This paper has been redacted for public release.

Office of the Minister Responsible for GCSB

Cabinet Domestic and External Security Committee

REVIEW OF GOVERNMENT COMMUNICATIONS SECURITY BUREAU ACT 2003: PAPER 2

Proposal

1. To seek Cabinet approval to amend the Government Communications Security Bureau Act 2003 (the Act) to improve the legislative framework, enabling the Bureau to perform its functions effectively and efficiently with enhanced authorisation processes and controls.

Executive Summary

2. The Government Communications Security Bureau (GCSB) performs three core functions in contributing to the protection of New Zealand's security and interests. First, It has a key role to play in the cyber security domain. It hosts New Zealand's National Cyber Security Centre, and Cabinet has indicated its expectation that the Bureau will considerably enhance its cyber security capabilities to assist a range of organisations (government, state sector, critical infrastructure providers and key economic contributors). The purpose of this assistance is to protect information and ICT networks and infrastructure from cyber threats.

3. Second, the Bureau's foreign intelligence function contributes to informed government decision-making through generating intelligence about the capabilities, intentions and activities of foreign organisations and foreign persons. The function includes the interception of communications, in keeping with the Bureau's unique signals intelligence role within the New Zealand intelligence community.

4. Third, the Bureau plays a crucial role in support of other entities – including the New Zealand Defence Force, the New Zealand Security Intelligence Service, and law enforcement agencies including the New Zealand Police. The Bureau's unique skill-set is invaluable for other agencies to draw upon and it would be unrealistic to duplicate it in those entities. It would not be cost-effective to do so.

5. The picture that emerges from the review of the Act and the compliance review is one of a legislative framework that is not fit for purpose – and may never have been. The Act does not contain sufficient clarity or transparency to adequately support the Bureau's legitimate activities. The current framework leaves the Bureau with an ambiguous legal basis for conducting some of its core business as intended by the Act and as instructed by Cabinet. Any uncertainty in the application of the law to the Bureau's activities is highly undesirable, both legally and operationally, and carries risk. The responsible course of action is to make the legislation clearer and more transparent.

This paper has been redacted for public release.

6. The changes proposed to the Act do not represent an extension of powers. Rather, the changes will put the Bureau on a sound legal footing to continue performing the functions that the government expects it to in the interests of New Zealand. The proposals also modernise the Act to ensure it keeps up with the changing security environment and evolution in the global telecommunications environment

7. A clear and consistent governing statute is essential to underpin the oversight mechanisms that apply to the Bureau, which are also proposed to be strengthened. Together these enhancements will give confidence to the government and the wider public that the Bureau is operating within the legal parameters that have been set for it.

Background

8. On 11 December 2012, the Cabinet Committee on Domestic and External Security (DES), having taken Power to Act, agreed that a review of policy and legislation relating to the core New Zealand Intelligence Community be undertaken, including a review of the Government Communications Security Bureau Act 2003 [DES Min (12) 4/1-1].

9. Further background information is set out in the accompanying overview paper.

Comment

<u>Objectives and Functions</u>

10. Section 7 of the Act sets out a detailed statement of the Bureau's "objective", followed by an equally detailed elaboration of its "functions" in section 8. The drafting is complex, the provisions overlap and in critical ways they contradict each other. For example, section 7 effectively limits the Bureau's information security function to the public sector, whereas section 8 envisages that the Bureau may provide advice to entities outside the public sector. Given that the Bureau may only perform its functions in pursuit of its objective, it is difficult to reconcile the role envisaged in section 8 with the narrower expression of the Bureau's objective in section 7. The need for clarity is crucial at a time when the Bureau's unique cyber expertise is increasingly being called on to help manage the risks to New Zealand and New Zealanders from cyber threats.

11. The current framework also creates uncertainty as to the Bureau's function of providing expert advice and assistance to other entities in support of their lawful activities. This role is reflected in the Bureau's functions but is not referred to in the objective provision. The same tension therefore arises with respect to a function which Parliament intended the Bureau to perform, but for which no clear enabling objective exists – in effect stifling the ability of other entities (particularly New Zealand's law enforcement agencies) to draw on the Bureau's capabilities in the performance of their own lawful duties.

12. Collectively the provisions are unwieldy and create significant legal uncertainty as to the precise scope of the Bureau's legal functions. In the current environment, with rising public interest in the roles and activities of the intelligence agencies and growing reliance on GCSB's capabilities to help New Zealand meet its cyber security requirements, it is essential to address this uncertainty by restating the Bureau's core functions within a clarified and simplified legislative framework.

This paper has been redacted for public release.

13. The core functions of the GCSB should continue to be:

    (i) Information assurance/cyber security

    (ii) Foreign (communications) intelligence

    (iii) Co-operating with other entities

14. It is considered that there is scope to modify the existing sections 7 and 8 to ensure that these functions are described in a way that allows the Bureau's role and activities to be more easily comprehended.

