The New Zealand Security Intelligence Service Act 1969 (NZSIS Act) requires that "the value of the information sought to be obtained under the proposed warrant justifies the particular interception or seizure or electronic tracking …" (s 4A(3)(b)); and

    11.2. The Government Communications Security Bureau Act 2003 (GCSB Act) requires that "the outcome sought to be achieved under the proposed interception or access justifies the particular interception or access" (s 15A(2)(b)).

12. Leaving aside the special case of "purpose" warrants (addressed separately below), the Bill does not indicate a reason for the removal of these important controls. In my view they should be retained, for several reasons:

    12.1. While I have found that some past warrant applications by the agencies did not meet these requirements,[2] better information is now generally provided in those applications. The agencies are evidently able to meet the current requirements.

    12.2. While the wording of cl 57 reflects the wording of part of the summary in the Review,[3] the Review does not propose a relaxation of current requirements but instead a "more explicit" proportionality requirement.[4]

    12.3. I understand from officials that the broad terms may have resulted from the inclusion within the authorisation regime of testing and training as additional purposes in cl 57(a)(ii) and (iii), which are not intelligence-gathering powers. However, the inclusion of those quite separate functions does not justify reduced controls for intelligence-gathering.

13. The lack of specificity in the Bill's test for proportionality, compared to existing and other comparable warrant provisions, means that the Minister and Commissioner will in some cases have little real ability to assess or control the steps to be taken. Public confidence requires specificity. The United Kingdom Investigatory Powers Bill, for example, requires an assessment of the proportionality of the particular conduct (not the overall surveillance, as in the Bill) against "what is sought to be achieved by that conduct" (cl 19(1)(b)). It also requires warrants to specify the steps to be taken, the bases for target identification and other detail (cl 29).

Use of the term "purpose" with different meanings

14. The use of the term "purpose" in subclauses 57(a), (b) and (c) may also introduce a risk of generality in warrant applications. As I read the Bill, subclause 57(a) delineates the overall scope

---

2 See, for example, my 2014/2015 Annual Report at 21.
3 At [41].
4 At 102.

of warranted activities, whose "purposes" must relate to the agencies' broadly expressed functions. Subclauses 57(b) and (c), however, are concerned with whether the proposed activity is proportionate and necessary to the particular objective – the "purpose", in a more specific sense – of the warrant. The use of the same term could however lead to the interpretation that a warrant could be granted on the very broad basis that it falls within an agency's statutory function in terms of cl 57(a)(i). I suggest this be avoided by revising the terminology in clauses 57(a)-(c).

Basis for a warrant application

15. Under both current Acts, and in line with other warrant provisions, the warrant applicant must state that there is, in his or her opinion, a basis for the warrant sought. Further, s 4A(2) of the NZSIS Act requires warrant applications to be supported by evidence under oath. The GCSB Act does not, perhaps because of its foreign intelligence focus and consequent lesser impact upon New Zealanders. The Bill requires neither a statement that there is a basis for the warrant sought, nor evidence under oath.

16. Requiring evidence under oath in support of a warrant application is proportionate in my view to the intrusiveness of the powers available to the agencies. It places a burden on the applicant (generally the Director of the agency) to advance a considered and supported belief that the powers sought under the warrant are necessary. It also emphasises the responsibility of the applicant for the content of the application and for the terms of the powers sought. For these reasons, provision of evidence under oath is a common statutory requirement for applications for warrants and other intrusive authorisations.[5]

17. The requirement for evidence under oath in support of applications for search warrants was removed from a large number of statutes by the Search and Surveillance Act 2012.[6] It was replaced by cross-reference to that Act's requirement for "a statement by the applicant confirming the truth and accuracy of the contents of the application,"[7] with a corresponding offence of making a false application.[8] This followed a Law Commission recommendation.[9] The Commission argued that requiring evidence on oath emphasised the solemnity of the occasion and created the potential for criminal liability – but that these could also be achieved by a statement (not on oath) at the end of an application "confirming the applicant's belief in the truth and accuracy of its contents and acknowledging the consequences of knowingly making a false statement".[10] This should be accompanied by a specific offence for making a statement that would amount to perjury if made in judicial proceedings.[11]

