DEPARTMENT OF THE PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

29 April 2025

[redacted]

Ref: OIA-2024/25-0625

Tēnā koe [redacted]

Official Information Act request for Cabinet papers for the GCSB Amendment and Related Legislation Amendment Bill, 2013

Thank you for your Official Information Act 1982 (the Act) request received on 5 February 2025. You requested:

> *"… the cabinet papers for the Government Communications Security Bureau Amendment and Related Legislation Amendment Bill from 2013;*
> *cabinet papers for what became the Government Communications Security Bureau Amendment Act 2013; and*
> *any cabinet papers that came in response to the Compliance Review of GCSB report published by Rebecca Kitteridge in 2013."*

The time frame for responding to your request was extended under section 15A of the Act by 36 working days. The extension was required because the Cabinet papers you have requested date back to 2012 and 2013, so we have needed to locate and compile hard copies of papers that may be relevant. Once assessed as to which documents are in scope of your request, these were compiled into an electronic form to enable consultations to be undertaken prior to making a decision on your request.

The Cabinet documents we have compiled directly relate to the drafting and introduction of the Government Communications Security Bureau Amendment and Related Legislation Amendment Bill, which was introduced on 8 May 2013 and received Royal Assent on 26 August 2013. A copy of the 2013 Act with the Related Bill and Versions of the Act can be found on the New Zealand Legislation website at: www.legislation.govt.nz/act/public/2013/0057/latest/DLM5177706.html.

The Government Communications Security Bureau Amendment Act 2013 was itself repealed, on 28 September 2017, and replaced with the Intelligence and Security Act 2017.

Please find attached a copy of the Cabinet documents identified as relevant to all parts of your request. We have included both Cabinet Committee and Cabinet papers and their related Minutes. Where there was only a Minute recording decisions made, we have included together with any relevant documentation identified from the meeting.

The documents released to you are set out in the table below:

Item	Portfolio	Date	Title	Decision
Item 1	Prime Minister	23/11/2012 26/11/2012	DES (12) 4 DES Min (12) 13/1 New Zealand Intelligence Community Policy and Legislation Review	Release with some information withheld under: s6(a) Some information Not in Scope
Item 2	Prime Minister	26/11/2012 23/01/2013	CAB (13) 7 CAB Min (13) 1/5 Report of the Cabinet Committee on Domestic and External Security: period ended 14 December 2012	Release with some information withheld under: s6(a) Some information Not in Scope
Item 3	Prime Minister	7/12/2012 11/12/2012	DES (12) 5 DES Min (12) 4/1-1 New Zealand Intelligence Community Policy and Legislation Review [*Remainder of Title not in scope*]	Release with some information withheld under: s6(a) Some information Not in Scope
Item 4	Prime Minister	15/02/2013 10/02/2013 25/02/2013	DES (13) 5 DES Min (13) 1/1 CAB Min (13) 5/5 New Zealand Intelligence Community Policy and Legislation Review: Overview	Release with some information withheld under: s6(a) Some information Not in Scope
Item 5	GCSB	25/03/2013	DES (13) 10 Review of the Government Communications Security Bureau Act 2003: Paper 1: Overview	Release with some information withheld under: s6(a) Some information Not in Scope
Item 6	GCSB	25/03/2013	DES (13) 11 Review of the Government Communications Security Bureau Act 2003: Paper 2: Proposals	Release with some information withheld under: s6(a) s9(2)(h)
Item 7	GCSB	26/03/2013 28/03/2013 2/04/2013	DES Min (13) 3/2-3 CAB (13) 175 - Part 2 CAB Min (13) 10/8 Review of the Government Communications Security Bureau Act 2003	Release with some information withheld under: s6(a) Some information Not in Scope
Item 8	GCSB	8/04/2013 April 2013 22/04/2013	DES (13) 12 DES Min (13) 4/1 CAB Min (13) 13/6(A) GCSB Act Review: Alternative Proposals on Ministerial Authorisation	Release with some information withheld under: s6(a)
Item 9	GCSB/ NZSIS	3/05/2013 6/05/2013	CAB (13) 239 CAB Min (13) 14/1 Government Communications Security Bureau and Related Legislation Amendment Bill: Approval for Introduction	Release with some information withheld under: s6(a) Some information Not in Scope

Item	Portfolio	Date	Title	Decision
Item 10	Prime Minister/ Finance	20/06/2014	CAB (14) 324 New Zealand Intelligence Community Strategy, Capability and Resourcing Review: Commencement and Policy Expectations	Release with some information withheld under: s6(a) Some information Not in Scope

As marked in table above and the documents released to you, some information has been withheld under the following sections of the Act:

- section 6(a), to protect the security or defence of New Zealand or the international relations of the Government of New Zealand
- section 9(2)(h), to maintain legal professional privilege.

In addition, where there is information included in the Cabinet documents that is not relevant to your request, such as information about other matters and other legislation, it has been marked as not in scope.

Where section 9 applies, in making my decision, I have considered the public interest considerations in section 9(1) of the Act. No public interest has been identified that would be sufficient to outweigh the reasons for withholding that information.

You have the right to ask the Ombudsman to investigate and review my decision under section 28(3) of the Act.

This response will be published on the Department of the Prime Minister and Cabinet's website during our regular publication cycle. Typically, information is released monthly, or as otherwise determined. Your personal information including name and contact details will be removed for publication.

Yours sincerely

Bridget White
Executive Director
National Security Group

Cabinet Committee on Domestic and External Security

DES (12) 4

Copy No: 15

Summary of Paper

23 November 2012

New Zealand Intelligence Community Policy and Legislation Review

Portfolio Prime Minister

Purpose This paper seeks agreement to a review of policy and legislation relating to the core New Zealand Intelligence Community (the NZIC).

Previous Consideration None.

Summary

The core NZIC comprises three key agencies together with the Intelligence Coordination Group (ICG) in the Department of the Prime Minister and Cabinet (DPMC). The agencies are the:

- New Zealand Security Intelligence Service (NZSIS);
- Government Communications Security Bureau (GCSB); and
- National Assessments Bureau in DPMC.

The NZIC has been the subject of reviews relating to priorities for the NZIC, and NZIC governance and management arrangements. Significant progress has been made in NZIC integration. However, the functions and powers of the NZIC agencies were out of scope of the reviews.

The paper proposes a single review of NZIC policy and legislation, which will include:

- completing NZSIS' current review of the New Zealand Security Intelligence Service Act 1969;
- reviewing the Government Communications Security Bureau Act 2003 including its objectives, functions and powers of the GCSB, and the current wording of section 14 prohibiting the interception of communications of New Zealand citizens and permanent residents;
- considering changes to the NZSIS and GCSB Acts to address the changing cyber environment;
- considering whether the Intelligence and Security Committee Act 1996 and the Inspector-General of Intelligence and Security Act 1996 continue to be fit for purpose;
- focusing on the relationship between the GCSB and other agencies and making recommendations to provide clarity about who can work with whom, on what;

- recommending any legislative changes to facilitate the NZIC's shared administrative services and enable greater collaboration.

The review will be carried out by DPMC (the ICG and the National Cyber Policy Office), GCSB and NZSIS, and overseen by a Steering Committee comprising the: Chief Executive, DPMC; the Director, GCSB; the Director, NZSIS; the Director, ICG; and an Associate Director, GCSB.

Policy proposals will be considered by the Officials Committee on Domestic and External Security Coordination in close consultation with the Treasury and the State Services Commission. A number of other government agencies will be consulted, and the review will take into account related policy work in other portfolios.

Regulatory Impact Analysis	A Regulatory Impact Statement is not required as the paper does not seek decisions on policy options.
Baseline Implications	The cost of the review will be met from the baselines of DPMC, GCSB, and NZSIS.
Legislative Implications	An omnibus Intelligence and Security Bill will contain any required amendments to NZIC legislation. The Prime Minister will give consideration how best to manage the parliamentary stages of the amending legislation, including the role of the Intelligence and Security Committee.
Timing Issues	A timetable for the review and enactment of amending legislation is set out on page 7.
Announcement	None.
Consultation	Paper prepared by DPMC in consultation with the NZSIS and the GCSB. Treasury and SSC were informed. The Prime Minister indicates that discussion is not required with the government caucus or with other parties represented in Parliament.

The Prime Minister recommends that the Committee:

1 note that the core New Zealand Intelligence Community comprises the New Zealand Security Intelligence Service, the Government Communications Security Bureau, and the National Assessments Bureau, supported by the Intelligence Coordination Group;

2 agree that a review of policy and legislation relating to the core New Zealand Intelligence Community be undertaken;

3 agree that the review of the policy and legislation will include:

3.1 the existing review of the New Zealand Security Intelligence Service Act 1969;

3.2 a review of the Government Communications Security Bureau Act 2003;

3.3 a review of the functions and powers needed to address cyber security, cyber effects, critical infrastructure protection and other related capabilities;

3.4 a review of external oversight mechanisms, in particular a review of the Intelligence and Security Committee Act 1996 and the Inspector-General of Intelligence and Security Act 1996;

3.5 a review of the ability of intelligence agencies to collaborate and cooperate with other agencies under existing legislation;

3.6 an assessment of any legislative changes required to facilitate the commitment to "one community, many agencies";

4 note that the review will be undertaken by the Department of the Prime Minister and Cabinet, the New Zealand Security Intelligence Service and the Government Communications Security Bureau, and be funded from within their baselines;

5 note that a bid will be prepared for the 2013 Legislation Programme for an Intelligence and Security Bill with a category 2 priority (must be passed in 2013);

6 note that consideration will be given to the appropriate form of parliamentary consideration of the bill.

Gerrard Carter
Committee Secretary

Distribution:
Cabinet Committee on Domestic and External Security Co-ordination
Office of the Prime Minister
Chief Executive, DPMC
Director, Security and Risk, DPMC
Director, Intelligence Coordination Group, DPMC
Director, National Assessments Bureau, DPMC
Director, NZSIS
Director, GCSB
Secretary to the Treasury
Secretary of Foreign Affairs and Trade
State Services Commissioner

Office of the Prime Minister

Cabinet Domestic and External Security Committee

NEW ZEALAND INTELLIGENCE COMMUNITY POLICY AND LEGISLATION REVIEW

Proposal

1. The purpose of this paper is to seek agreement on a review of policy and legislation relating to the core New Zealand Intelligence Community.

Executive Summary

2. The core New Zealand Intelligence Community (NZIC) comprises three key agencies together with the Intelligence Coordination Group (ICG), which is located in the Department of Prime Minister and Cabinet (DPMC):

    a. the New Zealand Security Intelligence Service (NZSIS);
    b. the Government Communications Security Bureau (GCSB); and
    c. the National Assessments Bureau (NAB), which is located in DPMC.

3. The NZIC has been the subject of internally and externally led reviews relating to priorities for the NZIC, and NZIC governance and management arrangements. These reviews have been considered by Cabinet and their recommendations have largely been implemented. Significant progress has been made on integration of the NZIC, and the banner of "one community, many agencies" has been adopted.

4. Integration is important not simply for cost and efficiency reasons but more importantly because given the range and complexity of national security challenges, a small intelligence community needs to be as integrated as possible to meet them. A review of existing administrative legislative provisions may offer opportunities to support the commitment to "one community, many agencies".

5. The functions and powers of the NZIC agencies, however, were out of scope of the recently completed reviews. The NZSIS has been considering its role and functions and how they should be updated to reflect contemporary threats to national security and ways of mitigating the risks these threats pose, and their policy and legislative work is well advanced.

6. The GCSB has been considering potential areas of future need, particularly in the area of cyber security and related matters. However, policy or legislative work has yet to be undertaken to determine whether any amendments are required to their legislation. In addition, recent events have given rise to concerns about GCSB's compliance with legislation and operational processes. The Secretary of the Cabinet was seconded to conduct a compliance review, which may identify other areas for policy work and possible legislative amendment. One area of focus may be how GCSB supports and cooperates with other government agencies.

7. The current work being undertaken by the NZIC regarding functions and powers raises the question of whether the external oversight mechanisms (the Intelligence and Security Committee, the Inspector-General of Intelligence and Security and the Commissioner of Security Warrants) will be fit for purpose in light of any changes to functions and powers.

8. While separate work is underway on some of these issues (integration, functions and powers) and in the case of the NZSIS is well advanced, given the relationship between the issues I propose to bring them together in a single NZIC policy and legislation review. The review will be carried out by DPMC, NZSIS and GCSB, and be funded from within their baselines. The review will be overseen by a Steering Committee chaired by the Chief Executive of DPMC.

9. Any change to legislation arising from the review will be progressed through an omnibus "Intelligence and Security Bill", with the aim of enacting it before the end of 2013. A bid for such a bill will be made for the 2013 Legislation Programme.

10. Any bill relating to the GCSB or NZSIS would normally be referred to the Intelligence and Security Committee. While that process has generally worked well I will be considering whether any alternative approaches might provide a better forum for the bill. A key consideration will be the ability to manage sensitive information that may need to be put before the committee to explain the provisions in the bill.

Background

11. The legislative framework for the NZIC is contained in four pieces of legislation:

- Government Communications Security Bureau Act 2003 (GCSB Act),
- Inspector-General of Intelligence and Security Act 1996 (IGIS Act),
- Intelligence and Security Committee Act 1996 (ISC Act),
- New Zealand Security Intelligence Service Act 1969 (NZSIS Act).

12. [Not in Scope] , no substantive changes have been made to the GCSB Act and the two oversight Acts.

13. Over the last few years the NZIC has also been the subject of internally and externally led reviews, and making operational changes to implement the outcomes of those reviews that have been finalised. This work, which is set out in brief below, provides the background and drivers for the proposed NZIC policy and legislation review.

Governance and management of the NZIC

14. In June 2009 Cabinet initiated a review of the intelligence agencies, which was conducted by Simon Murdoch on behalf of the State Services Commissioner (Murdoch review). The review did not identify performance failure at an agency or system level, but proposed a range of adjustments to support the New Zealand intelligence community.

15. The outcome of the Murdoch review was considered by Cabinet in February 2010, and Cabinet agreed to a number of proposals to strengthen governance, management and co-ordination arrangements in the intelligence community [DES Min (10) 1/1].

16. Those proposals have largely been implemented. The agencies have come together in a practical sense with the co-location in Pipitea House. The ICG has been established and joint NZIC planning and accountability documents (Statement of Intent and Four Year Budget Plans) have been prepared.

17. The NZIC has adopted a banner of "One Community, Many Agencies" to encapsulate the commitment to greater integration, and to meet broader government objectives relating to Better Public Services, value for money and moving to shared back office functions.

18. The objectives, functions, and powers of the NZSIS and GCSB were out of the scope of the Murdoch review.

Priorities for the New Zealand Intelligence Community

19. The report by Michael Wintringham "A National Security and Intelligence Framework for New Zealand" (September 2009) considered the NZIC's role in supporting a national security system. It provides a much more systematic framework for examining national security risks and prioritising work to mitigate them, including the NZIC's roles of watch and warn, reducing vulnerability and developing counter measures.