Information Assurance/Cyber Security

15. The Bureau's information assurance/cyber security and co-operation functions are currently compressed into a single paragraph of the Act (section 8(1)(e)) which is both complex to negotiate and inadequate to empower the Bureau to carry out the full scope envisaged for those functions. Splitting the two apart will improve transparency and make it easier to articulate clearly what it is that the government intends the Bureau to do, beyond its foreign intelligence role, to support New Zealand's security, international relations and economic prosperity through the provision of expert advice and assistance.

16. The Bureau has a key role to play in the wider cyber security domain. It hosts New Zealand's National Cyber Security Centre, and Cabinet has indicated its expectation that the Bureau will considerably enhance its cyber security capabilities and use its expertise to assist a range of organisations (government, state sector, critical infrastructure providers and key economic contributors) to protect their information, ICT, networks and infrastructure from cyber threats [DES Min (10) 4/1, SEC Min (12) 4/1]. However, in the absence of a clearly legislated role beyond strict information security, and given the ways in which sections 7 and 8 further restrict rather than enable this function, the Act provides a dubious legal basis, if any, for the Bureau to develop and use new capabilities and discharge these broader responsibilities.

17. The particular role of assisting with information security is clearly indicated in the legislation as a function of the Bureau. But because the information security function must be interpreted with reference to the Bureau's objective, even this function can be read narrowly to apply only within the public sector. On one interpretation, then, the Act as currently worded excludes critical national infrastructure providers and organisations of national significance from receiving any useful assistance from the Bureau.

18. The wording of the Act also casts doubt on the Bureau's ability to collaborate with foreign partner agencies on cyber security issues. Participating in an international network of cyber security excellence gives the Bureau a valuable edge in detecting and responding to advanced cyber threats aimed at New Zealand. [text removed]

This paper has been redacted for public release.

Foreign Intelligence

19. The Bureau's foreign intelligence function is defined in the Act in a highly prescriptive way which states not only what the overall function is, but exactly what it consists of and how it is to be achieved – to a level of detail that includes deciphering, decoding, translating, examining and analysing communications. This approach was presumably intended to facilitate the production of foreign intelligence; but it is excessively specific and locks the Bureau into a certain set of activities rather than empowering it to carry out its foreign intelligence function in any manner that is legitimate. This is far from ideal, given the major changes in the ways technology is used to communicate since the Act was passed 10 years ago – and in light of future changes which can already be anticipated.

20. It is more appropriate to describe at a higher level the foreign intelligence function that the Bureau is expected to carry out, complemented by a set of powers and limitations to govern what activities may be conducted in pursuit of the function. This approach will provide transparency about the nature and scope of the function, without expressly legislating the skills required in pursuit of these functions and powers.

21. The core activity of "intercepting communications" described in section 8 was designed to be technology-neutral while defining the Bureau's unique signals intelligence role within New Zealand's intelligence community. But "intercept" and "communication" are defined so broadly in the Act that they can be read in such a way as to capture activities which do not involve interception in any ordinary sense of the word – such as exchanging foreign intelligence reporting or even imagery data with an overseas partner. This lack of clarity has created uncertainty and therefore risk for the Bureau in undertaking core business.

22. The same lack of clarity is adversely affecting activities which are unrelated to the production of foreign intelligence, but which end up being captured within the broad definition of "intercepting communications" and are therefore theoretically subject to the same restrictions that apply to the foreign intelligence function. This has the potential to impact adversely on the Bureau's ability to provide cyber security advice and assistance to government entities or private organisations. It is also hampering the Bureau from assisting law enforcement agencies in any meaningful way.

Co-operating with Other Entities

23. The Bureau fulfils a crucial role in support of other entities. The New Zealand Defence Force and the New Zealand Security Intelligence Service, as New Zealand's other security agencies, are the two domestic partners with whom the Bureau has the potential – and a need – to collaborate in certain circumstances. Law enforcement agencies including the New Zealand Police can also gain clear value from being able to draw on the Bureau for technical and other assistance in some circumstances.

24. The Act contemplates this support role, but provides no clear basis for defining the limits of such assistance. Indeed it appears to constrain the role by stating (in section 8(2)) that advice and assistance may be provided to other entities in fulfilling their functions,

but only on matters that are relevant to the pursuit of the Bureau's own objective (or to the safety of any person; or the commission of serious crime).

25. As a result, it is uncertain what basis the Bureau has for its co-operative role, and for sharing its expertise across the intelligence community and the wider public sector. It is not clear that the government can fully exploit the Bureau's capabilities for purposes that fall outside the Bureau's own objective, even when those purposes may be entirely legitimate and lawful [text removed]. Such an outcome is at odds with the drive for greater collaboration expected as part of the delivery of better public services.