---

5 See for example: Bail Act 200 s 37(1); Criminal Investigations (Bodily Samples) Act 1995 ss 13(2), 18(2), 45(4); Children, Young Persons, and Their Families Act 1989 s 296C(2); Misuse of Drugs Amendment Act 1978 ss 13E(1) and (2); Transport Accident Investigation Commission Act 1990 s 12(2); Serious Fraud Office Act 1990 ss 6(1) and 10(1); Customs and Excise Act 1996 s 38J(2); Coroners Act 2006 s 122(1) and (2), s 128(1); Immigration Act 2009 ss 289(1) and (2), 316(2), 317A(2)(a), 317C(2)(a), 323(4)(a), 324A(3)(a).

6 Search and Surveillance Act 2012, Part 5.

7 Section 99.

8 Section 175.

9 Law Commission *Search and Surveillance Powers* (NZLC R97, 2007) Recommendation 4.11 at 59.

10 At [4.47].

11 At [4.48].

18. In my view the Bill should require evidence under oath in support of an application for an intelligence warrant. I have considered the alternative of requiring a statement of truth and accuracy backed up by a specific offence of knowingly making a false statement. I do not however think it is adequate. I do not see any reason why the intelligence and security agencies, when seeking to exercise intrusive powers, should be subject to lesser requirements than agencies seeking to exercise similar or lesser powers. If anything there should be a higher level of formal rigour.

19. Adopting this approach would extend to the GCSB the obligation to provide evidence under oath. In my view that is no less appropriate than it is for the NZSIS, as the GCSB's powers are no less intrusive.

Purpose-based warrants

20. Clause 64 provides for the issue of "purpose-based" warrants. These would not specify persons or places as targets, only the type of information sought and the purposes for which it is required. This new power was recommended by the Review, subject to a presumption that it could be used only where the objective could not be achieved by a targeted authorisation.[12]

21. One precedent cited by the Review is the proposal for purpose-based warrants in the United Kingdom draft Investigatory Powers Bill. That proposal, however, is directed at what the Bill terms "bulk interception", which is limited to "overseas-related communications" and subject to additional and detailed safeguards.[13] The New Zealand Bill as introduced does not contain a "bulk interception" regime.

22. The Review also gave two examples of situations in which purpose-based warrants would be desirable. The first was that:

> "An interception authorisation might, for example, enable interception of communications inside Islamic State ("ISIL")-controlled territory in Syria for the purpose of identifying New Zealanders who are fighting for or otherwise supporting ISIL.
>
> We consider the ability to obtain purpose-based authorisations is necessary to enable the Agencies to perform their functions effectively, particularly at the stage of identifying initial leads for further investigation. At this early stage, the Agencies often will not have sufficient information to identify a specific person as a target ..."[14]

The second was that:

> "Purpose-based authorisations will also make it easier for the Agencies to be sufficiently responsive when leads are received at short notice. For example, the NZSIS may be informed a foreign intelligence officer is intending to travel to New Zealand the day before he or she arrives. Under the current arrangements, the NZSIS must obtain a new warrant each time this occurs. The time delay in obtaining a warrant and then

---

12 Recommendation 59.
13 See cls 130 & 134.
14 At [6.58]-[6.59].

> setting up a surveillance operation means the NZSIS may not always be able to respond in these types of situations. Under the new framework we are proposing, the NZSIS could have a purpose-based tier 2 authorisation already in place that would allow it to commence surveillance of foreign intelligence officers immediately on arrival."[15]

23. In my view the first situation – a need to identify New Zealanders seeking to join ISIL – could be dealt with by a warrant directed at that class of individuals, as provided for in cl 63(1)(a)(i). While such a warrant might, in practical terms, involve the collection and filtering of substantial volumes of communications to identify those people, that exercise can be considered and, if necessary, authorised by the warrant issuers and subjected to appropriate safeguards.

24. The second situation – conducting surveillance on a foreign intelligence agent – could also be met through a specific warrant, supplemented in urgent cases through the exercise of the proposed urgency powers provided in cls 70 and 77.