20. A set of national assessments were commissioned from the NAB-led National Assessments Committee, covering issues identified by Michael Wintringham as the key potential threats to national security and other broad issues impacting New Zealand's foreign policy. These proposed a set of overall priorities for the NZIC, which were subsequently endorsed by Cabinet in July 2012 [DES Min (12) 2/1]. They under pin the NZIC's activities in 2012 – 2016, shape decision making on resourcing and form the basis for mitigating those national security risks to New Zealand that can be informed by intelligence sources. The priorities agreed by Cabinet are set out in the table below.

Summary of Priorities for the New Zealand Intelligence Community	
Priority	**Topic**
High	• Intelligence support for deployed defence and law enforcement personnel • Cyber threats to New Zealand s6(a) • Espionage threat to New Zealand • Selective economic issues • New Zealand's maritime domain • Transnational organised crime threat to New Zealand

Medium	• Terrorism threat to New Zealand s6(a) [redacted] • Threat to New Zealand interests from proliferation of WMD
Low	• Threat to New Zealand from deliberate use of biological agents and pests • Threat to New Zealand of sabotage and subversion

[Not in Scope] [redacted]

GCSB compliance review and GCSB future needs and capabilities

23. GSCB has yet to undertake any detailed policy work on its future needs or capabilities. Work has been carried out on identifying potential areas of future need, particularly related to cyber security, but further consideration on how that relates to the role and functions of GCSB as set out in statute needs to be assessed.

24. In addition recent events (the Dotcom case) have given rise to concerns about GCSB's compliance with legislation and operational requirements. This has had a negative impact on public trust and confidence in the GCSB.

25. The Secretary of the Cabinet has been seconded to the GCSB to lead a compliance review. The purpose of the review is to provide assurance to the GCSB Director that the Bureau's activities are undertaken within its powers, and that adequate assurance and safeguards are in place.

Comment

Impetus for the NZIC policy and legislation review

26. The drivers of change in the background section above, can be summarised under four broad headings:

    - Compliance, safeguards and internal oversight
    - Future capabilities, functions and powers
    - Effectiveness of existing functions and powers
    - "One community" and greater integration

27. While there has been work undertaken on some of these matters, there are overlaps and connections that need to be addressed. For example, if new or more effective functions and powers are to be granted they will need to be supported by an adequate system of compliance, safeguards and internal oversight mechanisms.

28. The external oversight mechanisms, which cover both NZSIS and GCSB, have not been reviewed recently. In light of recent events relating to GCSB and in the context of considering the effectiveness of current functions and new functions I believe it is important to test whether the ISC Act and IGIS Act continue to be fit for purpose.

29. Consequently, given the relationship between all of these issues, I propose that they should be considered together in a single NZIC policy and legislation review. This will build on the Murdoch review which did not have in scope the issue of function and powers.

Scope of the review

30. The review will address the following matters:

Subject	Description
[Not in Scope]	
GCSB Act review	The GCSB Act review will include the objectives, functions and powers of the GCSB, and the current wording of s14 of the GCSB Act (which prohibits the interception of communications of New Zealand citizens and permanent residents). The findings of the compliance review, legal issues and other operational requirements will be taken into account. It will also consider the relationship to the recommendations of the NZSIS Act review.
Cyber security, cyber effects and other related capabilities	A number of issues have been raised in relation to the changing cyber environment, both in terms of intelligence activities, information assurance, "effects", cyber security and critical infrastructure protection. Providing services to

	the private sector and charging for protection services are also policy issues. The review will make recommendations on what changes need to be made to the GCSB and NZSIS Acts to address these emerging issues.
External oversight mechanisms	The ISC and IGIS Acts will be reviewed to consider whether they continue to be fit for purpose, or whether improvements could be made. It will also involve consideration of the role of the external oversight bodies in relation to internal oversight policies and processes.
Cooperation and collaboration	[Not in Scope] The review will focus on the relationship between the GCSB and other agencies (both domestic and international), and make recommendations to provide clarity about who can work with whom, on what. It will take into account the NZSIS Act review conclusions.
"One Community, Many Agencies"	The NZIC has decided to establish shared administrative services, and enable greater collaboration. The review will make recommendations for any legislative change required to facilitate this approach.

Manner of conducting the review

31. The review will be carried out by DPMC (ICG and the National Cyber Policy Office), GCSB and NZSIS. The review will be overseen by a Steering Committee with the following members:

    - Chief Executive of DPMC (chair)
    - Director, GCSB
    - Director, NZSIS
    - Director, ICG
    - Associate Director, GCSB/ Compliance reviewer.

32. Policy proposals will be considered by the Officials Committee on Domestic and External Security Coordination (ODESC) and made in close consultation with central agencies (Treasury and State Services Commission).

33. Consultation with government agencies and key stakeholders will be important, particularly in relation to the issues of agency support and cooperation, external oversight and cyber related matters.

34. Government agencies that will be consulted include the Ministry of Foreign Affairs and Trade, Ministry of Defence, New Zealand Defence Force, New Zealand Police, New Zealand Customs Service, Immigration New Zealand (MBIE), The Treasury, State Services Commission, and Ministry of Justice.

35. Other stakeholders that may need to be approached during the review include the Commissioner of Security Warrants, the Inspector-General of Intelligence and Security, the Privacy Commissioner, Chief Ombudsman, and Chief Human Rights Commissioner.

36. The review will also take into account related policy work in other portfolios, in particular the review of the Privacy Act 1993 and the review of the Telecommunications (Interception Capability) Act 2004.

Timeframes

37. To allow the NZIC to meet the priorities set by Cabinet, and align with the Budget cycle, enactment should occur by the end of 2013. Based on that end date the following timetable is proposed:

Milestone	Date
Cabinet policy approvals	By 30 April 2013
Introduction of amending legislation and first reading	By 30 June 2013
Report back by committee to House	By 31 October 2013
Final parliamentary stages	November – December 2013

38. This is a demanding timetable and will require the NZIC to prioritise its resources, and House time to be available at the relevant time.

Consultation

39. This paper was prepared by DPMC in consultation with NZSIS and GCSB.

40. The Treasury and the State Services Commission were informed.

Financial Implications

41. There are no financial implications arising from this paper. The cost of the review will be met from the baselines of DPMC, GCSB and NZSIS.

Human Rights

42. There are no human rights issues arising from this paper. Human rights and privacy considerations will be taken into account during the review.

Legislative Implications

43. There are no legislative implications arising from this paper, however the review will result in recommendations for legislative change.

44. There are three broad approaches to recommendations for legislative change.

a. Do nothing legislatively and focus on operational changes.
b. Make amendments to the existing Acts.
c. Repeal and replace the existing the Acts with a new legislative framework.

45. Doing nothing is not tenable given the drivers for change. The repeal and replace option raises a number of challenges, both in terms of the time required to complete the policy and drafting process, and the time it would take to take such a comprehensive bill through the parliamentary process. The needs of the NZIC are more immediate. Consequently I have instructed officials to proceed on the basis of implementing the outcome of the review through amendments to the existing Acts.

46. I propose to introduce an omnibus "Intelligence and Security Bill", which will contain all agreed amendments to the Acts requiring change. A bid will be prepared for the 2013 Legislation Programme, seeking a category 2 priority (must be passed in 2013). The final size and scale of the bill will depend on the recommendations of the review.

Select committee consideration

47. The ISC Act establishes the Intelligence and Security Committee (ISC). The ISC is a statutory committee, not a select committee established by the House. One of its core functions is to consider any bill or other matter relating to the NZSIS and GCSB that is referred to it by the House.

48. The membership of the ISC consists of the Prime Minister, Leader of the Opposition, two members of Parliament nominated by the Prime Minister (Hon John Banks and Hon Peter Dunne) and one member nominated by the Leader of the Opposition (Dr Russel Norman). The membership of the nominated members must be endorsed by the House. Members are senior Members of their respective Parties and have an understanding of the role and functions of the Intelligence Community.

49. The Act establishing the ISC sets out a framework which enables sensitive information to be disclosed to the Committee (where appropriate) while protecting classified information. It includes offences for inappropriate recording and use of information; a process requiring the relevant Chief Executive to consider whether "sensitive information" can be released to the ISC; and a qualified power for the Prime Minister to direct disclosure if desirable in the public interest. Proceedings of the ISC are, generally, to be held in private unless the ISC unanimously resolves to the contrary. The ISC is also required to have regard to security considerations in any report it makes to the House.

50. The normal process for an "Intelligence and Security Bill" would be to refer it to the ISC. The GCSB Act and all legislation amending the NZSIS Act have been considered by the ISC since it was established. The most significant advantage of this is that sensitive information explaining the policy decisions underpinning a bill can be put before the ISC with confidence because of the rules on how information is managed.

51. The process generally works well, but there are some practical considerations due to the requirements in the ISC Act. The ISC involves busy members of Parliament and it can be difficult to find a common time for them to hear submissions and conduct deliberations. Unlike select committees, the members cannot be substituted (in order to limit the distribution of classified information). The decision in 2011 for the ISC to call for and hear submissions on the NZSIS Bill in private was also subject to criticism by some

submitters and ISC members. These practical considerations could be addressed by careful planning of members' time and the ISC resolving to adopt select committee hearing processes as much as possible, which would assist in building trust and confidence with the public.

52. An alternative to the ISC would be to establish an ad hoc select committee. This would require a motion with notice to be debated and adopted by the House. The notice of motion can set out the membership (including who should be the chair, whether attendance can be delegated to a nominated alternate, and whether it should have a representative from all parties represented in the House) and any special powers and procedures that the select committee is to operate under which could vary Standing Orders. The main issue to address with this approach is whether sufficient protections could be placed around sensitive information, in terms of its presentation to the committee and what happens once the committee has reported to the House.

53. This approach would enable the practical considerations to be addressed, and support actions to build trust and confidence. It may also be appropriate for a committee other than the ISC to consider a bill if it contains changes to the ISC Act. Before considering such an approach, in the first instance, discussion with the Clerk of the House and consultation with other parties represented in the House would be required. Careful consideration would also need to be given to the ability of the NZSIS, in particular, to provide certain highly classified evidence to an ad hoc committee.

54. A further alternative would be to amend the ISC Act prior to referring a bill to it to address the practical considerations around membership (including who should be the chair, whether attendance can be delegated to a nominated alternate, and whether it should have a representative from all parties represented in the House). Such an amendment would either require a very short stand alone bill or inclusion in an existing bill that had sufficient scope to accommodate it. The benefit of this approach is that it would maintain the regime relating to sensitive information while addressing the practical considerations.

55. I will be considering how best to manage the parliamentary stages of amending legislation during the course of the review, taking into account the nature and scope of the final package of amendments. A final recommendation will be made in the papers seeking policy decisions.

Regulatory Impact Analysis

56. A Regulatory Impact Statement is not required for this paper as it does not seek decisions on policy options. Any future papers that make recommendations as a result of the review will include a regulatory impact analysis.

Publicity

57. I do not plan to make any public announcements about the content of this paper.

Recommendations

58. The Prime Minister recommends that the Committee:

1. **note** that the core New Zealand Intelligence Community comprises the New Zealand Security Intelligence Service, Government Communications Security Bureau, and the National Assessment Bureau, supported by the Intelligence Coordination Group;
2. **agree** that a review of policy and legislation relating to the core New Zealand Intelligence Community be undertaken;
3. **agree** that the review of policy and legislation will include:
    i. the existing review of the New Zealand Security Intelligence Service Act 1969;
    ii. a review of the Government Communications Security Bureau Act 2003;
    iii. a review of the functions and powers needed to address cyber security, cyber effects, critical infrastructure protection and other related capabilities;
    iv. a review of external oversight mechanism, in particular a review of the Intelligence and Security Committee Act 1996 and the Inspector-General of Intelligence and Security Act 1996;
    v. a review of the ability of intelligence agencies to collaborate and cooperate with other agencies under existing legislation;
    vi. an assessment of any legislative changes required to facilitate the commitment to "one community, many agencies";
4. **note** that the review will be undertaken by the Department of Prime Minister and Cabinet, the New Zealand Security and Intelligence Service and the Government Communications Security Bureau, and be funded from within their baselines;
5. **note** that a bid will be prepared for the 2013 Legislation Programme for a Intelligence and Security Bill with a category 2 priority (must be passed in 2013);
6. **note** that consideration will be given to the appropriate form of parliamentary consideration of the Bill.

Prime Minister

23 / 11 / 2012

10

File

Cabinet Committee on Domestic and External Security

DES Min (12) 3/1

Copy No: 15

Minute of Decision

New Zealand Intelligence Community Policy and Legislation Review

Portfolio: Prime Minister

On 26 November 2012, the Cabinet Committee on Domestic and External Security (DES):

1 **noted** that the core New Zealand Intelligence Community comprises the New Zealand Security Intelligence Service, the Government Communications Security Bureau, and the National Assessments Bureau, supported by the Intelligence Coordination Group;

2 **agreed** that a review of policy and legislation relating to the core New Zealand Intelligence Community be undertaken;

3 **noted** that the review of the policy and legislation could include:

3.1 the existing review of the New Zealand Security Intelligence Service Act 1969;

3.2 a review of the Government Communications Security Bureau Act 2003;

3.3 a review of the functions and powers needed to address cyber security, cyber effects, critical infrastructure protection and other related capabilities;

3.4 a review of external oversight mechanisms, in particular a review of the Intelligence and Security Committee Act 1996 and the Inspector-General of Intelligence and Security Act 1996;

3.5 a review of the ability of intelligence agencies to collaborate and cooperate with other agencies under existing legislation;

3.6 an assessment of any legislative changes required to facilitate the commitment to "one community, many agencies";

4 **directed** officials to report to DES on 5 December 2012 with further advice on the:

4.1 timeframe for undertaking the review and developing the Bill;

4.2 potential scope of the Bill, including the timing implications of different scope options;

5 **noted** that the review will be undertaken by the Department of the Prime Minister and Cabinet, the New Zealand Security Intelligence Service and the Government Communications Security Bureau, and be funded from within their baselines;

6 **noted** that a bid will be prepared for the 2013 Legislation Programme for an Intelligence and Security Bill (the Bill) with a category 2 priority (must be passed in 2013);

7 **noted** that consideration will be given to the appropriate form of parliamentary consideration of the Bill.