26. Greater clarity is required about whether, in what circumstances, and to what extent the Bureau may provide assistance to others in accordance with its legal functions and powers. The goal should be to enable the Bureau to provide assistance to the full extent of its capability, without going beyond powers that the other agency is otherwise lawfully entitled to exercise (but may be lacking the capability). In other words, the Bureau should be able to assist another agency with any activity that the other agency is lawfully able to conduct itself, and that intersects with a capability of the Bureau, subject to any limitations imposed by law on that agency in performing its lawful duties.

27. Where the agency seeking assistance has inherent authority to conduct a particular activity, the Bureau should be able to provide assistance without requiring further evidence of authorisation from that agency. For example, no warrant would be required for the Bureau to provide assistance with processing [text removed] material that had been lawfully obtained. In some instances, depending on the nature of the activity in question, the agency requiring assistance will first need to obtain a warrant authorising such activity. For example, the Police would need an interception warrant before they could intercept communications and, by implication, before they could request assistance from the Bureau in undertaking that activity.

28. Warranted activities are by their nature more intrusive and require a greater degree of authorisation. To reassure the public that the Bureau is appropriately authorised – and as a matter of risk management on the part of the Bureau – there should be a clear audit trail in writing that accompanies any request for assistance, before the Bureau is able to take action. In this way it would be clear on its face that a request for Bureau assistance had been made and, ideally, pursuant to which authorisation. This is not to say that the Bureau may do anything at all under another agency's warrant. Clear limits exist under well-established principles of constitutional law.

29. To give additional reassurance that there will be appropriate oversight of the Bureau's activities, and to mitigate any risk of legal challenge, it would be prudent also to require the Bureau to seek its own Ministerial authorisation where advice or assistance is requested. The legislation should be sufficiently flexible to allow authorisation to be sought for particular activities, or for classes of activities performed over a stated period of time. This approach would enable the Responsible Minister to control the precise parameters of any assistance to be provided (and impose conditions where desirable, following consultation).

This paper has been redacted for public release.

Recommended Approach to Functions

30. To properly address all the issues discussed above, the following approach is recommended to setting out the functions of GCSB in legislation:

    - Repeal or significantly rationalise section 7 of the Act ("Objective of Bureau") in favour of a consolidated section 8 ("Functions of Bureau") clearly describing the three core functions of the Bureau: information assurance/cyber security, foreign intelligence, and co-operating with other entities

    - Correct the imbalance between the Bureau's three high-level functions by separating them and providing clear legal authority for each

    - Extend the description of the information assurance/cyber security function to clearly accommodate roles and responsibilities that Cabinet expects the Bureau to fulfil, and to ensure that the role can extend beyond the public sector if the government so directs

    - Rationalise the foreign intelligence function to a clear, high-level description of what the Bureau does in this area rather than a detailed list of activities and methods

    - Clarify the function of co-operating with other entities by providing a simple mechanism for the Bureau to co-operate with entities in New Zealand and overseas, with appropriate limitations and safeguards

31. Based on the approach above, section 8 of the Act ("Functions of Bureau") will be amended to craft a description of the Bureau's three core functions around the following elements:

    - *Information assurance/cyber security* – Co-operating with, and providing advice and assistance to both public and private sector entities on matters relating to the security and integrity of electronic information, communications, and information infrastructures of importance to the government

    - *Foreign intelligence* – Gathering and sharing communications intelligence about the capabilities, intentions or activities of foreign organisations or foreign persons, in accordance with the government's intelligence requirements

    - *Co-operating with other entities* – Co-operating with, and providing advice and assistance to approved entities (notably security and law enforcement agencies) in the performance of their lawful duties; and co-operating with approved entities to facilitate the Bureau's performance of its own functions

32. Officials will consult the Responsible Minister and the Attorney-General when drafting the description of the Bureau's core functions.

<u>Powers, Controls and Limitations</u>

33. Part 3 of the Act sets out the intrusive powers available to the Bureau, namely the power to intercept certain communications and to access certain computer systems with

This paper has been redacted for public release.

authorisation as required. These powers are subject to section 14 of the Act, which imposes strict limitations where the communications of New Zealanders are involved. The basic premise that the GCSB is not to conduct foreign intelligence activities against New Zealanders remains valid. But the evolution of communications technology and the rigid formulation of section 14 have conspired to cause unanticipated consequences that are preventing the Bureau from conducting legitimate core business, including support for other agencies and responsibilities in the cyber security domain that Cabinet expects the Bureau to fulfil.