25. I do not therefore see a basis for this new power. Justifying it requires both an important practical need and a cogent explanation of why the need cannot be otherwise met. The examples given do not establish that need. The second example also indicates the potential deficiency of such a warrant: under a specific warrant, the warrant issuer(s) would consider whether there was a need to conduct surveillance of each officer, the means by which that could occur and the conditions to apply and, further, would do so in consultation with the Minister of Foreign Affairs. Under a purpose-based warrant, there would be no specific external consideration or consultation. It would be left to the responsible agency to decide whether and how to conduct surveillance, including assessing any foreign policy implications.

26. Nor does the Bill provide for the proposed power to be appropriately controlled and overseen. The key difficulty of purpose-based warrants is that the extent of any exercise of intrusive powers and the targeting of particular subjects would be left to the agency to determine. The external assessment of proportionality and the external authorisation of particular steps and safeguards would be lost.

27. If an alternative and sufficient justification for purpose warrants can be identified and they are retained in the Bill, the need for robust reasoning in warrant applications will be especially acute. Cabinet paper 2 suggests that a critical check on the issue of a purpose-based warrant will be the need for the applicant agency to demonstrate that a targeted warrant is unsuitable.[16] I do not see this requirement for a demonstrated case clearly reflected in the Bill. Subclauses 64(2)(a) and (b) require the Attorney-General and Commissioner to be satisfied that the objectives of the warrant cannot be accomplished by a targeted warrant. This emphasises the reasoning of the decision-makers rather than the duties of the applicant for the warrant. To promote robust arguments for purpose-based warrants, the Bill would need to demand expressly that the agencies demonstrate that a targeted warrant could not deliver the outcome sought. The argument above for retaining an obligation to provide evidence under oath in support of an application would also apply with particular force to any provision for purpose-based warrants.

---

15 At [6.65].
16 At [63]-[64].

Privileged information

28. Clause 67 says a warrant "may not authorise the carrying out of any activity …. for the purpose of obtaining privileged communications." Currently the NZSIS Act (s 4A(3)(d)) and the GCSB Act (s 15C) provide (in slightly different terms) that no warrant is to be sought for the purpose of intercepting privileged communications. In my view the risk of capture of privileged material has to be addressed in a warrant application, so the decision-makers can impose relevant conditions if necessary, not only in the duties of the agencies when performing warranted activities. I think the Bill should require the agencies to identify all practicable steps that are reasonable in the circumstances to minimise the likelihood of collecting privileged information. Where the risk exists, mitigation measures should be proposed.

Impact on third parties

29. The GCSB Act (s 24) and the NZSIS Act (s 4F) impose a duty on the agencies to take all reasonable practicable steps to minimise the likelihood of intercepting third party communications. In addition the NZSIS Act requires the Minister and Commissioner to consider whether to include conditions in a warrant to minimise the risk of impact on third parties (s 4B(4)). Third party safeguards are also addressed in the GCSB Act through the requirement that the Minister and Commissioner must be satisfied of safeguards on authorised activity (s 15A(2)(d)-(e)). As with the existing requirements for proportionality and necessity, my experience is that these provisions have not always meant that warrant applications contain adequate detail on possible third party impacts and mitigation.

30. Clause 82 of the Bill seems to be intended to cover similar ground to the provisions in the NZSIS and GCSB Acts cited above, but it appears to me to be narrower. Clause 82 requires the agencies to take all reasonable and practicable steps to minimise the likelihood of "collecting intelligence outside the scope of the authorised activity". Because not all communications constitute intelligence, this seems a more limited duty than the GCSB's current obligation to minimise the likelihood of intercepting third party communications. Similarly NZSIS activities may have impacts on third parties that are not captured by the description "collecting intelligence". This does not appear to be a policy decision, from my reading of the Cabinet papers. If it is unintended I would like to see clause 82 redrafted to at least retain the duties arising from the current legislation.