G. Carter

Gerrard Carter
Committee Secretary

Reference: DES (12) 4

Present:
Rt Hon John Key (Chair)
Hon Gerry Brownlee
Hon Steven Joyce
Hon Judith Collins
Hon Christopher Finlayson
Hon Anne Tolley
Hon Dr Jonathan Coleman
Hon Amy Adams

Officials present from:
Office of the Prime Minister
Department of the Prime Minister and Cabinet
New Zealand Security Intelligence Service
Government Communications Security Bureau
Crown Law Office

Distribution:
Cabinet Committee on Domestic and External Security Co-ordination
Office of the Prime Minister
18 Chief Executive, DPMC
19 Director, Security and Risk, DPMC
20 Director, Intelligence Coordination Group, DPMC
21 Director, National Assessments Bureau, DPMC
22 Director, NZSIS
23 Director, GCSB
24 Secretary to the Treasury
25 Solicitor-General
26 Secretary of Foreign Affairs and Trade
27 State Services Commissioner

Item 2

Cabinet

CAB (13) 7

Copy No: 24

Decisions of the Cabinet Committee on Domestic and External Security

18 January 2013

Report of the Cabinet Committee on Domestic and External Security: period ended 14 December 2012

The Committee met on 26 November 2012:

1 New Zealand Intelligence Community Policy and Legislation Review Pages 2-3
Portfolio: Prime Minister

[Not in Scope]

The Committee met on 11 December 2012:

1 New Zealand Intelligence Community Policy and Legislation Review Pages 4-5
Portfolio: Prime Minister

[Not in Scope]

Sam Gleisner
for Secretary of the Cabinet

The Cabinet Committee on Domestic and External Security met on 26 November 2012

s6(a)

1 **New Zealand Intelligence Community Policy and Legislation Review**
Portfolio: Prime Minister
DES Min (12) 3/1, DES (12) 4

The Committee:

1 **noted** that the core New Zealand Intelligence Community comprises the New Zealand Security Intelligence Service, the Government Communications Security Bureau, and the National Assessments Bureau, supported by the Intelligence Coordination Group;

2 **agreed** that a review of policy and legislation relating to the core New Zealand Intelligence Community be undertaken;

3 **noted** that the review of the policy and legislation could include:

3.1 the existing review of the New Zealand Security Intelligence Service Act 1969;

3.2 a review of the Government Communications Security Bureau Act 2003;

3.3 a review of the functions and powers needed to address cyber security, cyber effects, critical infrastructure protection and other related capabilities;

3.4 a review of external oversight mechanisms, in particular a review of the Intelligence and Security Committee Act 1996 and the Inspector-General of Intelligence and Security Act 1996;

3.5 a review of the ability of intelligence agencies to collaborate and cooperate with other agencies under existing legislation;

3.6 an assessment of any legislative changes required to facilitate the commitment to "one community, many agencies";

4 **directed** officials to report to DES on 5 December 2012 with further advice on the:

4.1 timeframe for undertaking the review and developing the Bill;

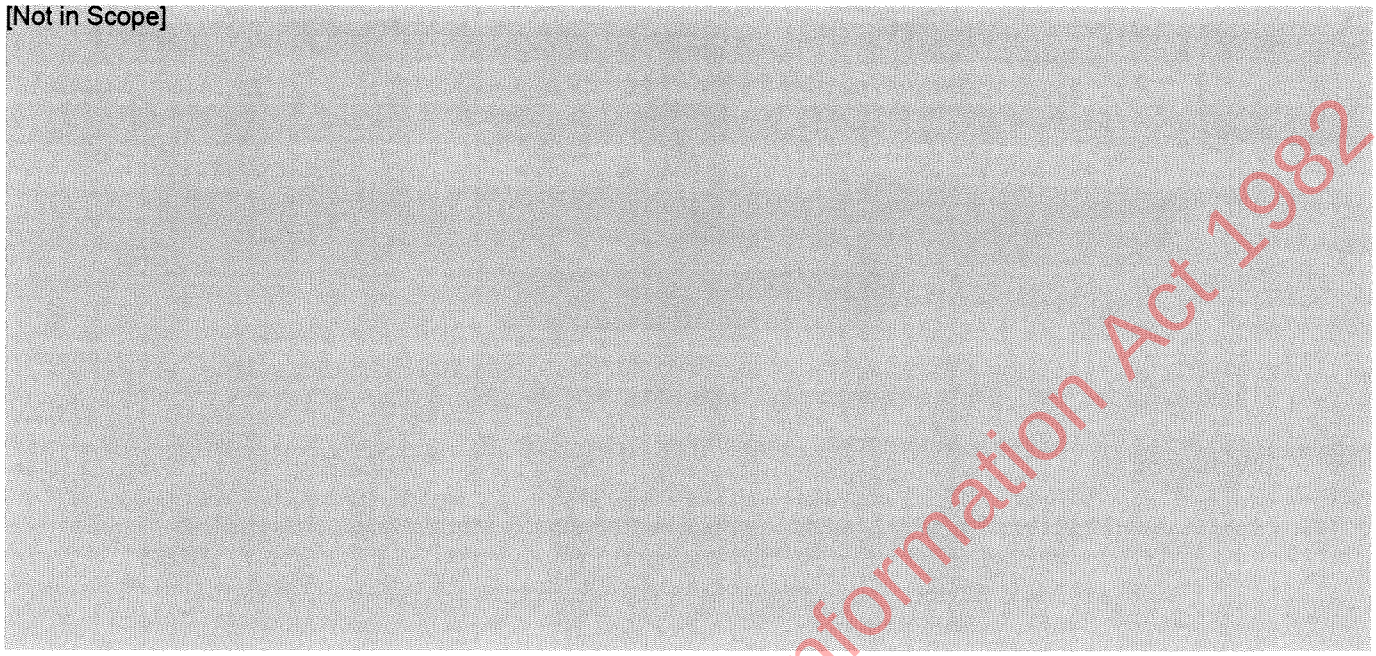
4.2 potential scope of the Bill, including the timing implications of different scope options;

5 **noted** that the review will be undertaken by the Department of the Prime Minister and Cabinet, the New Zealand Security Intelligence Service and the Government Communications Security Bureau, and be funded from within their baselines;

6 **noted** that a bid will be prepared for the 2013 Legislation Programme for an Intelligence and Security Bill (the Bill) with a category 2 priority (must be passed in 2013);

7 **noted** that consideration will be given to the appropriate form of parliamentary consideration of the Bill.

[Not in Scope]



The Cabinet Committee on Domestic and External Security met on 11 December 2012

SECRET

1 New Zealand Intelligence Community Policy and Legislation Review [Not in Scope]

Portfolio: Prime Minister

DES Min (12) 4/1/-1 [Not in Scope]

The Committee, having taken Power to Act in accordance with its terms of reference:

Background

1 **noted** that the core New Zealand Intelligence Community comprises the New Zealand Security Intelligence Service, the Government Communications Security Bureau, and the National Assessments Bureau, supported by the Intelligence Coordination Group;

Policy and legislation review

2 **agreed** that a review of policy and legislation relating to the core New Zealand Intelligence Community be undertaken;

3 **agreed** that the review of the policy and legislation include:

3.1 the existing review of the New Zealand Security Intelligence Service Act 1969;

3.2 a review of the Government Communications Security Bureau Act 2003;

3.3 a review of the functions and powers needed to address cyber security, cyber effects, critical infrastructure protection and other related capabilities;

3.4 a review of external oversight mechanisms, in particular a review of the Intelligence and Security Committee Act 1996 and the Inspector-General of Intelligence and Security Act 1996;

3.5 a review of the ability of intelligence agencies to collaborate and cooperate with other agencies under existing legislation;

3.6 an assessment of any legislative changes required to facilitate the commitment to "one community, many agencies";

4 **noted** that the review will be undertaken by the Department of the Prime Minister and Cabinet, the New Zealand Security Intelligence Service and the Government Communications Security Bureau, and be funded from within their baselines;

Legislative process

5 **agreed** that a bid for the 2013 Legislation Programme be prepared for an Intelligence and Security Bill with a category 2 priority (must be passed in 2013);

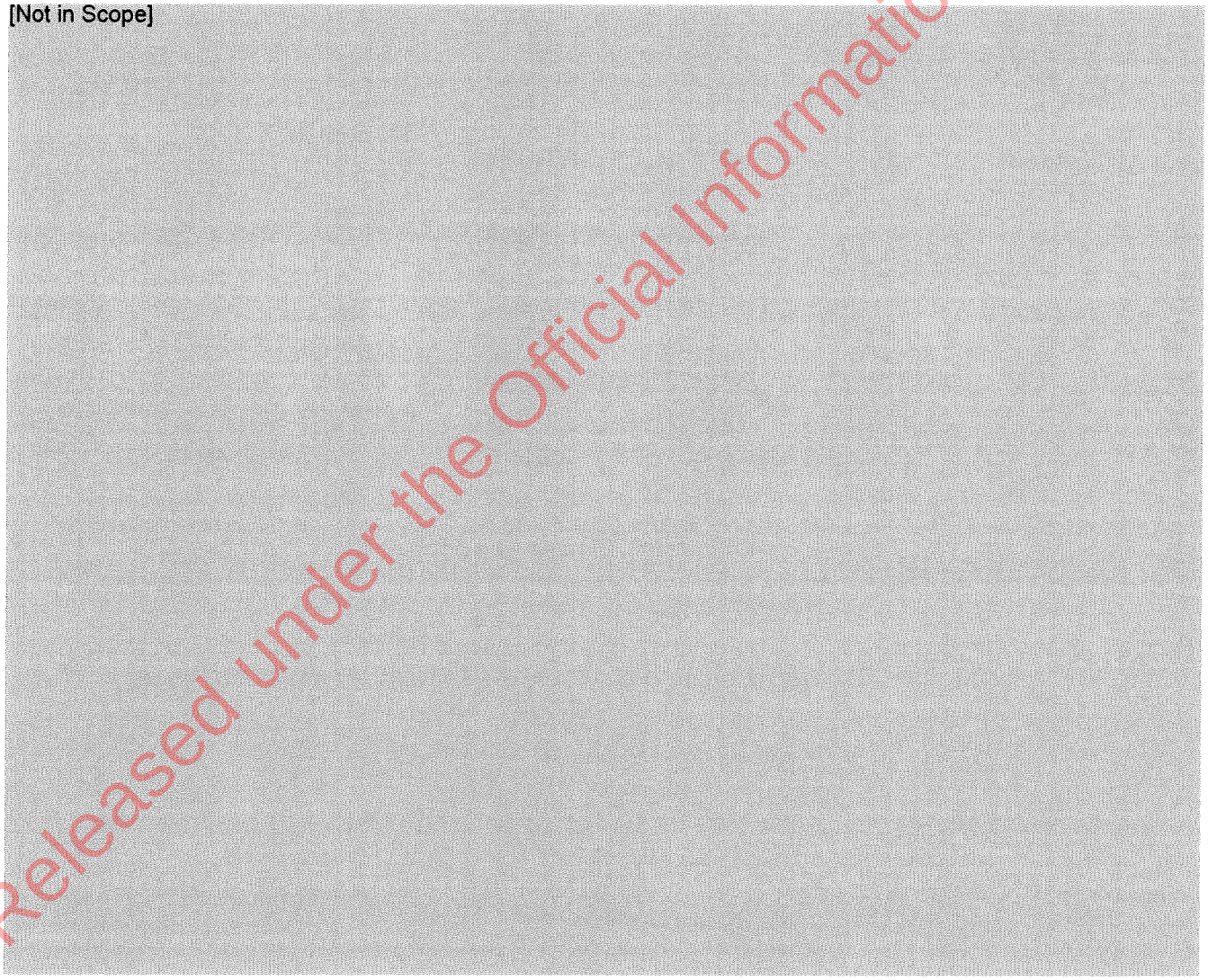
[Not in Scope]

7 **noted** that the Business Committee's agreement may be sought to treat the two bills referred to in paragraphs 5 and 6 above as cognate bills for their first, second and third readings;

8 **noted** that the bills will be enacted by August 2013;

9 **noted** that further consideration will be given to the appropriate form of parliamentary consideration of the bills.

[Not in Scope]



[One additional pages not in scope removed]

Legislative process

[Not in Scope]

14 **noted** that:

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

14.2 the Business Committee's agreement may be sought to treat the two bills referred to in paragraph 13 and 14.1 above as cognate bills for their first, second and third readings;

14.3 the bills will be enacted by August 2013.

File

Cabinet

CAB Min (13) 1/5

Copy No: 4

Minute of Decision

Report of the Cabinet Committee on Domestic and External Security: Period Ended 14 December 2012

On 23 January 2013, Cabinet made the following decisions on the work of the Cabinet Committee on Domestic and External Security (DES) for the period ended 14 December 2012 (covering the meetings of DES on 26 November and 11 December):

DES Min (12) 3/1 **New Zealand Intelligence Community Policy and Legislation Review** CONFIRMED
Portfolio: Prime Minister

[Not in Scope]

DES Min (12) 4/1-1 **New Zealand Intelligence Community Policy and Legislation Review** CONFIRMED
Portfolio: Prime Minister

[Not in Scope]

for Secretary of the Cabinet

Reference: CAB (13) 7

Distribution: (see over)

Distribution:

1 Prime Minister
7 Chief Executive, DPMC
8 Director, Security and Risk, DPMC
9 Director, Intelligence Coordination Group, DPMC
10 Director, National Assessments Bureau, DPMC
11 Director, NZSIS
12 Director, GCSB
13 Minister of Finance
14 Secretary to the Treasury
15 Attorney-General
16 Solicitor-General
17 Minister of Foreign Affairs
18 Secretary of Foreign Affairs and Trade
19 Minister of State Services
20 State Services Commissioner
21 Secretary of Defence
22 Chief of Defence Force
23 Minister for Communications and Information Technology
24 Chief Executive, MBIE (Communications and IT)
25 Chief Parliamentary Counsel
26 s6(a)

2 s6(a)
3 s6(a)
4 File
5 Meeting File
6 Meeting File

Item 3

DES (12) 5

Cabinet Committee on Domestic and External Security

Copy No:

Summary of Paper

7 December 2012

This document contains information for the New Zealand Cabinet. It must be treated in confidence and handled in accordance with any security classification, or other endorsement. The information can only be released, including under the Official Information Act 1982, by persons with the appropriate authority.

New Zealand Intelligence Community Policy and Legislation Review

[Not in Scope]

The Chair of the Cabinet Committee on Domestic and External Security (DES) has requested the attached documents be circulated for consideration at the DES meeting on 11 December 2012.

The documents attached below this cover sheet include:

- a cover note from the Chair of the Officials Committee on Domestic and External Security;
- an A3 on the New Zealand Intelligence Community Policy and Legislation Review;

[Not in Scope]

A summary of the recommendations are set out on pages 7-8 of the cover note.

Sam Gleisner
Committee Secretary

Distribution:
Cabinet Committee on Domestic and External Security
Office of the Prime Minister
Chief Executive, DPMC
Director, Security and Risk, DPMC
Director, Intelligence Coordination Group, DPMC
Director, National Assessments Bureau, DPMC
Director, NZSIS
Director, GCSB
Secretary to the Treasury
Solicitor-General
Secretary of Foreign Affairs and Trade
State Services Commissioner

DEPARTMENT
of the PRIME MINISTER
and CABINET

7 December 2012

Prime Minister

NZIC Policy and Legislation Review [Not in Scope]

Introduction

Attached for discussion at the DES meeting to be held on 11 December are:

- an A3 on the NZIC Policy and Legislation Review;
- [Not in Scope]

These papers attempt to bring together two separate but related workstreams for Ministers so that they can both be considered as an integrated package and advanced to legislation together.

I **recommend** that you:

1. refer these papers to Ministers ahead of the DES meeting on 11 December.
2. invite officials at the meeting to speak first to the NZIC Policy and Legislation Review paper.

[Not in Scope]

4. invite discussion of the options to progress.
5. note officials' recommendations to DES, as set out in this overview paper.

NZIC: Policy and Legislation Review

The NZSIS has been developing necessary updates to its role and functions to reflect contemporary threats to national security and ways of mitigating the risks these threats pose. Changes to the NZSIS Act are also required to address gaps in powers and capabilities and to modernise administrative arrangements. This policy and legislative work is well advanced.