34. It is imperative that these anomalies be addressed in a way that respects the paramountcy of New Zealanders' privacy while allowing the Bureau to perform its lawful functions effectively. Modifications to the approach in section 14 are recommended to resolve the unanticipated effects of that provision. This involves applying limitations to the Bureau's foreign intelligence function while enabling the Bureau:

- to conduct activities that do not impinge, or do not unduly impinge, on New Zealanders' privacy (in particular, interception of openly broadcast information; interception with the consent of the parties to a communication; or training and testing of equipment);
- [text removed]
- [text removed]
- to collect information on New Zealanders when assisting another agency in the performance of its lawful duties.

Section 14

35. Section 14 of the Act states that:

> Neither the Director, nor an employee of the Bureau, nor a person acting on behalf of the Bureau may authorise or take any action for the purpose of intercepting the communications of a person… who is a New Zealand citizen or permanent resident.

In its intent, section 14 reflects a basic premise that the GCSB is not to conduct foreign intelligence activities against New Zealanders.

36. Section 14 was designed to place limits on the Bureau's foreign intelligence gathering function. This is evident from section 13, which currently describes the Bureau's powers only in terms of the foreign intelligence role. What was not foreseen was that section 14 might impinge on the Bureau's ability to perform a key cyber security role: that is, working to ensure that New Zealand people and organisations can operate in a safe and secure cyber environment. Cyber attacks are launched against New Zealand by foreign adversaries, but they are carried on New Zealand infrastructure and impact on New Zealand victims. GCSB cannot identify, investigate or defend against these attacks if it is prevented from directing its analytic tools towards the communications infrastructure within which the attacks are hidden.

This paper has been redacted for public release.

37. [text removed]

38. [text removed]

39. [text removed]

40. [text removed]

41. On matters relating to national security, NZSIS has expressed concern about impacts on its operational effectiveness with respect to persons of security concern to New Zealand. In particular, section 14 prevents the Bureau from providing assistance in the following situations where NZSIS may lack capability:

    - foreigners known to be of security concern making contact with New Zealand citizens and permanent residents; and
    - [text removed].

42. [text removed]

43. In summary, section 14 is outwardly attractive as a prominent, unequivocal safeguard of the privacy of New Zealanders. However, the absolute way in which the provision is expressed, together with developments in communications technology and broadly defined terms, are preventing the Bureau from carrying out core business. In its current wording section 14 is hampering the Bureau in performing its foreign intelligence and co-operation functions, and prevents it from effectively fulfilling the evolving cyber security responsibilities assigned to it by Cabinet. [text removed]

44. The protection of New Zealanders' privacy is fundamental and should be an integral part of GCSB's compliance framework. But the rigid expression of that expectation in section 14 is no longer fit for purpose, and needs to be recast in a way that permits the Bureau to carry out legitimate activities to fulfil its functions in an effective and efficient manner. The controls should be as robust and as credible as they are now; and they should take full account of human rights and contemporary privacy considerations, including developments in the area of unreasonable search and seizure.

45. As noted above, section 14 interacts closely with other provisions in the Act to create an overarching framework for the Bureau's intrusive powers. In the course of developing a new approach for section 14, other modifications to the interception and access authorisation mechanism, or to related defined terms, may prove necessary to ensure that the process as a whole works seamlessly and achieves the right balance between protecting New Zealanders' privacy and facilitating the Bureau's legitimate activities.

Recommended Approach to Section 14

46. To properly address the issues discussed above, it is proposed to modify the approach taken in section 14 of the Act so as to resolve the unanticipated effects of that provision. The modifications would aim to:

This paper has been redacted for public release.

- Preserve the basic premise that foreign intelligence activities may not be directed at New Zealanders
- Apply limitations to the Bureau's foreign intelligence function only
- Permit the Bureau to conduct activities that do not impinge, or do not unduly impinge, on New Zealanders' privacy (in particular, interception of openly broadcast information; interception with the consent of the parties to a communication; or training and testing of equipment)
- [text removed]
- [text removed]
- Enable the Bureau to collect information on New Zealanders when assisting another agency in the performance of its lawful duties, subject to any limitations imposed by law on that agency in the performance of its duties, and subject to the Bureau obtaining Ministerial authorisation (which may be given for one or more activities or for one or more classes of activities; and subject to any directions, conditions or restrictions that the Responsible Minister considers appropriate)

Powers

47. As noted earlier, Part 3 of the Act confers three powers of interception on the Bureau:

    (i) Warrantless interception in situations not involving the physical connection of an interception device to a network; and not involving the installation of an interception device in any place in order to intercept communications in that place (sections 15 and 16)

    (ii) Interception of communications by an interception device under an interception warrant granted by the Responsible Minister (section 17)

    (iii) Access to a computer system under a computer access authorisation granted by the Responsible Minister (section 19)

48. This construct continues to provide the basic tools that the Bureau needs to perform its functions effectively and efficiently, though the language used to capture the powers is in some respects outdated and would benefit from being refreshed. There may also be opportunities to clarify and streamline aspects of the powers related to the wider overhaul of the legislation.