31. I would also like to see the minimisation of impacts on third parties more clearly expressed as a criterion for issuing an authorisation. Current legislation requires the agencies and warrant issuers to consider possible impacts on third parties before an authorisation is issued. Clause 82, however, expresses a duty that arises when an agency is "carrying out an authorised activity" – ie after the authorisation is issued. The Bill is less clear than current law on the agencies' duty, when applying for an authorisation, to evaluate the likelihood of effects on third parties so that the Minister and Commissioner can decide whether conditions on the warrant are necessary. Clauses 57(b) and (c) require that the proposed activity is proportionate and necessary, while clause 57(d) requires that "there are satisfactory arrangements in place to ensure that nothing will be done in reliance on the warrant beyond what is necessary and reasonable ...". These *could* encompass consideration of effects on third parties, as could the provision in clause 60 for a warrant to include restrictions or conditions "in the public interest". However I think it desirable that the Bill is more specific in imposing a duty on the agencies, when seeking authorisations, to

set out what reasonable and practicable steps can be taken to minimise impacts on third parties – and a duty on the decision-makers to consider what conditions they should impose for that purpose. The relevant clauses could include 57, 60 and 61.

Permissions to access restricted information

32. Clause 113 provides for the Attorney-General and Commissioner to permit access to restricted information (which is defined in clause 111). These permissions therefore follow a similar approval process to warrants, but do not appear to be subject to review by the Inspector-General of Intelligence and Security (the Inspector-General) in the same way, as they are not "authorisations" under clause 121(3). I do not see any reason for this and think it would be helpful to clarify that such permissions are subject to review by the Inspector-General.

Data retention and deletion

33. Clause 74 requires all information collected under an urgent warrant (issued under cl 69 or cl 70) to be destroyed as soon as practicable if the warrant is revoked. Clause 80 states the same requirement for all information collected under a very urgent authorisation (issued under cl 77). There is however no comparable requirement for information collected under the other forms of authorisation provided for in the Bill: a Type 1 or Type 2 intelligence warrant (cls 55 and 56) or a purpose-based warrant (cl 64). I think there should be.

34. Clause 83 requires that "intelligence" (rather than "all information") that is unintentionally collected must be destroyed unless its collection is retrospectively warrantable (under cl 83(3)) or it can be disclosed to Police or other authorities to prevent or detect crime etc (under cl 91). There is however no timeframe specified for destruction, in contrast to cls 74 and 80. I do not see why the requirement to destroy "as soon as practicable" should not apply here also. Additionally, as with clause 82 (see earlier comment in paragraph 29 above) the scope of the term "intelligence" in cl 83 is not entirely clear. I think it would be helpful for the Bill to refer consistently to "information".

35. A Type 1 or Type 2 warrant can be issued for the purposes of testing, maintaining or developing the capabilities of an intelligence and security agency, or training its employees.[17] Where information is collected under warrants for those purposes there is no justification for retaining it. It would not necessarily be covered, however, by a requirement to destroy unintentionally collected material. I think there should be an express requirement for the destruction of such information as soon as practicable after collection.

36. I suggest the Bill should also require the agencies to identify and destroy material that, although legitimately collected, is or has become irrelevant. This would retain the existing obligations of the agencies under the NZSIS Act (s 4G) and the GCSB Act (s 23). Comparable requirements can found in cls 51, 121 and 140 of the UK Investigatory Powers Bill.

---

[17] Clause 57(a)(ii) and (iii).

Ministerial Policy Statements

37. The Bill would make the issue of a Ministerial Policy Statement (MPS) mandatory for the processes of authorising and acquiring an assumed identity and creating a legal entity (cl 165) and for cooperation and intelligence sharing with "overseas public authorities" (cl 166). Any other MPS is discretionary (cl 167).

38. This appears to be a significant reduction in the coverage of MPSs compared to that anticipated in Cabinet paper 2, which proposed eight topics to be covered by them: surveillance in a public place; obtaining and using publicly available information; requests to telecommunications providers for communications data; provision of cyber security and information assurance services by consent; use of cover as a means to support intelligence collection or obfuscate activities; information sharing with foreign partners; requests for information from any other agency of the Crown and the private sector; and lawful human intelligence collection.[18]

39. It is not clear to me why, in contrast to the emphasis in the Cabinet papers on the role of MPS as a regulatory mechanism, the Bill does not require or at least indicate the desirability of a greater range of MPSs. The absence from the Bill of any requirement for an MPS on cyber security and information assurance services by consent, for example, would mean that CORTEX (and related but non-CORTEX) activities would not necessarily be subject to MPS guidance. I agree with the arguments in the Cabinet papers that MPSs would be an important component of the proposed new regime. They have the potential to enhance oversight and compliance by improving transparency in the agencies' exercise of their lawful powers.