The GCSB has also been considering potential areas of future need, particularly in the area of cyber security and in light of new and emerging telecommunications technologies. However, related policy and legislative work has yet to be undertaken. In addition, recent events have given rise to concerns about GCSB's compliance framework, the suitability of its legislation and operational processes. A compliance review is underway, which may identify other areas for policy work and potential legislative amendment. One area of focus may be how GCSB supports and cooperates with other government agencies.

548752v1

Executive Wing, Parliament Buildings, Wellington, New Zealand 6011
☎ 64 4 817 9700 Facsimile 64 4 472 3181 www.dpmc.govt.nz

Work undertaken by the NZIC regarding functions and powers raises the question of whether the external oversight mechanisms (the Intelligence and Security Committee and Inspector-General of Intelligence and Security) are suitably effective and robust.

Given the relationship between these issues, the proposal is to bring these issues together in a single NZIC policy and legislation review, carried out by DPMC, NZSIS and GCSB.

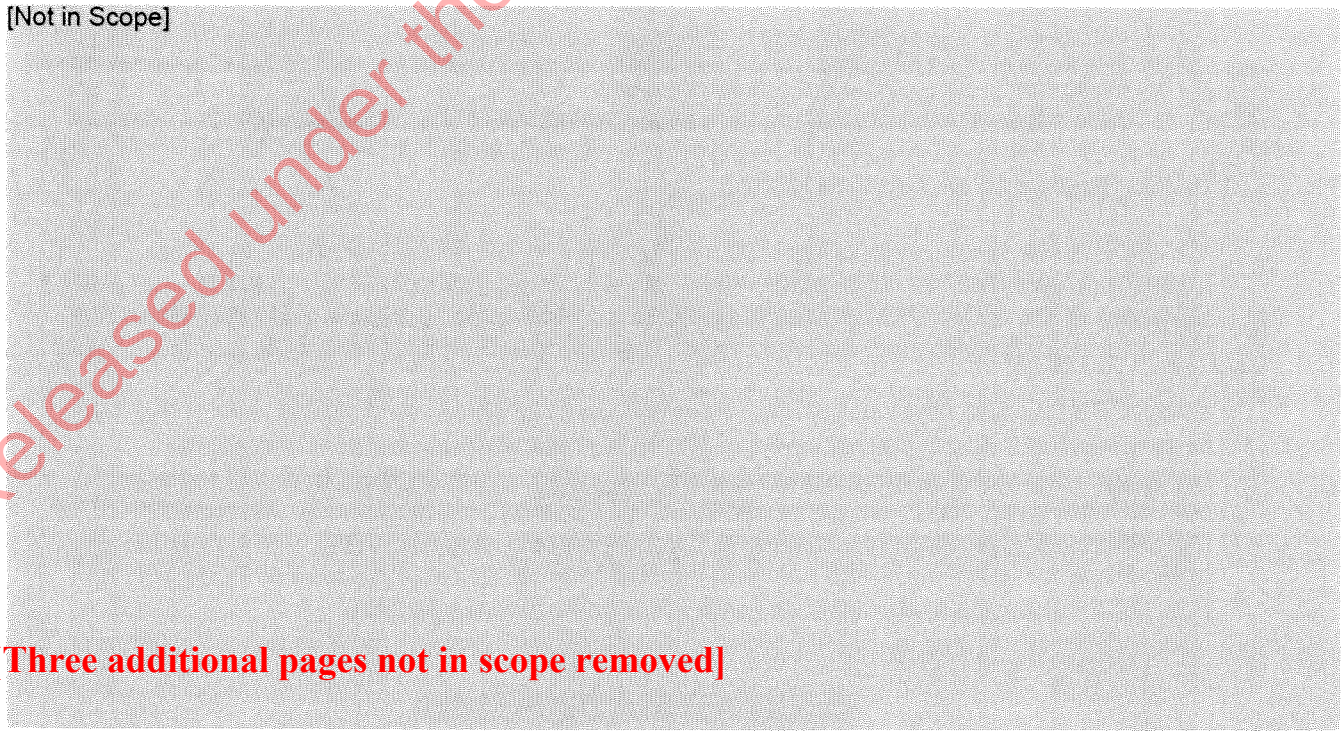
Officials outlined this NZIC work to DES on 26 November [CAB Min (12) 3/1 refers], including a proposed end of 2013 enactment timetable. Ministers sought advice on a shorter timeframe and the impact that would have on the scope of the review. The A3, attached as Annex 1, provides a basis to discuss a reduction in scope to achieve enactment by the end of July 2013. The main reduction in scope from the Cabinet paper is the work on "One Community, Many Agencies". Please note, however, the GCSB compliance and legal review is still underway and further issues may be identified which may impact on the timeframe and/or scope.

Officials have looked to tighten the proposed scope of the legislation as much as possible whilst still addressing the serious issues identified.

We recommend the Committee:

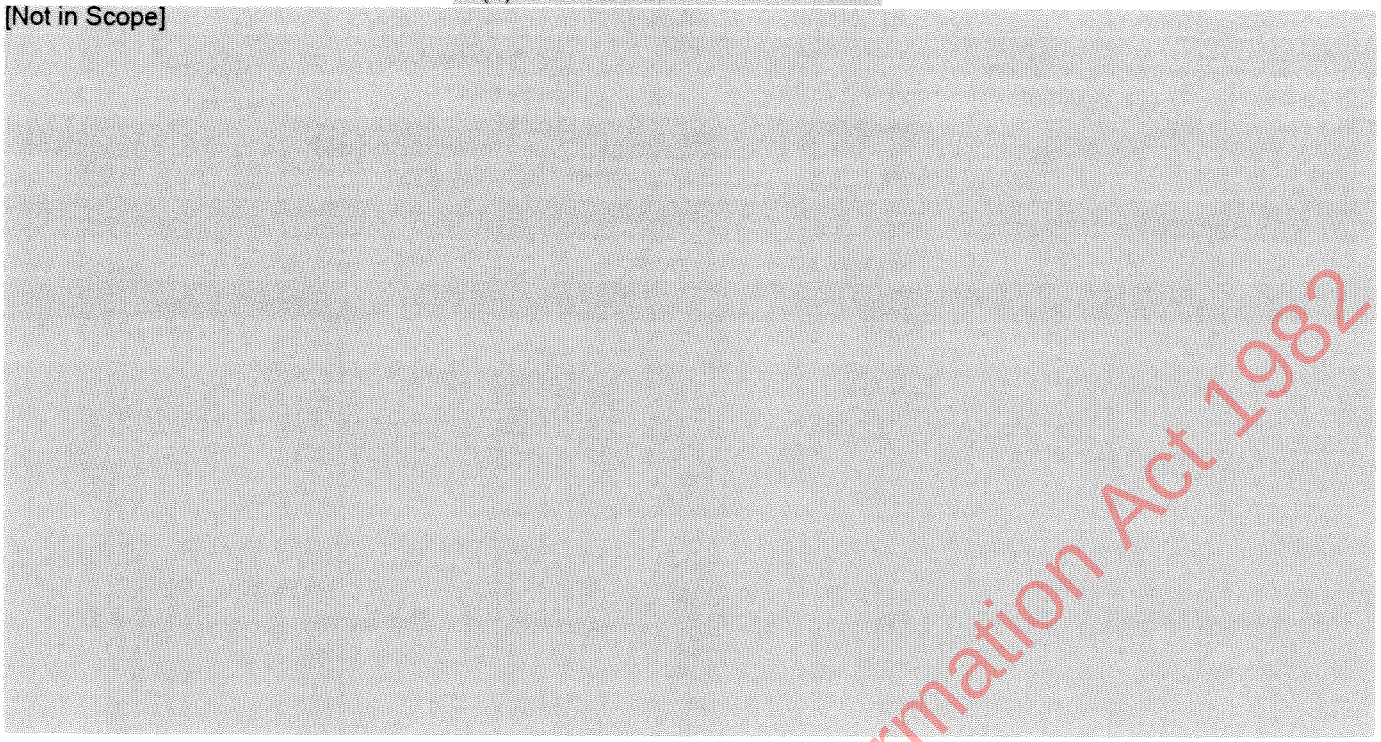
6. agree the scope of the proposed Intelligence and Security Bill include:
   - the existing review of the NZSIS Act;
   - a review of the GCSB Act;
   - a review of the ability of intelligence agencies to assist and cooperate with other agencies under existing legislation;
   - a review of external oversight mechanisms; and
   - a review of the functions and powers needed to protect designated organisations (including government and private sector) from advanced cyber intrusions and to develop related cyber capabilities.
7. agree the timeframe for enacting the proposed Intelligence and Security Bill covering this scope is by the end of July 2013 (see also the discussion of legislative options below).

[Not in Scope]



[Three additional pages not in scope removed]

[Not in Scope]



Next Steps: Policy and Legislative Processes

The principal questions to be considered here relate to timeframes and legislative vehicles.

There are significant advantages in advancing the NZIC work and the telecommunications work together. This would enable a single conversation to be had with key constituencies, focused on the significant security and law enforcement impacts of technological change and the need for modern, effective and proportionate responses to this. There may, however, be a requirement for different forms of consultation process around each of the proposals. For example there may be a need for a more extensive consultation with industry around the TICA package. As a consequence, introducing cognate bills that can be represented by different agencies, and can progress at similar speeds or, if necessary, be decoupled, may be the best way to proceed.

We recommend the Committee:

20. agree two cognate Bills be prepared that can, ideally, share the same passage through the House, or be de-coupled if necessary.

Summary of Recommendations

Officials recommend that you:

Process

1. refer these papers to Ministers ahead of the DES meeting on 11 December.

2. invite officials at the meeting to speak first to the NZIC Policy and Legislation Review paper.

[Not in Scope]

4. invite discussion of the options to progress.

5. note officials' recommendations to DES, as set out in this overview paper.

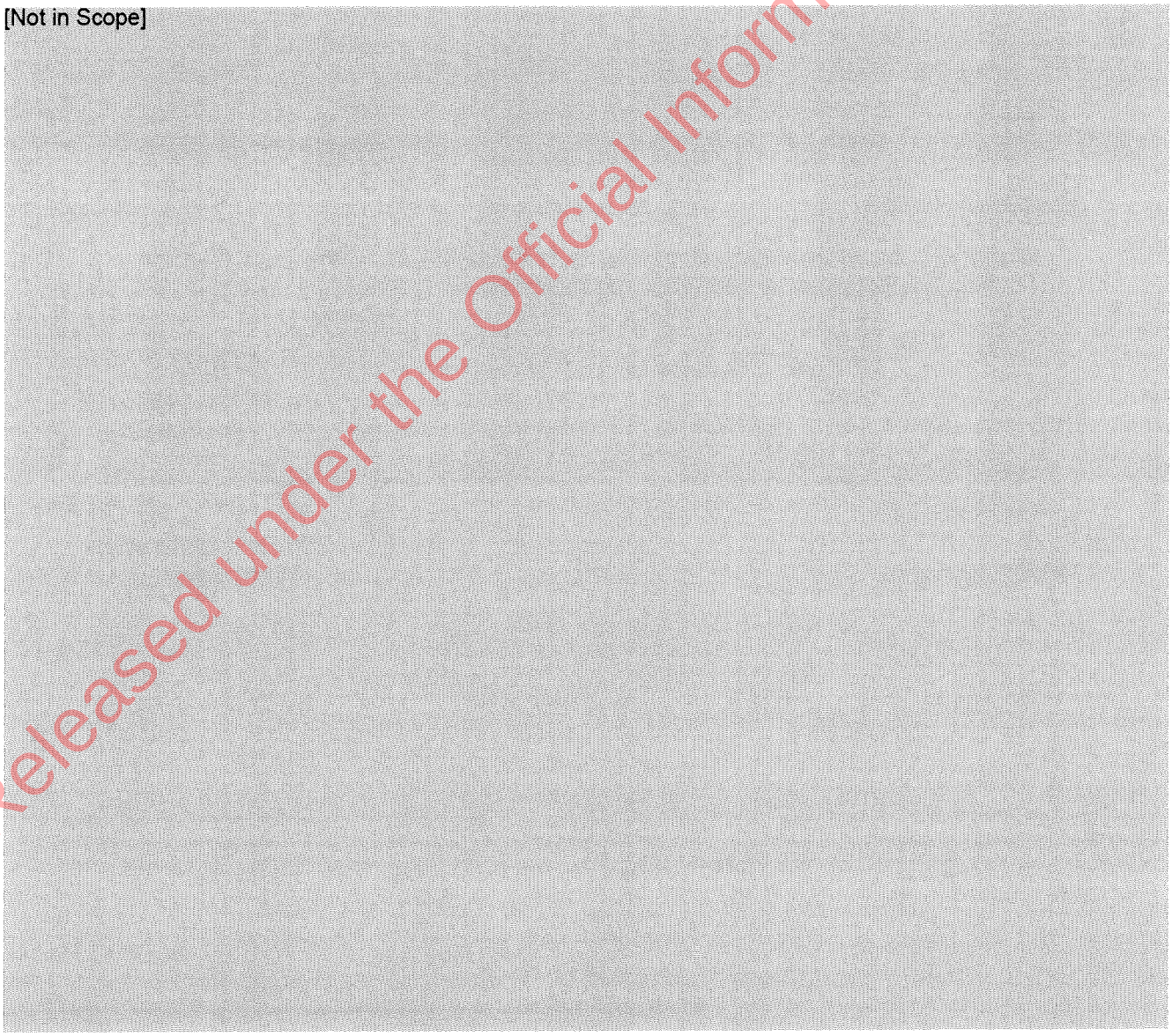
Officials recommend that Committee:

NZIC legislation

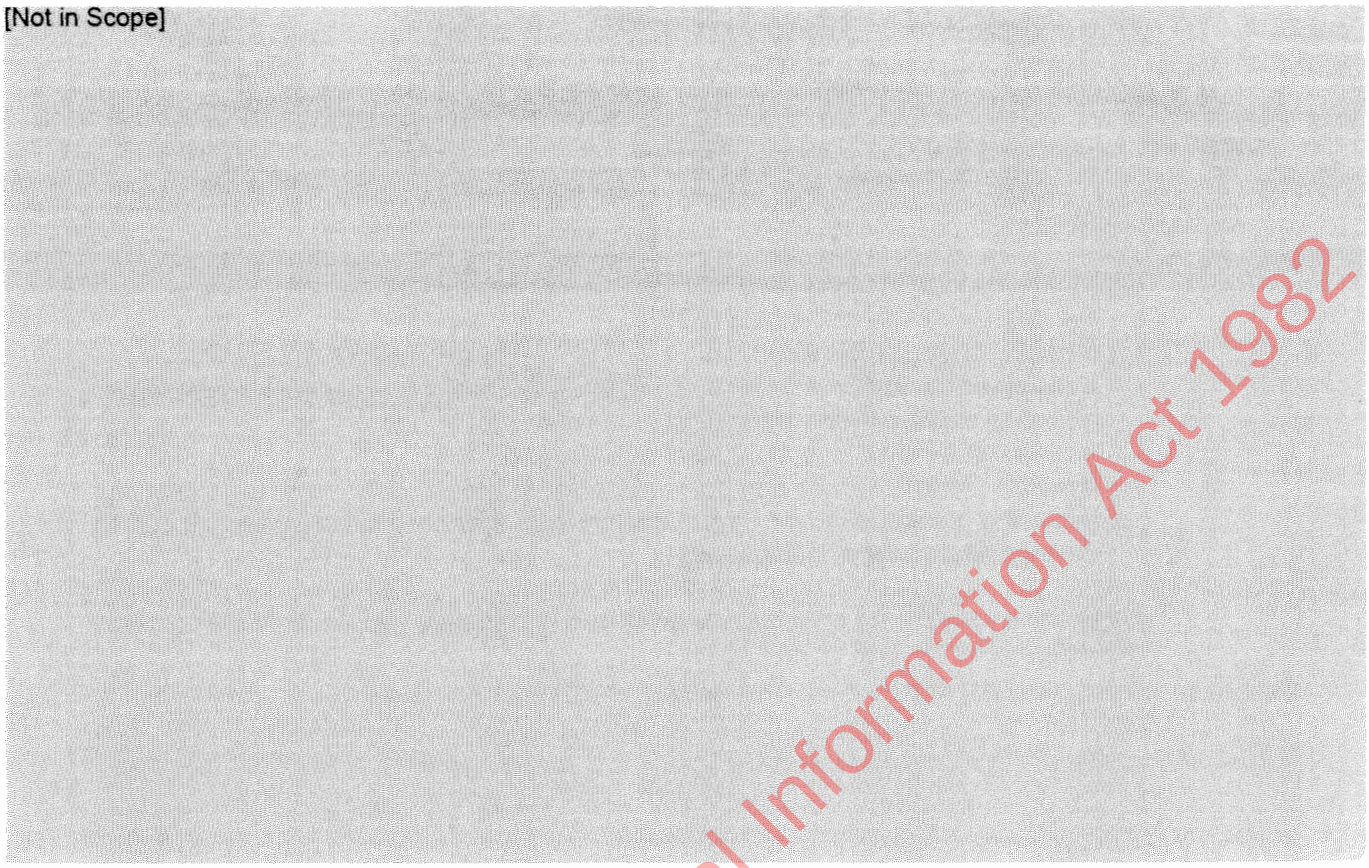
6. agree the scope of the proposed Intelligence and Security Bill include:
   - the existing review of the NZSIS Act;
   - a review of the GCSB Act;
   - a review of the ability of intelligence agencies to assist and cooperate with other agencies under existing legislation;
   - a review of external oversight mechanisms; and
   - a review of the functions and powers needed to protect designated organisations (including government and private sector) from advanced cyber intrusions and to develop related cyber capabilities.

7. agree the timeframe for enacting the proposed Intelligence and Security Bill covering this scope is by the end of July 2013.

[Not in Scope]



[Not in Scope]



Legislative process

20. agree two cognate Bills be prepared that can, ideally, share the same passage through the House, or be de-coupled if necessary.

Andrew Kibblewhite
Chair
ODSEC

Refer Yes / No

Rt Hon John Key
Prime Minister

s6(a)

NZIC POLICY AND LEGISLATION REVIEW

SCOPE

[Not in Scope]

2.
GCSB Act Review
Cooperation & Assistance
Oversight, Cyber Issues

In priority order from essential to highly recommended:

- Review the functions and powers of GCSB to address compliance and legal issues, and meet government intelligence priorities
- Consider GCSB's ability to assist other agencies in performing their lawful functions
- Review application of s14 (prohibiting interception of New Zealanders' communications) to the information assurance function and when assisting other agencies
- Ensure oversight mechanisms are fit for purpose and support public trust and confidence in NZIC
- Update powers to take advantage of new technology to deliver foreign intelligence and information assurance functions
- Enable GCSB to protect designated organisations (including government and private sector) from advanced cyber intrusions
- Provide for capabilities extending beyond immediate cyber defence s6(a)

ESSENTIAL → HIGHLY RECOMMENDED

+

3.
"One Community, Many Agencies"

- Enhance ability to meet broader Government objectives (Better Public Services, value for money and shared back office services)
- Enable greater workforce mobility

Note: Can achieve some elements through administrative mechanisms

DISCRETIONARY

+

OR

4.
Single Agency and Act

- Fully address all issues and concerns as a single package
- Would enable merger of agencies
- Would require total repeal and replacement of legislation
- Could fail to re-enact some fundamental existing powers and functions

Note: Legislative process would take until at least 2014

NOT RECOMMENDED

TIMEFRAME FOR ITEMS 1 AND 2

	February	March	April	May	June	July
Option 1: Recommended		By 31 March: Cabinet policy decision	By 30 April: Legislation drafted and approval to introduce	6 May: Introduction 9 May: First reading 14 May: Call for submissions	7 June: Submissions close 10-14 June: Hear submissions	By 5 July: Report back 11 July: Second Reading 30-31 July: Committee of the Whole and Third Reading
Option 2: Higher Risk	By 28 February: Cabinet policy decision	By 31 March: Legislation drafted and approval to introduce	8 April: Introduction 11 April: First reading 15 April: Call for submissions	10 May: Submissions close 13-17 May: Hear submissions	By 7 June: report back 13 June: Second Reading 25-27 June: Committee of the Whole and Third Reading	

Note: GCSB compliance and legal review still underway. Further issues may be identified, which could impact on timeframes and/or scope.

[Two additional pages not in scope removed]

s6(a)

Cabinet Committee on Domestic and External Security

DES Min (12) 4/1-1

Copy No: 50

Minute of Decision

[Note: Minute paper reference corrected to read as "DES (12) 5" 12/04/16.]

New Zealand Intelligence Community Policy and Legislation Review

Portfolio: Prime Minister

On 11 December 2012, the Cabinet Committee on Domestic and External Security (DES), having taken Power to Act in accordance with its terms of reference:

Background

1 **noted** that the core New Zealand Intelligence Community comprises the New Zealand Security Intelligence Service, the Government Communications Security Bureau, and the National Assessments Bureau, supported by the Intelligence Coordination Group;

Policy and legislation review

2 **agreed** that a review of policy and legislation relating to the core New Zealand Intelligence Community be undertaken;

3 **agreed** that the review of the policy and legislation include:

3.1 the existing review of the New Zealand Security Intelligence Service Act 1969;

3.2 a review of the Government Communications Security Bureau Act 2003;

3.3 a review of the functions and powers needed to address cyber security, cyber effects, critical infrastructure protection and other related capabilities;

3.4 a review of external oversight mechanisms, in particular a review of the Intelligence and Security Committee Act 1996 and the Inspector-General of Intelligence and Security Act 1996;

3.5 a review of the ability of intelligence agencies to collaborate and cooperate with other agencies under existing legislation;

3.6 an assessment of any legislative changes required to facilitate the commitment to "one community, many agencies";

4 **noted** that the review will be undertaken by the Department of the Prime Minister and Cabinet, the New Zealand Security Intelligence Service and the Government Communications Security Bureau, and be funded from within their baselines;

Legislative process

5 **agreed** that a bid for the 2013 Legislation Programme be prepared for an Intelligence and Security Bill with a category 2 priority (must be passed in 2013);

[Not in Scope]

7 **noted** that the Business Committee's agreement may be sought to treat the two bills referred to in paragraphs 5 and 6 above as cognate bills for their first, second and third readings;

8 **noted** that the bills will be enacted by August 2013;

9 **noted** that further consideration will be given to the appropriate form of parliamentary consideration of the bills.

Sam Gleisner
Committee Secretary

Reference: DES (12) 5

Present:
Rt Hon John Key (Chair)
Hon Bill English
Hon Gerry Brownlee
Hon Steven Joyce
Hon Judith Collins
Hon Christopher Finlayson
Hon Anne Tolley
Hon Dr Jonathan Coleman
Hon Amy Adams

Officials present from:
Office of the Prime Minister
Department of the Prime Minister and Cabinet
New Zealand Security Intelligence Service
Government Communications Security Bureau

Distribution:
Cabinet Committee on Domestic and External Security Co-ordination
Office of the Prime Minister
Chief Executive, DPMC
Director, Security and Risk, DPMC
Director, Intelligence Coordination Group, DPMC
Director, National Assessments Bureau, DPMC
Director, NZSIS
Director, GCSB
Secretary to the Treasury
Solicitor-General
Secretary of Foreign Affairs and Trade
State Services Commissioner
Chief Parliamentary Counsel
Legislation Coordinator

#51 s6(a) Nat Security - viewed & returned (8.4.16)

File

Item 4

Cabinet Committee on Domestic and External Security

DES (13) 5

Copy No: 15

Summary of Paper

15 February 2013

New Zealand Intelligence Community Policy and Legislation Review: Overview

Portfolio	Prime Minister
Purpose	This paper provides background and context for the suite of four papers on the outcome of the review of the New Zealand Security and Intelligence Service Act 1969 (the NZSIS Act). This paper should be read in conjunction with the related papers under DES (13) 1, DES (13) 2, DES (13) 3 and DES (13) 4.
Previous Consideration	In December 2012, the Cabinet Committee on Domestic and External Security agreed that a review of policy and legislation relating to the core New Zealand Intelligence Community (NZIC) be undertaken [DES Min (12) 4/1-1];
Summary	The key issues underpinning the review of the NZIC legislation are: • the changing security environment (discussed on pages 2-3); • the cyber environment and information security (page 3-4); • the changing public law environment (page 4); • maintaining public confidence through external oversight (pages 4-5). The four papers on the outcome of the review of the NZSIS Act, for consideration in conjunction with this paper, are the first set of papers on the NZIC Policy and Legislation Review (the Review).
Regulatory Impact Analysis	A Regulatory Impact Statement is not required.
Baseline Implications	None.
Legislative Implications	None as a result of this paper. The review will result in recommendations for legislative change.

Timing Issues The following is the anticipated timing of key steps in the review of NZIC legislation:

[Not in Scope]

- policy approvals for the GCSB Act review and review of external oversight: 26 March 2013
- approval to introduce legislation: Week of 6 May 2013
- introduction of legislation: By 9 May 2013

Announcement DPMC and the Office of the Prime Minister are considering the approach to announcing the preparation and introduction of legislation.

Consultation Paper prepared by ICG (DPMC). NZSIS and GCSB were consulted.

The Prime Minister indicates that discussion is not required with the government caucus or with other parties represented in Parliament.

The Prime Minister recommends that the Committee:

1 note that in December 2012, the Cabinet Committee on Domestic and External Security agreed that a review of policy and legislation relating to the core New Zealand Intelligence Community be undertaken (the review) [DES Min (12) 4/1-1];

[Not in Scope]

3 note that proposals to amend the Government Communications Security Bureau Act 2003 (the GCSB Act) and the oversight arrangements will be submitted in due course;

4 note the following anticipated timetable for the review:

[Not in Scope]

4.2 policy approvals for the GCSB Act review and review of external oversight: 26 March 2013

4.3 approval to introduce legislation: Week of 6 May 2013

4.4 introduce amending legislation: By 9 May 2013

5 note that consideration is being given to:

5.1 the appropriate form of parliamentary consideration of the bill to amend the New Zealand Security Service Act 1969;

5.2 the announcement of the preparation and introduction of the bill;

5.3 the provision of information to stakeholders in light of the security classification of certain information.

Sam Gleisner
Committee Secretary

Distribution:
Cabinet Committee on Domestic and External Security
18 Office of the Prime Minister
19 Chief Executive, DPMC
20 Director, Security and Risk, DPMC
21 Director, Intelligence Coordination Group, DPMC
22 Director, NZSIS
23 Director, GCSB

Office of the Prime Minister

Cabinet Domestic and External Security Committee

NEW ZEALAND INTELLIGENCE COMMUNITY POLICY AND LEGISLATION REVIEW: OVERVIEW

Proposal

1. The purpose of this paper is to provide the background and context for the NZSIS suite of Cabinet papers, which is the first set of papers from the New Zealand Intelligence Community Policy and Legislation Review to be considered by the Committee.

Executive Summary

2. The core New Zealand Intelligence Community (NZIC) comprises three key agencies together with the Intelligence Coordination Group (ICG), which is located in the Department of Prime Minister and Cabinet (DPMC):

    a. the New Zealand Security Intelligence Service (NZSIS);
    b. the Government Communications Security Bureau (GCSB); and
    c. the National Assessments Bureau (NAB), which is located in DPMC.

3. The key reason for reviewing the legislation governing the NZSIS and GCSB is that their powers need to be modernised to equip them to meet the changing security environment, particularly threats in cyberspace. Their oversight also needs to be strengthened given the intrusive powers they exercise.

4. These papers will be followed by papers on GCSB and on the oversight regime for the intelligence agencies in late March, with the objective of introducing amending legislation in early May.

Background

5. On 11 December 2012 the Cabinet Committee on Domestic and External Security (DES) agreed that a review of the policy and legislation relating to the core New Zealand Intelligence Community be undertaken. The scope of the Review would include [DES Min (12) 4/1-1]:

[Not in Scope]

- A review of the GCSB Act;
- A review of the functions and powers needed to address cyber security, cyber effects, critical infrastructure protection and other related capabilities;
- A review of external oversight mechanisms, in particular a review of the Intelligence and Security Committee Act 1996 and the Inspector General of Intelligence and Security Act 1996;
- A review of the ability of intelligence agencies to assist and cooperate with other agencies under existing legislation;

- An assessment of any legislative changes required to facilitate the commitment to "one community, many agencies".

Comment

6. The key issues underpinning the review of the NZIC legislation can be summarised under four headings:

   - Changing security environment;
   - Cyber environment and information security;
   - Changing public law environment;
   - Maintaining public confidence through external oversight.

7. Each of these issues is discussed below. Taken together they require the functions and powers of the NZSIS and GCSB to be reviewed with a view to amendment or addition so that the government can respond to the security threats facing New Zealand.

8. In undertaking this review and developing recommended changes, respect for human rights and individual privacy, and the importance of free speech in New Zealand are guiding principles. However, legislation for intelligence agencies involves conferring on them intrusive powers beyond those normally exercised by government agencies and some qualifications to these basic principles need to be considered. The approach being taken by the review is that any qualifications must be shown to be necessary, and that functions and powers must operate within a framework of a carefully formulated and consistent policy along with robust external oversight mechanisms.

Changing security environment

9. The security environment facing New Zealand today presents new challenges. Security issues are increasingly interconnected and national borders are less meaningful. Globalisation means that New Zealand is no longer as distant from security problems as it was in the past, shown most clearly in the domain of cyberspace. Threats arise from non-state actors such as terrorist groups and transnational criminals.

s6(a)

10. In 2012 Cabinet considered ten national assessment papers prepared by the National Assessments Committee addressing the major security risks to New Zealand. The purpose of these papers was to provide a basis to prioritise those risks and consequently guide the allocation of resources by the NZIC. The priorities agreed by Cabinet [DES Min (12) 2/1] are set out in the table below.