49. At present, section 13 of the Act dictates that the Bureau's powers are only available for the purpose of obtaining foreign intelligence. While much of the Bureau's work (including in the cyber security domain) can ultimately be linked to a foreign intelligence objective, the Act was conceived at a time when the nature, extent and potential impact of the cyber threat was dramatically different from the threat posed now, and the approach imposed by section 13 is anachronistic and overly limiting. It is proposed to broaden the ambit of the powers in Part 3 to the performance of any or all of the Bureau's functions, subject to appropriate controls and limitations.

This paper has been redacted for public release.

50. Section 25 of the Act currently allows the Bureau to retain and pass on any information that comes into its possession relating to the prevention or detection of serious crime – even if the Bureau would ordinarily be obliged to destroy that information as irrelevant. It is proposed to retain this concept of "incidentally obtained intelligence" to enable the Bureau to communicate information in a slightly expanded range of situations such as activities involving a threat to life; a threat to security; persons acting as an agent of a foreign power; as well as the commission of a serious crime.

Ministerial Authorisation

51. Sections 17 and 19 of the Act currently provide the mechanisms for seeking Ministerial authorisation to intercept communications and to access specified computer systems. Approval may only be granted if the Minister is satisfied that certain conditions exist, including: that the activities are essential to advance an objective of the Bureau; that the value of the information sought justifies the proposed activity; and that the information is not likely to be obtained by other means. It is proposed to augment these with further conditions requiring an assurance that nothing will be done beyond what is required to properly perform a function of the Bureau; and that the nature and consequences of the acts done will be reasonable, having regard to the purposes for which they are carried out. These tests draw on similar provisions in the Search and Surveillance Act 2012 (section 68, for example) and in Australia's Intelligence Services Act 2001.

52. In order to bring greater transparency and consistency to Ministerial oversight of the Bureau's activities, an additional mechanism is proposed, in line with a similar provision in Australia's Intelligence Services Act 2001. The mechanism would enable the Minister to issue written directions to the Bureau setting out the particularly sensitive or non-routine activities or classes of activities for which the Bureau would be required to obtain explicit Ministerial authorisation before proceeding. This additional control measure might apply, for example, to [text removed] particular forms of co-operation with other agencies.

53. It is proposed that the same strict conditions would apply to all avenues for seeking Ministerial authorisation. This will establish a higher degree of consistency across the mechanisms and provide greater confidence that all activities proposed by the Bureau are truly necessary, justified and reasonable.

54. The enhanced Ministerial authorisation process suggested in this section sits within a wider framework of enhanced oversight – in particular through the revamped role of Inspector-General of Intelligence and Security – which is proposed in the accompanying paper on oversight of the intelligence agencies.

Recommended Approach to Powers and Authorisations

55. With regard to the powers of the Bureau and the associated authorisation mechanisms, the following approach is proposed:

- Retain the basic construct of specific powers to intercept communications and to access computer systems with appropriate authorisation processes

This paper has been redacted for public release.

- Retain the concept of "incidentally obtained intelligence" in section 25 of the Act, and enable its application to a modestly expanded range of situations such as a threat to life; a threat to security; acting as an agent of a foreign power; as well as the commission of a serious crime

- Introduce greater Ministerial oversight with a new mechanism through which the Minister would specify particularly sensitive or non-routine activities or classes of activities requiring explicit Ministerial authorisation

- Enhance the range of conditions that must be satisfied before Ministerial authorisation may be granted to include assurances that the activities proposed by the Bureau are necessary, justified and reasonable, and apply those conditions to all Ministerial authorisation processes to improve consistency across the authorisation mechanisms

- Clarify that the Bureau's powers apply to the performance of all its functions

- During the drafting phase, make other amendments as appropriate to update, clarify and streamline the framework underpinning the Bureau's powers and related controls and authorisation processes

Miscellaneous Amendments

56. Several miscellaneous amendments have been identified to complement other proposals for the Bill, to promote operational efficiency in the Bureau's business, and in the interests of updating the Act generally.