40. The requirements for compliance with MPSs also seem unusually low, considering the emphasis in Cabinet papers on the statements as a control mechanism. Subclause 26(4) requires the agencies only to "have regard" to the relevant Ministerial Policy Statement (MPS) when dealing with assumed identities and related false documents. There appears to be no comparable direction at all in relation to the MPS required by clause 166 for cooperation with overseas public authorities. By contrast, Cabinet paper 2 describes the MPS as "a mechanism to enable the responsible Minister to regulate the lawful activities of the agencies."[19] In my view the Bill should require the agencies to act consistently with a relevant MPS, or some such wording.

41. There is no express provision in the Bill for the Inspector-General to review the activity of an agency under an MPS. The Inspector-General can review the issue of an authorisation and the carrying out of an activity under an authorisation (cl 121(1)(h)(i) and (ii)). In doing so I could (and would) take into account any relevant MPS. I could also potentially review activities governed by an MPS under the power to conduct an own motion inquiry into the propriety of a particular activity (cl 121 (1)(d)) and/or the powers to review and conduct yearly procedural and compliance reviews (cl 121 (1)(f)) and/or unscheduled audits of operational activity (cl 121 (1)(g)). Again however, given the apparent policy intention for MPS to have a significant place in the governance of the agencies, I suggest an express review function for the Inspector-General is probably appropriate.

---

18 At [100].
19 At [99].

42. Subclause 166(2) requires the Minister to provide the Intelligence and Security Committee with a copy of the mandatory MPS on cooperation and intelligence sharing with overseas public authorities. There is no corresponding requirement however regarding the mandatory MPS relating to covert activities. The committee would seem to have a legitimate interest in receiving a copy of any MPS. I suggest also that there should be a requirement to provide my office with a copy of any MPS issued.

Disruptive activities

43. It is not clear how the Bill is intended to address disruptive activities by the intelligence agencies, including counter-intelligence operations, warnings and "effects operations" (including, for example, some computer network exploitation operations). Clause 19 excludes enforcement from the agencies' functions, replicating s 4(2) of the NZSIS Act and extending the prohibition to the GSCB. The definition in subclause 14(2) of "protective security services, advice and assistance", as one of the functions of the agencies, does not clearly encompass counter-intelligence. Considering these provisions the Bill might be construed as prohibiting disruptive activities. If that is not the intent – if it is envisaged that some such activities falling short of "enforcement" will be permissible – the legislation could usefully clarify this. It might be appropriate to provide for a Ministerial Policy Statement in this area.

Comments on specific clauses

44. **Clause 12**: Subclause 12(1)(d) requires the agencies to act "in a manner that facilitates effective democratic oversight". Cl 12(2) then provides that subclause (1) "does not impose particular duties" on the agencies. One of the most important ways in which the agencies can act in a manner that facilitates effective democratic oversight is by keeping comprehensive and timely records of their actions. There is currently no general statement in the Bill of a duty to keep such records. I suggest one could be included here, by way of a subclause stating an exception to 12(2). This could be structured similarly to 12(3), with a cross reference to (12)(1)(d).

45. **Clause 17:** The scope and anticipated effect of this clause are unclear. It empowers the agencies to cooperate with "any entity" dealing with an "imminent threat" to the life and safety of a New Zealander, here or overseas, or a threat to the life and safety of anyone for whom New Zealand has search and rescue responsibilities (cl 17(1)). In these circumstances an agency may do things that otherwise could not be authorised "in any circumstance" by an intelligence warrant (cl 17(2)(b)). Performing this function might "involve the exercise of powers or the sharing of capabilities that the agency is not, or could not be, authorised to exercise or share in the performance of its other functions" (cl 17(2)(d)).

46. In effect, this appears to add a non-intelligence or security function to the functions of the agencies. On its terms, the drafting suggests that the agencies may act in any way they can, above and beyond their significant powers, including emergency powers, and without external authorisation. It is difficult to see a rationale for that. It would be constructive to identify the intended objective and then review whether cl 17 is still required or can be more narrowly drafted.