Summary of Priorities for the New Zealand Intelligence Community

Priority	Topic
High	• Intelligence support for deployed defence and law enforcement personnel • Cyber threats to New Zealand s6(a) • Espionage threat to New Zealand • Selective economic issues • New Zealand's maritime domain • Transnational organised crime threat to New Zealand
Medium	• Terrorism threat to New Zealand s6(a) • Threat to New Zealand interests from proliferation of weapons of mass destruction (WMD)
Low	• Threat to New Zealand from deliberate use of biological agents and pests • Threat to New Zealand of sabotage and subversion

The priorities agreed by Cabinet highlight the changes in the national security environment which mean the legislation governing the NZSIS and GCSB needs review and amendment. The national security environment is more complex than when those agencies' current functions and powers were established. The need to mitigate cyber threats, provide support to deployed defence and law enforcement personnel, and intelligence on economic issues are new and are continuing to grow in importance. Yet issues that once predominated such as terrorism and proliferation of WMDs have not gone away. The NZSIS Act and the GCSB Act were largely enacted and amended to address issues and threats relating to the Cold War threat environment when subversion and espionage were the major concerns. [Not in Scope] The GCSB Act was enacted at a time when terrorism was of high importance and has not been amended since. In particular neither act addresses the security challenges posed by cyberspace.

Cyber environment and information security

11. The innovation and greater shift of activity of both business and government to the cyber environment is a particular issue. It is not only government information that is subject to espionage/theft or even interference by other states, cybercriminals and issue motivated groups. Major New Zealand companies have been subject to cyber intrusions and IP theft by foreign states.

12. The Government has responded by launching the Cyber Security Strategy in June 2011, which includes a range of actions. However, the current laws mean that GCSB and NZSIS are unable to fully address security threats in this environment. For example, in

the GCSB Act very little is said about information security and the assistance that it can provide is focused on government agencies.

13. GCSB is uniquely placed with its advanced capabilities developed through its intelligence work to contribute to responses to cyber security issues. That is why, as part of the Cyber Security Strategy, the National Cyber Security Centre was created within the GCSB. However, the implementation of the NCSC has highlighted limitations on the ability of GCSB to contribute to this work.

14. In a small jurisdiction such as New Zealand we cannot afford to duplicate expensive and sophisticated assets, and there are limited numbers of people who can work with such assets. Consistent with the Better Public Services programme, the capabilities such as those developed or acquired by the GCSB, where appropriate and subject to necessary safeguards, need to be made available to meet Government priorities.

Changing public law environment

15. The legal environment in which the GCSB Act and NZSIS Act are interpreted has also developed since their enactment. The enactment of the New Zealand Bill of Rights Act 1990 has resulted in a number of cases over the years that have reviewed the exercise of intrusive powers by Crown agents (largely the NZ Police). These cases, while not directly on point, do give rise to matters that impact on the interpretation of the functions and powers of the GCSB and NZSIS.

16. The cases decided by the courts give rise to possibly greater restrictions on the use of some powers, and also highlight areas where powers may no longer be sufficient to be effective investigation tools given the change in how crimes are committed. A recent high profile example is the use of covert video surveillance in the *Hamed* case, which required urgent legislative amendment pending enactment of the Search and Surveillance Bill.

17. For law enforcement and regulatory agencies, these issues were reviewed comprehensively over a number of years by the Law Commission and the Ministry of Justice, and resulted in the Search and Surveillance Act 2012.

[Not in Scope]

Maintaining public confidence through external oversight

19. The public's confidence in the GCSB has been impacted by the Dotcom case. In the past controversy has arisen over the actions of the NZSIS (for example the *Choudry* case in the late 1990's). The NZIC agencies are under the law, and not above. They are answerable to the law. However, the nature of their operations means that it is difficult to apply the usual accountability mechanisms exercised by the courts and parliament.

20. The establishment of stronger external oversight mechanisms is important to demonstrate to the public that the agencies are answerable in both legal and political terms consistent with New Zealand's democratic traditions.

21. The current mechanisms are the Inspector-General of Intelligence and Security, the Commissioner of Security Warrants and the Intelligence and Security Committee. Recent experience (including errors that contributed to the unlawful interceptions of Kim

Dotcom's communications) and a comparison with the more rigorous regime in Australia, suggest that legislative amendment and/or additional resources will likely be required to these oversight functions.

Timeframes and milestones

22. DES agreed [DES Min (12) 4/1-1] that legislation should be introduced in early May 2013 with enactment by early August 2013. Based on those broad timeframes, officials are working to the following milestones:

Milestone	Date
[Not in Scope]	
Cabinet policy approvals – GCSB Act review and review of external oversight	26 March 2013
Cabinet approval to introduce legislation	*Week of 6 May 2013*
Introduction of amending legislation	Early May 2013 (by 9 May at latest)

23. The Review is reporting progressively rather than with one set of papers. This approach allows the greatest time possible for Parliamentary Counsel to draft the amendments.

Implementation of legislation and operational changes

24. The enactment of legislation is only one step in enabling the NZIC agencies to respond to the new security environment. Processes and procedures will need to be adapted or developed to ensure that new and amended functions and powers are exercised within the law. New capabilities will also need to be developed by the agencies.

25. In the case of the GCSB the compliance review is likely to result in a number of recommendations to change organisational structures, compliance and audit systems, and processes to manage relationships with other agencies.

26. The financial implications associated with these changes, in terms of allocating resources to intelligence priorities and for any new capabilities, will be addressed by the NZIC as a whole through the Four Year Budget Plan process.

Publicity

27. DPMC with the Office of the Prime Minister is considering the approach to announcing the preparation and introduction of legislation and the linkages with the work on telecommunications security and industry obligations. This includes how to manage the provision of information to stakeholders given that this area of work is subject to strict security classifications.

28. DPMC is working with all the relevant agencies to prepare recommendations for consideration by Ministers.

Legislative Implications

29. There are no legislative implications arising from this paper, however the review will result in recommendations for legislative change.

30. The Office of the Leader of the House has been consulted and consideration is being given to the appropriate parliamentary process and timetable for both the proposed

Intelligence and Security Bill [Not in Scope] ;

.

Consultation

31. This paper was prepared by DPMC in consultation with NZSIS and GCSB.

Financial Implications

32. There are no financial implications arising from this paper.

Human Rights

33. There are no human rights issues arising from this paper.

Regulatory Impact Analysis

34. A Regulatory Impact Statement is not required for this paper as it does not seek decisions on policy options. Papers that make recommendations as a result of the Review will include a regulatory impact analysis.

Recommendations

35. The Prime Minister recommends that the Committee:

1. **note** that DES has agreed that a review of policy and legislation relating to the core New Zealand Intelligence Community be undertaken;
2. **note** that the first suite of papers resulting from the review relates to the New Zealand Security Service Act 1969;
3. **note** that proposals to amend the GCSB Act and the oversight arrangements will follow shortly;
4. **note** the timetable in paragraph 22;
5. **note** that consideration is being given to the appropriate form of parliamentary consideration of the bill;
6. **note** that consideration is being given to the announcement of the preparation and introduction of the bill, and the provision of information to stakeholders in light of the security classification of certain information.

for Prime Minister

15 February 2013

File

Cabinet Committee on Domestic and External Security

DES Min (13) 1/1

Copy No: 15

Minute of Decision

New Zealand Intelligence Community Policy and Legislation Review: Overview

Portfolio: Prime Minister

On 20 February 2013, the Cabinet Committee on Domestic and External Security (DES):

1 **noted** that in December 2012, DES agreed that a review of policy and legislation relating to the core New Zealand Intelligence Community be undertaken (the review) [DES Min (12) 4/1-1];

[Not in Scope]

3 **noted** that proposals to amend the Government Communications Security Bureau Act 2003 (the GCSB Act) and the oversight arrangements will be submitted in due course;

4 **noted** the following anticipated timetable for the review:

[Not in Scope]

4.2 policy approvals for the GCSB Act review and review of external oversight: 26 March 2013;

4.3 approval to introduce legislation: Week of 6 May 2013;

4.4 introduce amending legislation: By 9 May 2013;

5 **noted** that consideration is being given to:

[Not in Scope]

5.2 the announcement of the preparation and introduction of the bill;

5.3 the provision of information to stakeholders in light of the security classification of certain information.

Sam Gleisner
Committee Secretary

Reference: DES (13) 5

Present:
Rt Hon John Key (Chair)
Hon Bill English (part of item)
Hon Gerry Brownlee
Hon Steven Joyce (part of item)
Hon Christopher Finlayson (part of item)
Hon Murray McCully
Hon Amy Adams

Officials present from:
Office of the Prime Minister
Department of the Prime Minister and Cabinet
New Zealand Security Intelligence Service
Government Communications Security Bureau
Ministry of Justice

Distribution:
Cabinet Committee on Domestic and External Security
18 Office of the Prime Minister
19 Chief Executive, DPMC
20 Director, Security and Risk, DPMC
21 Director, Intelligence Coordination Group, DPMC
22 Director, NZSIS
23 Director, GCSB

Cabinet

CAB Min (13) 5/5

Copy No: 6

Minute of Decision

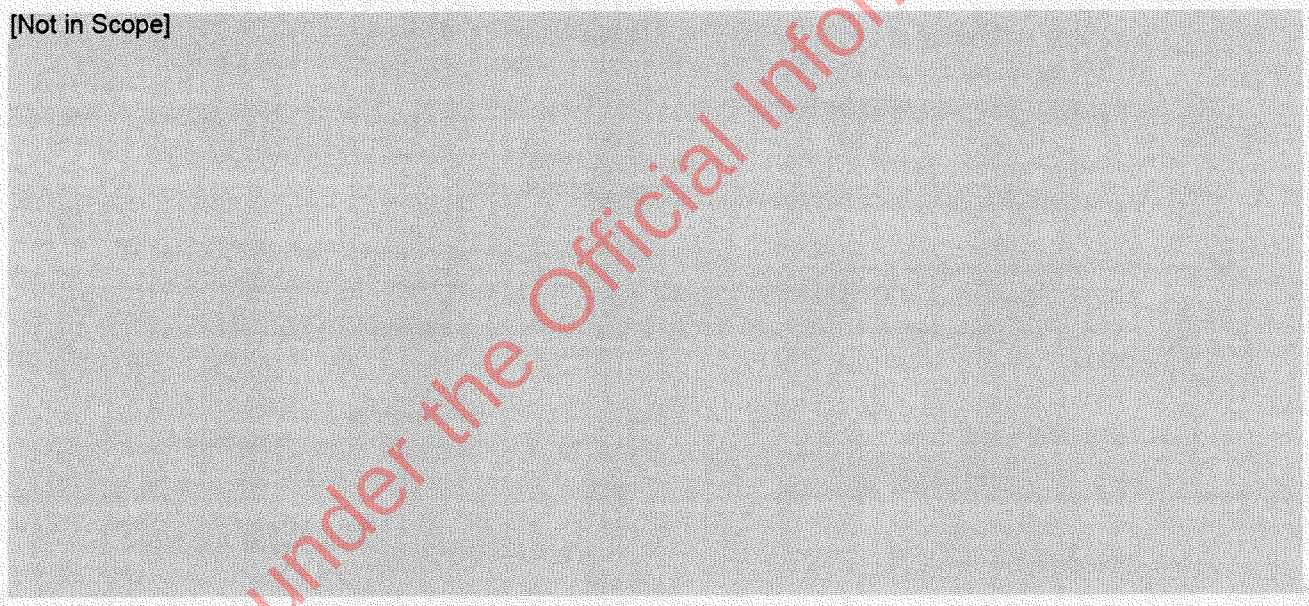
Report of the Cabinet Committee on Domestic and External Security: Period ended 22 February 2013

On 25 February 2013, Cabinet made the following decisions on the work of the Cabinet Committee on Domestic and External Security for the period ended 22 February 2013.

DES Min (13) 1/1 **New Zealand Intelligence Community Policy and Legislation Review: Overview** CONFIRMED

Portfolio: Prime Minister

[Not in Scope]



for Secretary of the Cabinet

Reference: CAB (13) 75

Distribution:
Cabinet Committee on Domestic and External Security
Chief Executive, DPMC
Director, PAG, DPMC
Director, Security and Risk Group, DPMC
Director, Intelligence Coordination Group, DPMC
Director, NZSIS
Director, GCSB

Item 5

Cabinet Committee on Domestic and External Security

DES (13) 10

Copy No: 15

Summary of Paper

25 March 2013

Review of the Government Communications Security Bureau Act 2003: Paper 1: Overview

Portfolio Minister Responsible for the GCSB

The Minister Responsible for the GCSB recommends that the Committee:

1 note that in December 2012, the Cabinet Committee on Domestic and External Security (DES) agreed that a review of policy and legislation relating to the core New Zealand Intelligence Community be undertaken [DES Min (12) 4/1-1];

2 note that in February 2013, DES considered the NZSIS Act review suite of papers and agreed to changes to the NZSIS Act [DES Min (13) 1-1/5];

3 note that on 26 March 2012, DES will consider a related paper under DES (13) 9 on the review of external oversight mechanisms, in particular a review of the Intelligence and Security Committee Act 1996 and the Inspector General of Intelligence and Security Act 1996;

4 note the contents of the submission under DES (13) 10 that provides a summary of the findings and recommendations of the review of the Government Communications Security Bureau Act 2003 (GCSB Act);

5 note that the related paper under DES (13) 11 proposes changes to the GSCB Act to:

5.1 provide for greater and more effective oversight;

5.2 update the GCSB Act to respond to changes in the operating environment;

6 note that DES consideration of the GCSB Act review papers will conclude the reports of the review of policy and legislation relating to the core New Zealand Intelligence Community referred to in paragraph 1 above;

7 note that consideration is being given to the announcement of the preparation and introduction of the Intelligence and Security Bill.

Sam Gleisner
Committee Secretary

Distribution:
Cabinet Committee on Domestic and External Security
Office of the Prime Minister
Chief Executive, DPMC
Director, Security and Risk, DPMC
Director, Intelligence Coordination Group, DPMC
Director, National Assessments Bureau, DPMC
Director, NZSIS
Director, GCSB
Secretary to the Treasury
Secretary for Justice
Privacy Commissioner
Secretary of Foreign Affairs and Trade
Secretary of Defence
Chief of Defence Force
State Services Commissioner
Commissioner of Police
Minister of Customs
Comptroller of Customs
Chief Parliamentary Counsel

Office of the Minister responsible for the GCSB

Cabinet Domestic and External Security Committee

REVIEW OF THE GOVERNMENT COMMUNICATIONS SECURITY BUREAU ACT 2003: PAPER 1 OVERVIEW

Proposal

1. The purpose of this paper is to provide background and context for the Government Communications Security Bureau Act 2003 (GCSB Act) review, and a summary of the findings and recommendations of the review.