Privacy Protections

57. Under section 57 of the Privacy Act 1993, the Bureau and NZSIS are exempt from all the privacy principles except principles 6 (access to personal information), 7 (correction of personal information) and 12 (unique identifiers). In the 1998 report *Necessary and Desirable*, the Privacy Commissioner recommended that the Act be amended to make a further four principles applicable to the intelligence agencies:

    - Principle 1 (purpose of collection of personal information)

    - Principle 5 (storage and security of personal information)

    - Principle 8 (accuracy of personal information to be checked before use)

    - Principle 9 (agency not to keep personal information for longer than necessary)

58. The Law Commission considered and supported this recommendation in its June 2011 review of the Privacy Act. [text removed]

59. Effective oversight will help to give confidence in the Bureau's implementation of privacy protections. The Office of the Privacy Commissioner and the Inspector-General of Intelligence and Security have overlapping responsibilities in this regard (see section 15(3) of the Inspector-General of Intelligence and Security Act 1996). During the

This paper has been redacted for public release.

drafting phase, consideration will be given to how this should best be managed, including the possibility of legislative amendments, given the range of proposals in this paper.

60. The Privacy Act was amended in February 2013 to introduce a new regime for the sharing of personal information to facilitate the provision of public services. During the drafting phase, consideration will be given to the practical implications of the new regime, including whether the Bureau should look to develop an information sharing framework that mirrors Part 9A of the Privacy Act, with the possibility of exemptions from or modifications to the information privacy principles, if appropriate.

Record of Warrants/Authorisations

61. To enable the Inspector-General of Intelligence and Security to have access to the best possible information [text removed], it is proposed that the Act be amended to formalise the Bureau's current practice by requiring it to maintain a written record of all warrants and authorisations, in a form readily available for inspection by both the Responsible Minister for GCSB and the Inspector-General. [text removed] this will not only provide clarity for the Inspector-General, but will also support a strong compliance culture within the intelligence agencies. Further context for this proposal is set out in the accompanying paper on oversight of the intelligence agencies.

Immunity from Criminal and Civil Liability

62. The functions and powers set out in the Act (both currently, and as it is proposed to be amended) empower the Bureau to undertake activities that would otherwise be in breach of law. It is important to safeguard Bureau employees, and others who may be authorised to assist the Bureau in its lawful duties, against exposure to criminal or civil proceedings when acting in good faith in the performance of a legitimate function. This includes situations where the Bureau is providing assistance to another entity.

63. Section 21 of the Act currently provides that every person who is authorised to give effect to an interception warrant or a computer access authorisation is justified in taking any reasonable action necessary to give effect to it. The language of section 21 is somewhat outmoded and is at present confined to activities conducted under Ministerial authorisation. It is proposed to update section 21 of the Act to align it with any revisions to the provisions on powers, and to acknowledge that the Bureau has a limited number of powers that may be exercised without Ministerial authorisation. Consistent with the equivalent regime in the Search and Surveillance Act 2012, the intent is to ensure that the Act provides a person with immunity from civil and criminal liability in New Zealand for any reasonable act done in New Zealand or elsewhere in good faith in accordance with the legislation, including under the function of assisting other entities.

Penalties for Unauthorised Disclosure of Information

64. Under section 11 of the Act, it is an offence for a current or former employee of the Bureau to disclose or use without authorisation any information obtained through the person's connection with the Bureau. The offence carries a maximum penalty of two

years' imprisonment or a fine not exceeding $2,000. It is timely to update the maximum penalty for this offence in line with equivalent provisions elsewhere in the statute book, commensurate with the seriousness of disclosing information affecting national security and New Zealand's international reputation (see, for example, s78A of the Crimes Act 1961). With this in mind, it is proposed that the penalty be increased to a maximum of three years' imprisonment or a fine of $5,000, or both.

Authorisation in Situations of Urgency

65. Under the Act as it stands, only the Responsible Minister has authority to grant an interception warrant or a computer access authorisation. It is proposed to amend the Act to provide alternative avenues for obtaining Ministerial authorisation in situations of urgency when the Responsible Minister is not readily available. In such circumstances the Bureau would be able to seek authorisation from specified other Ministers, including the Minister of Defence, the Minister of Foreign Affairs and the Attorney-General.

Consequential Amendments

66. Depending on the final shape of the provisions on Ministerial authorisations, consequential amendments may be required to associated provisions such as section 18 (which relates to persons acting under an interception warrant). These amendments would be of a largely administrative nature.

Amendment to the Appointment Framework for the Director of GCSB

67. In 2010, Cabinet agreed that the appointment framework for the chief executive of GCSB (and of NZSIS) be adjusted to provide the State Services Commissioner with a statutory mandate to manage and advise on the selection process, defining the term of office of up to five years, providing for the reappointment of chief executives, and establishing the role of the State Services Commissioner in setting conditions of service and the process for termination [CAB Min (10) 38/8]. These decisions were given effect through non-legislative measures until such time as it was practicable to make the necessary legislative amendments. The review of the Act presents such an opportunity.

Consultation

68. This paper was prepared by the Department of the Prime Minister and Cabinet in collaboration with the Government Communications Security Bureau. The New Zealand Security Intelligence Service, New Zealand Defence Force, Ministry of Foreign Affairs and Trade, New Zealand Police, Office of the Privacy Commissioner, New Zealand Customs Service, Ministry of Defence, Ministry of Justice, State Services Commission and the Treasury were consulted.