47. Clause 17(3) provides that any action by the agencies under cl 17 is subject to Inspector-General oversight. That would be more effective if the Bill expressly required the agencies to notify the

Inspector-General when action was taken under cl 17. As this clause is apparently intended to enable action in rare circumstances, a notification requirement would not seem burdensome.

48. **Clauses 19-23:** These clauses cover fundamental principles underpinning the definition and performance of the agencies' functions. As such, in my view, they should be moved up in the Bill to follow clause 12. This would create a coherent group of "Principles" clauses, which could be followed by a "Functions" group beginning with cl 13.

49. **Clause 22:** Subclause 22(2) states that lawful advocacy, protest, or dissent "… does not of itself, justify an intelligence and security agency *collecting intelligence* on any person …" (my emphasis). This compares to s 2(2) of the NZSIS Act 1969, which states that exercising the right to lawful advocacy, protest, or dissent "does not, of itself, justify the Security Intelligence Service in *instituting surveillance* of any person …" (again, my emphasis). To the extent that "collecting intelligence" could be construed as collection under an intelligence warrant, while "instituting surveillance" could encompass observation undertaken legally without a warrant, the Bill can be read as proscribing a narrower range of action than the current legislation. In my view however, lawful advocacy, protest or dissent do not in themselves justify the agencies taking any action at all. I suggest the clause be reworded to this effect.

50. **Clause 47:** "Private communication" is defined in clause 47 in substantially similar terms to the current definition in s 4 GCSB Act: "… a communication made under circumstances that may reasonably be taken to indicate that any party to the communication desires it to be confined to the parties to the communication". The definition is relevant to cls 63 and 64, which refer to a warrant authorising, among other things, "intercepting any private communications". I think the definition in the relevant Canadian legislation is clearer: "[any communication] … that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it …".[20]

51. **Clause 63(1)(g):** This provision proposes that a warrant may authorise human intelligence activity that amounts to an unlawful act short of violence, threat of violence or perversion of the course of justice. The Cabinet papers suggest that this provision is necessary, for example, to enable an intelligence agent to join a prohibited terrorist group for intelligence purposes. However, that and similar examples are served by the concealment power in cl 65(1)(k) or other ancillary provisions. There is no obvious basis for the very broad terms of this new proposed power.

52. **Clause 77:** This clause provides for the issue of "very urgent authorisations" by the Director-General of an intelligence and security agency, but contains no criteria on which the Director may issue an authorisation. In my view there should be a reference back to the criteria the Attorney-General and Commissioner must apply under cls 55 -57.

53. **Clause 137:** This clause expands the grounds on which the Inspector-General may decline to inquire into a complaint, or continue an inquiry. It follows a Cabinet decision that the current grounds should be amended to reflect the approach taken in section 17 of the Ombudsmen Act 1975.[21] However the Bill adopts the approach in a previous iteration of that section, not the current provision. As a result the possible reasons for deciding not to inquire (under cl 137(1)) do

---

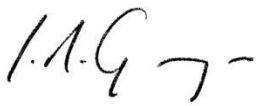
[20] National Defence Act RSC 1985 c. N-5, s 273.61, adopting s 183 of the Criminal Code 1985.

[21] Cabinet paper 4, recommendation 34.

not include that an inquiry is “unnecessary”, as is currently provided for in the Ombudsmen Act. I would prefer that the current wording of the Ombudsmen Act was followed.

54. **Cls 213-214:** These clauses amend the Employment Relations Act 2000. They would add a new section to that Act requiring the Employment Relations Authority, if dealing with a matter concerning an NZSIS recommendation regarding a person’s security clearance, to request a report from the Inspector-General to inform its proceedings. The Inspector-General would have to provide a report on request. Although I have reviewed the relevant background material in Cabinet paper 4, I remain unsure of the problem this proposal is meant to address. It is also unclear to me how the jurisdictions of the Authority and my Office are expected to interact. The proposal touches on an underlying question of how findings from my inquiries are to be treated by courts, and on practical problems faced by courts in dealing with classified material. I am happy to address specific aspects of this when appearing before the Committee, or by supplementary written submission if that would assist.

Thank you for your consideration.



Cheryl Gwyn
Inspector-General of Intelligence and Security