Executive Summary

2. The core New Zealand Intelligence Community (NZIC) comprises three key agencies together with the Intelligence Coordination Group (ICG), which is located in the Department of Prime Minister and Cabinet (DPMC):
   - the New Zealand Security Intelligence Service (NZSIS);
   - the Government Communications Security Bureau (GCSB); and
   - the National Assessments Bureau (NAB), which is located in DPMC.
3. The GCSB has a vital role to play in protecting the security and safety of New Zealanders. With the other NZIC agencies, the GCSB contributes to the protection of the national security of New Zealand.
4. To achieve its goals and objectives, Parliament has necessarily provided the GCSB with intrusive powers, subject to controls and limitations on their use. The ability to exercise such powers comes with responsibility – responsibility to operate within the law and consequently to maintain the confidence of everyday New Zealanders.
5. On 11 December 2012 the Cabinet Committee on Domestic and External Security (DES) agreed that a review of the policy and legislation relating to the core New Zealand Intelligence Community be undertaken.
6. It is timely to review the GCSB Act for two reasons. First, to ensure the Act is modern and fit for purpose so the GCSB can undertake its role of protecting the interests of New Zealanders in a fast changing security environment. Second, to respond to the concerns that have arisen in recent months relating to the GCSB's compliance with its Act.
7. It is essential that the GCSB has a clearly formulated and consistent statutory framework to operate within, and the public needs to have confidence that it is operating within the bounds of that legal framework. While the GCSB Act can be interpreted to allow the GCSB to carry out its core activities, there is enough ambiguity that means the only responsible course of action when dealing with intrusive powers is to make the legislation clearer and more transparent.

8. The findings of the GCSB Act review led to recommendations to update and clarify the functions and powers of the GCSB. The recommended changes do not involve a fundamental change to the construction of the GCSB Act or the principles underpinning it. The proposed changes do not represent an extension of the range of powers. The changes will allow the GCSB to undertake the role the Governments expects of it to protect the security and sovereignty of New Zealand.

9. It has also led to recommendations to substantially improve the oversight regime the GCSB operates under. The recommendations regarding oversight in the GCSB Act papers need to be read in conjunction with the proposals in the paper on NZIC external oversight. The recommendations arising from the GCSB Act review will enable the proposed enhanced Office of the Inspector-General of Intelligence and Security to undertake a more intensive review of systems and individual cases to test compliance with the law.

10. The GCSB Act review has taken into account the findings of a compliance review of the GSCB recently completed by Rebecca Kitteridge, who was seconded from the Cabinet Office to undertake this task. In response to Ms Kitteridge's review the GCSB will make changes to improve its internal systems and compliance framework.

11. The GCSB Act review papers are the last set of papers from the New Zealand Intelligence Community Policy and Legislation Review to be considered by DES.

Background

12. On 11 December 2012 the Cabinet Committee on Domestic and External Security (DES) agreed that a review of the policy and legislation relating to the core New Zealand Intelligence Community be undertaken. The scope of the review would include [DES Min (12) 4/1-1]:

[Not in Scope]

- A review of the GCSB Act;
- A review of the functions and powers needed to address cyber security, cyber effects, critical infrastructure protection and other related capabilities;
- A review of external oversight mechanisms, in particular a review of the Intelligence and Security Committee Act 1996 and the Inspector General of Intelligence and Security Act 1996;
- A review of the ability of intelligence agencies to assist and cooperate with other agencies under existing legislation;
- An assessment of any legislative changes required to facilitate the commitment to "one community, many agencies".

13. The recent review of compliance at GCSB (Compliance Review) has identified a need to improve the compliance framework GCSB, to ensure that it is acting in accordance with the law. Rebecca Kitteridge was seconded to the GCSB to undertake the Compliance Review, and report the Director of the GCSB on these matters.

14. Related to that was a need to test whether the oversight legislation, which covers both the GCSB and the NZSIS, was sufficiently robust to provide the external oversight expected by the public, Parliament and the responsible Minister. Both the Inspector–General of Intelligence and Security Act and the Intelligence and Security Act were enacted in 1996. A review of those two acts was therefore included in the scope of the review.

15. Finally, separately there was a need to review the GCSB Act to determine whether updates were required in light of changes in the threat environment facing New Zealand, particularly in the area of cyber security, and developments in the law relating to privacy and search and surveillance. The GCSB Act has not been reviewed or amended since its enactment in 2003, and there have been a number of relevant developments during that time.

16. [Not in Scope] The GCSB Act review suite of papers is the last set of papers from the NZIC policy and legislation review.

Comment

Goals and approach to the GCSB Act review

17. The purpose of the GCSB Act review was:

- To provide for a clearly formulated and consistent statutory framework.
- To provide for greater and more effective oversight at all levels (internally by the Director, at ministerial level by the responsible Minister and externally by the Inspector-General and the Intelligence and Security Committee).
- To update the GCSB Act to respond to the changing security environment, cyber environment and information security, and the changes in the public law environment since the GCSB Act was passed in 2003. This mirrors the process undertaken by the NZSIS to review its legislation.

18. Respect for human rights, individual privacy and traditions of free speech in New Zealand were guiding principles in undertaking the GCSB Act review and developing recommendations.

19. However, in developing legislation for intelligence agencies some qualifications to these basic principles need to be considered. The approach taken was that any qualifications must be shown to be necessary, and that functions and powers must operate within a framework of a carefully formulated and consistent policy along with robust external oversight mechanisms.

20. It is important to state at the outset that the basic premise underpinning the operations of the GCSB is that it does not conduct foreign intelligence activities against New Zealanders. This premise predated the GCSB Act. Given its importance and significance it was incorporated into the GCSB Act (section 14). The repeal of this basic premise was not contemplated at any time during the GCSB Act review.

21. However, the way this basic premise was incorporated into the GCSB Act is less than ideal, and meant that it applied to not only the foreign intelligence function of the GCSB

but also its other two functions – namely information assurance and cooperation and assistance to other agencies. This has created a growing number of difficulties, and is restricting GCSB's ability to effectively carry out its other two functions. These issues are discussed in paper 2.

22. The basic premise underpinning the operations of the GCSB that it does not conduct foreign intelligence activities against New Zealanders will be retained. New wording will be proposed to preserve this basic premise and clarify that it only applies to GCSB's foreign intelligence function, and not to its information assurance and cooperation and assistance functions.

23. The officials working on the NZIC Policy and Legislation review were briefed by Ms Kitteridge about her review, and considered her findings in developing the proposals in the GCSB Act review and the external oversight papers. The extensive legal work carried out by the GCSB to assess its activities against the provisions of the GCSB Act was also taken into account. In addition the GCSB Act review was carried out in parallel with the review of external oversight mechanisms.

Findings of the GCSB Act review – clarity of the statutory framework

24. The GCSB Act review found that while the Act did provide for and authorise its current activities, a considerable amount of legal analysis and a number of legal opinions about the interplay of different provisions of the GCSB Act was needed to arrive at that conclusion. In some cases, it was not clear that a court would always support the interpretations adopted to arrive at those conclusions.

25. It is not easy, on the face of the statute, to determine whether any given activity falls within the scope of the prescribed functions. A high degree of legal risk remains about whether an activity is within the functions of the GCSB or not. While it might be acceptable for a private company to take on that risk, it is not appropriate for the Crown to knowingly adopt an approach where it knows that some of the activities may now not be considered legal by a court, especially where the exercise of intrusive powers of the state are involved.

26. The Compliance Review sums up the situation by saying that the GCSB Act is not (and probably has never been) completely fit for purpose. The responsible course of action is to make the legislation clearer and more transparent.

Findings of the GCSB Act review – providing for effective oversight

27. The lack of clarity means that the public (and Parliament as its representative), the Inspector-General of Intelligence and Security, the responsible Minister, and the Director of the GCSB (and GCSB staff) face an unacceptable degree uncertainty as to what the lawful functions of the GCSB constitute. This makes any oversight extremely difficult, relying as it does on extensive and complex analysis of the meaning of the GCSB Act.

28. The foundation of effective oversight is having a clearly formulated and consistent statutory framework. Without that the ISC, the IGIS and the responsible Minister must rely on interpretations, and distilling meaning from other sources as to the intention of the statute.

29. In addition the GCSB Act review found that more transparent and consistent ministerial authorisation processes should be set out in statute. This would provide greater

guidance and transparency for those making applications, for the responsible Minister when considering applications and enhance the ability of the Inspector-General to provide oversight of the decision making system.

Findings of the GCSB Act review – responding to changes to the operating environment

30. The third aspect of the review was to consider whether the GCSB Act needed updating to addressing changes in the operating environment. The issues found by the GCSB Act review that require the Act to be updated can be summarised under the following three headings:

- Changing security environment – the security environment facing New Zealand today presents new challenges. Security issues are increasingly interconnected and national borders are less meaningful. Globalisation means that New Zealand is no longer as distant from security problems as it was in the past. The increasing level of innovation in the cyber environment, while fueling economic growth and international trade opportunities, is also giving rise to new security issues. The GCSB Act was enacted 10 years ago when cyber matters were less sophisticated and prominent.

- Changing information security requirements – the cyber environment continues to innovate at a remarkable pace, and there is an increasing shift of activity, both business and government to that environment. To counter the threat to business and government information the Government launched the Cyber Security Strategy in June 2011.

  The GCSB currently has as one of its core functions information assurance, and it is uniquely placed with its advanced capabilities developed through its intelligence work to contribute to responses to cyber security issues. That is why, as part of the Cyber Security Strategy, the National Cyber Security Centre was created within the GCSB. The Cabinet has indicated its expectation that the GCSB will considerably enhance its cyber security capabilities and use its expertise to assist a range of organisations (government, state sector, critical national infrastructure providers, and key economic contributors). However, the implementation of the NCSC has highlighted limitations on the ability of GCSB to contribute to this work because of the provisions of the GCSB Act.

- Changing public law environment – the legal environment in which the GCSB Act is interpreted has developed since its enactment. The courts' consideration of law enforcement cases give rise to possibly greater restrictions on the use of some powers, and also highlight areas where powers may no longer be effective given the change in the telecommunications environment. For law enforcement agencies these issues were reviewed comprehensively over a number of years, and were addressed in the Search and Surveillance Act 2012.

Findings of the GCSB Act review – supporting other agencies

31. In addition to the three key issues above, the GCSB plays a crucial role in the support of other government agencies, in particular the New Zealand Defence Force and the NZSIS. The GCSB also supports the New Zealand Police in the detection and investigation of serious crime. The GCSB's unique capabilities are an invaluable resource for those agencies to draw upon.

32. The GCSB Act review considered that in a small jurisdiction such as New Zealand we cannot afford to duplicate expensive and sophisticated assets, and there are limited numbers of people that can work with such assets. Consistent with the Better Public Services programme, the capabilities such as those developed or acquired by the GCSB, where appropriate and subject to necessary safeguards, should be available to assist in meeting key Government priorities. This too should be addressed in the update of the GCSB Act.

Recommended changes to the GCSB Act

33. The GCSB cannot be left to operate under an ambiguous legal framework, which is having unintended consequences and carries risk. Taking into account the findings outlined above, I recommend that the functions and powers of the GCSB be updated and amended to ensure that a clear and consistent statutory framework supported by a robust ministerial authorisation process underpins its activities.

34. The recommended legislative changes are not revolutionary. They do not involve a fundamental change to the construction of the GCSB Act or the principles underpinning it.

35. Currently the GCSB Act provides for three functions:

- Information security and assurance,
- Foreign intelligence,
- Co-operation and assistance to other entities.

36. The proposal is that that these three functions remain, but that the descriptions are clarified to allow for more effective oversight, and updated to respond to the changing operational environment. These changes will complement and amplify the proposals to strengthen oversight with amendments to the Inspector–General of Intelligence and Security Act and the Intelligence and Security Act.

37. In the case of foreign intelligence and co-operation, both need to be clarified and the meaning made clear, and in the case of co-operation a ministerial authorisation process is proposed to provide a way of determining who GCSB can work with and under what circumstances.

38. With respect to the information assurance function, currently the GCSB Act focuses almost entirely on providing protective services to public sector entities. However, threats in the cyber environment also put at grave risk our critical infrastructure and businesses that drive our economy. This function needs to be given more prominence, and what is expected of GCSB to safeguard New Zealand information, both private and public sector, needs to be made clear.

39. In the case of powers, again a fundamental change is not recommended. The GCSB Act currently sets out three types of powers:

- Warrantless powers of interception and access,
- Interception warrants, and
- Computer network access authorisations.

40. The changes proposed to the Act do not represent an extension of powers, but the GCSB Act will be amended to make it clear that the powers can be used for both the foreign intelligence function and the information security and assurance function. Also, in light of changes in the legal environment, and the way in which communications are now carried and routed around the world the language used to describe these powers is outdated and needs to be refreshed.

41. In addition, more transparent and consistent ministerial authorisation processes are proposed to support greater oversight.

42. As stated at the outset, the basic premise underpinning the operations of the GCSB that it does not deliberately conduct foreign intelligence activities against New Zealanders will be retained. New wording will be proposed to preserve this basic premise and clarify that it only applies to GCSB's foreign intelligence function, and not to its information assurance and cooperation and assistance functions. This means that situations like those in the Kim Dotcom case would continue to be prohibited.

43. While the basic premise will not apply to the cooperation and assistance function, the GCSB will be required to obtain a Ministerial authorisation when providing assistance to other agencies in the performance of their lawful duties if that involves producing intelligence on New Zealanders.

44. The GCSB Act would also be clarified to make it clear that the GCSB is able to conduct activities that do not unduly impinge on New Zealanders' privacy (such as interception of openly broadcast information and interception with the consent of the parties to a communication) and to collect metadata (described further in paper 2) in bulk and analyse foreign metadata components for foreign intelligence purposes.

Implementation of legislation and operational changes

45. The enactment of legislation is only one step in enabling the NZIC agencies to respond to the new security environment. Processes and procedures will need to be adapted or developed to ensure that new and amended functions and powers are exercised within the law. New capabilities will also need to be developed by the agencies.

46. In the case of the GCSB the compliance review is likely to result in a number of recommendations to change organisational structures, compliance and audit systems, and processes to manage relationships with other agencies.

Publicity

47. DPMC with the Office of the Prime Minister is considering how to manage the announcement of the preparation and introduction of legislation, taking into account the outcome of the Compliance Review. In addition consideration is being given to how to manage the linkages with the telecommunications security and industry obligations work [DES Min (12) 4/1-2]. DPMC will be reporting to relevant Ministers with a recommended approach.

Legislative Implications

48. The proposals in GCSB Act review suite of papers will require amendments to the GCSB Act. The Committee agreed that amendments resulting from the NZIC Policy and Legislation Review should be progressed in an Intelligence and Security Bill, which has a category 2 priority [DES Min(12) 4/1-1].

49. The proposals in these papers have been developed in a short timeframe. Given one of the main issues being addressed is the lack of clarity of the GCSB Act, the drafting phase may reveal further questions that need to be addressed. To manage this situation paper 2 contains a recommendation noting that officials will consult with the Responsible Minister and the Attorney-General on the drafting of the functions, and a recommendation authorising those Ministers to make any decisions on additional matters that are necessary that are consistent with Cabinet's decisions.

Consultation

50. 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, Ministry of Foreign Affairs and Trade, New Zealand Defence Force, New Zealand Police, New Zealand Customs Service, Ministry of Defence, Ministry of Justice, Office of the Privacy Commissioner, State Services Commission and the Treasury were consulted.

Financial Implications

51. The NZIC Policy and Legislation Review project has been funded and supported in kind by DPMC, GCSB and NZSIS. The next phase of the project (drafting and parliamentary stages) will also be funded by DPMC, GCSB and NZSIS. The project team to this point has included seconded staff from other agencies, and it is likely that further secondments or extensions to existing secondments will be sought to complete the project.