Financial Implications

69. There are no financial implications arising from this proposal.

This paper has been redacted for public release.

Human Rights

70. The proposals in this paper were developed to be consistent with the right and freedoms affirmed in the New Zealand Bill of Rights Act 1990 (NZBORA) and the Human Rights Act 1993. The proposed amendments, in particular, engage the right to be free from unreasonable search and seizure affirmed in section 21 of the NZBORA.

71. A final view on the consistency with the NZBORA will possible once legislation is drafted. The Crown Law Office will be undertaking the NZBORA vet of the Intelligence and Security Bill.

Legislative Implications

72. Legislation is required to implement this proposal. On 11 December 2012, the Cabinet Committee on Domestic and External Security agreed that a bid be prepared for the 2013 Legislation Programme for an Intelligence and Security Bill with a category 2 priority (must be passed in 2013), and noted that the bill would be enacted by August 2013 [DES Min (12) 4/1-1].

73. It is proposed that the Act as amended will bind the Crown. This is consistent with the approach taken in section 5 of the current Act.

Regulatory Impact Analysis

74. Regulatory Impact Analysis requirements apply to this paper. A Regulatory Impact Statement has been prepared and accompanies this suite of papers.

Recommendations

75. The Minister Responsible for GCSB recommends that the Committee:

Background

1. **note** that on 11 December 2012 DES agreed that a review of the Government Communications Security Bureau Act 2003 (the Act) be undertaken [DES Min (1) 4/1-1];

2. **note** that the Act has been reviewed in light of prevailing circumstances, revealing a number of issues that are giving rise to legal risks, as well as hampering the Bureau's legislated powers in unanticipated ways, adversely impacting on the Bureau's ability to perform its legitimate activities and preventing it from being well positioned to deal with future issues;

Objective and Functions

3. **agree** that section 7 of the Act ("Objective of Bureau") be repealed or significantly rationalised in favour of a consolidated section 8 ("Functions of Bureau") clearly describing the three core functions of the Bureau: information assurance/cyber security, foreign intelligence, and co-operating with other entities;

This paper has been redacted for public release.

4. **agree** that the three core functions of the Bureau be reflected in the Act with equal prominence and with clear legal authority provided for each function;

5. **agree** that the description of the Bureau's information assurance/cyber security function should be adjusted to accommodate roles and responsibilities that Cabinet expects the Bureau to fulfil (such as assisting New Zealand organisations to protect their information, ICT systems and networks, and infrastructure, from cyber threats) and to ensure flexibility for the function to be delivered outside the public sector if so directed;

6. **agree** that the Bureau's foreign intelligence function should be rationalised to a clear, high-level description of what the Bureau does in this domain rather than a detailed list of activities and methods;

7. **agree** that the Bureau's co-operation and assistance function should be clarified to ensure that the Bureau can work with approved entities in New Zealand and overseas, with limitations and safeguards as appropriate;

8. **note**, based on the approach in recommendations 3 – 7, that section 8 of the Act ("Functions of Bureau") will be amended to craft a description of the Bureau's three core functions around the following elements:

   8.1 *Information assurance/cyber security* – Co-operating with, and providing advice and assistance to both public and private sector entities on matters relating to the security and integrity of electronic information, communications, and information infrastructures of importance to the government

   8.2 *Foreign intelligence* – Gathering and sharing communications intelligence about the capabilities, intentions or activities of foreign organisations or foreign persons, in accordance with the government's intelligence requirements

   8.3 *Co-operating with other entities* – Co-operating with, and providing advice and assistance to approved entities (notably security and law enforcement agencies) in the performance of their lawful duties; and co-operating with approved entities to facilitate the Bureau's performance of its own functions

9. **note** that officials will consult the Responsible Minister and the Attorney-General when drafting the description of the Bureau's core functions;

Powers, Controls and Limitations

10. **note** that the existing powers to intercept communications and to access computer systems in sections 16, 17 and 19 of the Act continue to provide the basic tools that the Bureau requires to perform its functions, subject to some updating of the language used;

This paper has been redacted for public release.

11. **note** that section 14 of the Act ("Interceptions not to target domestic communications") reflects a basic operating premise that the Bureau is not to conduct foreign intelligence activities against New Zealanders;

12. **note** that the rigid expression of section 14, together with broadly defined terms and changes in technology, are causing unanticipated consequences preventing the Bureau from conducting legitimate core business, including support for other agencies and responsibilities in the cyber security domain that Cabinet expects the Bureau to fulfil;

13. **agree** that the approach in section 14 of the Act should be modified in a way that resolves the unanticipated effects of that provision, including:

    13.1 safeguarding the privacy of New Zealanders and the basic premise that the Bureau's foreign intelligence activities may not be directed at New Zealanders;

    13.2 permitting the Bureau to conduct activities that do not impinge, or do not unduly impinge, on New Zealanders' privacy (in particular, interception of openly broadcast information; interception with the consent of the parties to a communication; or training and testing of equipment);

    13.3 [text removed]

    13.4 [text removed]

    13.5 enabling the Bureau to collect information on New Zealanders when assisting another agency in the performance of its lawful duties, subject to any limitations imposed by law on that agency in the performance of its duties, and subject to the Bureau obtaining Ministerial authorisation (which may be given for one or more activities or for one or more classes of activities; and subject to any directions, conditions or restrictions that the Responsible Minister considers appropriate);

14. **agree** that:

    14.1 the concept of "incidentally obtained intelligence" reflected in section 25 of the Act should be retained; and

    14.2 the application of the concept should enable the Bureau to retain and share information in a limited set of circumstances such as a threat to life; a threat to security; persons acting as an agent of a foreign power; or the commission of a serious crime;

15. **agree** that the Act should be amended to incorporate a new mechanism to enhance Ministerial oversight of Bureau activities, through which the Minister

This paper has been redacted for public release.

would specify particularly sensitive or non-routine activities or classes of activities requiring explicit Ministerial authorisation;

16. **agree** that the conditions under which Ministerial authorisation may be granted should be enhanced to include assurances that the activities proposed by the Bureau are necessary, justified and reasonable, and to provide consistency across the Ministerial authorisation mechanisms;

17. **agree** that the Act should be amended to reflect that the Bureau may exercise its legislated powers to fulfil any of its prescribed functions;

18. **agree** during the drafting phase that other amendments be made as appropriate to update, clarify and streamline the framework underpinning the Bureau's powers and related controls and authorisation processes;

Miscellaneous Amendments

19. **note** that, under section 57 of the Privacy Act 1993, the Bureau is currently exempt from all the privacy principles except principles 6 (access to personal information), 7 (correction of personal information) and 12 (unique identifiers);

20. **agree** that, [text removed]:

    20.1 privacy principle 5 should apply to the Bureau without modification;

    20.2 privacy principles 1, 8 and 9 should apply to the Bureau, modified if necessary to achieve the effective and efficient performance of the Bureau's functions, in consultation with the Office of the Privacy Commissioner, the Ministry of Justice and affected agencies;

21. **agree** that, [text removed] the Act should be amended to formalise the Bureau's current practice by requiring it to maintain a written record of all warrants and authorisations, in a form readily available for inspection by both the Responsible Minister for GCSB and the Inspector-General of Intelligence and Security;

22. **agree** that section 21 of the Act should be amended, consistent with the equivalent regime in the Search and Surveillance Act 2012, to ensure that it provides a person with immunity from civil and criminal liability in New Zealand for any reasonable act done in New Zealand or elsewhere in good faith in accordance with the legislation, including under the function of assisting other entities;

23. **agree** that the Act should be amended to increase the penalty for unauthorised disclosure of information to a maximum of three years' imprisonment/a fine of $5,000 or both, to align it with penalties for equivalent offending elsewhere in legislation;

This paper has been redacted for public release.

24. **agree** that the Act should be amended to enable authorisation to be granted by a Minister other than the Responsible Minister in situations of urgency when the Responsible Minister is not readily available or contactable;

25. **note** that consequential amendments may be needed to the provisions governing the execution of Ministerial authorisations;

26. **note** that in 2010, Cabinet agreed to modify the appointment framework for the Director of GCSB, providing the State Services Commissioner with a statutory mandate to manage and advise on the selection process and providing for other matters related to the office of Director [CAB Min (10) 38/8], and that amendments to the Act are required to give effect to these decisions;

Legislative Process

27. **note** that on 11 December 2012 DES agreed that a bid be prepared for the 2013 Legislation Programme for an Intelligence and Security Bill with a category 2 priority (must be passed in 2013) [DES Min (12) 4/1-1];

28. **note** that on 11 December 2012 DES noted that the bill would be enacted by August 2013 [DES Min (12) 4/1-1];

29. **invite** the Minister Responsible for GCSB, and the Minister of State Services in relation to the proposed amendments to the appointment framework for the Director of GCSB, to issue drafting instructions to Parliamentary Counsel to give effect to the above decisions;

30. **agree** that the Act as amended should bind the Crown, consistent with the present approach under section 5 of the Act;

31. **authorise** the Minister Responsible for GCSB and the Attorney-General to make any decisions on additional matters that are necessary for the above proposals, and that are consistent with Cabinet's decisions.

Rt Hon John Key
Minister Responsible for the Government Communications Security Bureau

……/……./2013