52. The financial implications associated with the changes in the GCSB Act review suite of papers, in terms of allocating resources to intelligence priorities and for any new capabilities, will be addressed by the NZIC as a whole through its joint Four Year Budget Plan process.

Human Rights

53. The proposals in the review of the GCSB Act papers 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 engage, in particular, the right to be free from unreasonable search and seizure affirmed in section 21 of the NZBORA.

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

Regulatory Impact Analysis

55. A Regulatory Impact Statement (RIS) has been prepared and is attached. A member of the Policy Advisory Group, within the Department of Prime Minister and Cabinet, has reviewed the RIS prepared by the Intelligence Co-ordination Group. The reviewer considers that the RIS meets the quality assurance criteria of the Regulatory Impact Analysis framework. As noted in the Cabinet paper, the reviewer observes that due to the nature of the issues dealt with in the paper and national security classifications associated with the material, no public consultation has been undertaken. This will occur during the parliamentary consideration of the amending legislation.

Recommendations

56. The Minister responsible for the Government Communications Security Bureau recommends that the Committee:

1. **note** that on 11 December 2012 DES agreed that a review of policy and legislation relating to the core New Zealand Intelligence Community be undertaken [DES Min (12) 4/1-1];

[Not in Scope]

3. **note** that DES, prior to the GCSB Act review papers, will be considering a paper on the review of external oversight mechanisms, in particular a review of the Intelligence and Security Committee Act 1996 and the Inspector General of Intelligence and Security Act 1996;

4. **note** that the GCSB Act review papers recommend changes to GCSB Act to provide for greater and more effective oversight and to update the Act to respond to changes in the operating environment;

5. **note** that DES consideration of the GCSB Act review papers will conclude the report backs of the review of policy and legislation relating to the core New Zealand Intelligence Community;

6. **note** that consideration is being given to the announcement of the preparation and introduction of the Intelligence and Security Bill.

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

22 / 3 / 2013

REGULATORY IMPACT STATEMENT

Government Communications Security Bureau Act Review

Agency Disclosure Statement

1. This regulatory impact statement has been prepared by the Department of Prime Minister and Cabinet with the Government Communications Security Bureau.
2. It provides an analysis of options to update and amend the Government Communications Security Bureau Act 2003 (the GCSB Act) to respond to the findings and recommendations of the recent review of compliance at GCSB carried out by Rebecca Kitteridge, and to respond to changes in GCSB's operating environment.
3. The analysis of options was conducted as part of a wider New Zealand Intelligence Community Policy and Legislation Review project, which included an existing review of the New Zealand Security Intelligence Service Act 1969 and a review of legislation providing for oversight mechanisms (the Intelligence and Security Committee Act 1996 and the Inspector-General of Intelligence and Security Act 1996). The analysis of options took into account the work on these other reviews, and the compliance review.
4. The GCSB Act contains intrusive state powers. Consequently any review of the GCSB Act will involve the consideration of human rights and privacy matters. Respect for human rights, and individual privacy and traditions of free speech in New Zealand were guiding principles in undertaking the review and developing recommendations.

Rajesh Chhana
Intelligence Co-ordination Group
Department of Prime Minister and Cabinet

22 March 2013

Status quo and problem definition

5. The GCSB has a vital role to play in protecting the security and safety of New Zealanders. Together with the other New Zealand Intelligence Community agencies, the GCSB contributes to the protection of the national security of New Zealand.

6. The GCSB was continued and established as a department of State by the Government Communications and Security Bureau Act 2003 (GCSB Act). The GCSB Act has not been amended since its enactment in 2003.

7. The GCSB Act sets out the objectives and functions of the GCSB, specifies the intrusive powers Parliament has necessarily provided to the GCSB to fulfill its functions and the related authorisation processes. The ability to exercise such powers comes with responsibility – responsibility to operate within the law and consequently to maintain the confidence of everyday New Zealanders.

8. In October 2012 Rebecca Kitteridge was seconded from the Cabinet Office to the GCSB to undertake a review of compliance at GCSB to provide assurance to the GCSB Director that the GCSB's activities are undertaken within its powers and that adequate safeguards are in place. Ms Kitteridge briefed officials working on the New Zealand Intelligence Community Policy and Legislation Review project about her review, and her findings have been taken into account in developing the proposals referred to in this paper.

9. Two broad problems with the GCSB Act have been identified. First, while the GCSB Act provides for and authorises its current activities, it is not easy to determine whether any given activity falls within the scope of the prescribed functions of the GCSB or not. A considerable amount of legal analysis about the interplay of different provisions within the GCSB Act is needed to arrive at any such conclusion.

10. This situation is not satisfactory. The foundation of effective oversight is having a clearly formulated and consistent statutory framework. The lack of such a framework makes management and oversight of the GSCB very difficult, having to rely as it does on extensive and complex analysis of the meaning of the GCSB Act. The only responsible course of action when dealing with intrusive powers is to make the legislation clearer and more transparent.

11. Second, since the enactment of the GCSB Act in 2003 there have been a number of changes in the threat environment facing New Zealand, particularly in the area of cyber security, and developments in the law relating to privacy and search and surveillance. The issues that require the GCSB Act to be updated can be summarised under four headings.

Changing information security requirements

12. The cyber environment continues to innovate at a remarkable pace, fueling economic growth and international trade opportunities. Consequently, there is an increasing shift of activity, both business and government, to that environment. To counter the threat to business and government information the Government launched the New Zealand Cyber Security Strategy in June 2011 (NZCSS).

13. The GCSB currently has as one of its core functions information security and assurance. The advanced capabilities developed through GSCB's intelligence work mean it is

uniquely placed to contribute to responses to cyber security issues. That is why, as part of the NZCSS, the National Cyber Security Centre (NCSC) was created within the GCSB. The Cabinet has indicated its expectation that the GCSB will considerably enhance its cyber security capabilities and use its expertise to assist a range of organisations (government, state sector, critical national infrastructure providers, and key economic contributors). However, the implementation of the NCSC has highlighted limitations on the ability of GCSB to contribute to this work because of the provisions of the GCSB Act (for example it is not clear that the GCSB can provide advice and assistance to private sector entities in New Zealand).

14. The impact of cyber threats is difficult to quantify precisely, but the NZCSS sets out some of the potential impacts, as well as some estimates suggesting New Zealanders lose up to $500m annually due to cyber-borne frauds and scams. Recent statistics on the NCSC website indicate that in the last 12 months cyber crime against New Zealanders cost $625m, and the global cost was estimated at up to $460 billion.

15. More broadly, the monetized cost of loss of intellectual property as a result of cyber intrusions into private sector entities is exceptionally difficult to quantify, in part because companies are reluctant to report losses or may not even know their property has been stolen. However, based on the scale of intrusions and exfiltrations seen in other jurisdictions and the number of intrusions reported in New Zealand the potential costs to New Zealand of cyber-based industrial espionage are likely to be significant.

16. Internationally the trend has been described as shifting from "exploitation" to "disruption" and "destruction". In other words the cyber threat is changing from theft of personal and intellectual property, to denial of service attacks and destruction of computer networks.

17. The NCSC 2012 Incident Summary reported that there was a significant increase (from 90 to 134) in the number of reported serious attacks against New Zealand government agencies, critical national infrastructure and private sector organisations.

18. If a major attack was directed at government agencies, critical national infrastructure providers (for example telecommunications networks and water supply) or companies that drive New Zealand's economy, there could be significant disruption to commercial and personal activities. It would also put at risk New Zealand's political and business reputation.

Changing security environment

19. The security environment New Zealand faces today presents new challenges. Globalisation means that New Zealand is no longer as distant from security problems as it was in the past. Security issues are increasingly interconnected and national borders are less meaningful. The increasing level of innovation in the cyber environment and the ubiquity of internet-based services is giving rise to new security threats and vulnerabilities. The GCSB Act was enacted 10 years ago when cyber matters were less sophisticated and prominent.

Changing public law environment

20. The legal environment in which the GCSB Act is interpreted has developed since its enactment. The courts' consideration of law enforcement cases has provided further guidance about how intrusive state powers should be set out in statute, and highlight areas where powers may no longer be effective given the change in the

telecommunications environment. For law enforcement agencies these issues were reviewed comprehensively over a number of years, and were addressed in the Search and Surveillance Act 2012.

Better Public Services

21. In addition to the issues above, the GCSB plays a crucial role in the support of other government agencies, in particular the New Zealand Defence Force and the NZSIS. The GCSB also supports the New Zealand Police in the detection and investigation of serious crime. The GCSB's unique capabilities are an invaluable resource for those agencies to draw upon.

22. The GCSB Act review considered that in a small jurisdiction such as New Zealand we cannot afford to duplicate expensive and sophisticated assets, and there are limited numbers of people that can work with such assets. Consistent with the Better Public Services programme, the capabilities such as those developed or acquired by the GCSB, where appropriate and subject to necessary safeguards, should be available to assist in meeting key Government priorities. This too should be addressed in the update of the GCSB Act.

Objectives

23. The objectives of the GSCB Act review are:

- To provide for greater and more effective oversight at all levels (internally by the Director, at ministerial level by the responsible Minister and externally by the Inspector-General and the Intelligence and Security Committee).
- To enable the GCSB to respond to the changing security environment, cyber and information security environment, and the changes in the public law environment since the GCSB Act was passed in 2003.

Regulatory Impact Analysis

24. Three policy options were assessed:

- non-legislative solutions;
- amending the GCSB Act;
- repealing and replacing the GCSB Act.

Non-legislative solutions

25. As noted above the GCSB Act is a piece of legislation that sets out and provides safeguards for the use of intrusive state powers. The GCSB cannot address any new threats beyond those it is permitted to address in its legislation.

26. The difficulties associated with the interpretation of the GCSB Act could be addressed by developing detailed guidance material, but it would be of limited benefit and consume considerable time and expenditure on legal advice to develop. This would not substantially address the need to improve management and external oversight of the GSCB.

27. Non-legislative solutions cannot satisfactorily meet the two objectives.

Amending the GCSB Act

28. The GCSB Act currently provides for three functions;

    - Foreign intelligence
    - Information security and assurance
    - Co-operation and assistance to other entities

29. The two objectives could be met by updating and clarifying the current functions set out in the GCSB Act. It is not considered that any new functions need to be added, but a refresh of the way in which the functions are articulated would ensure that the functions fit the changing operational environment, as well as providing greater clarity about what GCSB's functions actually are. These changes would complement and amplify the proposals to strengthen oversight by the Inspector-General of Intelligence and Security.

30. In the case of the foreign intelligence and cooperation functions, both would need to be clarified to allow for more effective oversight, and in the case of co-operation a ministerial authorisation process could be included in the GCSB Act to provide a way of determining who GCSB can work with and under what circumstances.

31. The information security and assurance function in the GCSB Act focuses almost entirely on providing protective services to public sector entities. However, threats in the cyber environment also put at grave risk our critical infrastructure and businesses that drive our economy. This function needs to be given more prominence. So too the expectations of the GCSB in safeguarding New Zealand information, in both public and private sectors, needs to be made clear.

32. The GCSB Act currently sets out three types of powers:

    - Warrantless powers of interception and access
    - Interception warrants
    - Computer network access authorisations

33. These powers are contained in Part 3 of the GCSB Act along with other provisions that control the use of those powers.

34. The objective of greater and more effective oversight would be met by still requiring the current range of authorisations but amending the GCSB Act so the authorisation processes are more transparent and consistent.

35. In order to meet the second objective, while the range of powers available to the GCSB does not need to be expanded the GCSB Act would be amended to make it clear that the powers can be used for both the foreign intelligence function and the information security and assurance function. The powers are needed to support the information security and assurance function to give the GCSB the ability to respond effectively to emerging cyber threats against New Zealanders.

36. The basic premise underpinning the operations of the GCSB that it does not conduct foreign intelligence activities against New Zealanders will be retained (currently contained in section 14 of the GCSB Act). However, because the information security and assurance function is about protecting New Zealanders, an amendment will also be required to allow the GCSB to see who (namely New Zealand individuals and

companies) is being attacked. This would allow the GCSB to determine where the threats are being generated from and develop measures to counter those threats.

37. Finally, amendments could be made to update the description of the powers to accommodate changes in how communication are now carried and routed around the world. This would be similar to the work undertaken for law enforcement powers in the Search and Surveillance Act 2012.

38. The costs of developing and drafting the proposed amendments and implementing them fall on the Government. The GCSB Act applies to the operation of the GCSB consequently the costs are part of its core operating expenses, and no compliance costs for business arise.

39. This approach would have the following outcomes and benefits:

Outcomes	Benefits
Greater clarity of the law governing the operation and administration of the GCSB	Provides basis for more effective oversight by external oversight bodies, thereby enhancing public trust and confidence.
	Responds to changes in the public law environment so that the law reflects current jurisprudence and is relevant to the current technological environment.
	Provides clarity to the public on the functions and powers of the GCSB.
	Provides clarity to staff and enhances management oversight of GCSB activities.
GSCB functions updated to allow GCSB to meet new threats, in particular cyber security.	Enables GCSB to support private sector in addition to public sector entities to counter cyber threats, which currently have an estimated impact on New Zealanders of over $0.50 billion in terms of cyber crime alone.
	Enables GCSB to more effectively detect and respond to cyber threats by allowing it to use the powers in the GCSB Act when undertaking its information security and assurance function.
	Allow GCSB to better fulfill the functions of the NCSC and play an effective part in the delivery of the NZCSS along with the other agencies tasked with its delivery.
GCSB able to assist and advise other Government agencies fulfill their lawful functions with its technical capabilities and expertise.	Other agencies will not have to duplicate technical capabilities and expertise already held by the Crown, and make effective and efficient use of the GCSB's capabilities.

Repealing and replacing the GCSB Act

40. The two objectives could be achieved by taking a more expansive approach to updating the GCSB's establishment statute, by repealing it and replacing it with a new statute.

41. The benefit of this approach, over and above the option to amend the GCSB Act, is that it would result in a new Act that would pick up the changes described in the discussion of the option to amend the GCSB Act as well as providing an opportunity to reenact all other existing provisions with updated drafting where necessary. However, as discussed above, the number of changes required to achieve the objectives can be targeted at particular parts and sections of the GCSB Act and the basic construction of the GCSB Act does not need to change to accommodate those amendments.

42. Consequently there does not seem to be any great benefit associated with dedicating additional time and resources to redrafting and reenacting provisions that do not need to be changed.

Consultation

43. The policy development process was undertaken by the New Zealand Intelligence Community (DPMC – lead, with GCSB, and NZSIS). The agencies consulted were the Ministry of Foreign Affairs and Trade, New Zealand Defence Force, New Zealand Police, New Zealand Customs Service, Ministry of Defence, Ministry of Justice, Office of the Privacy Commissioner, State Services Commission and the Treasury.

44. Given the nature of the issues being dealt with and the national security classifications associated with the material, there was no public consultation process. Public consultation on the proposals will occur during the parliamentary consideration of the amending legislation.

Conclusions and recommendations

45. As discussed above, the identified problems do not require a change to the scheme of the GCSB Act and the objectives of the review can be met by amendments to targeted provisions. The benefits of dedicating resources to a full redrafting of the Act are consequently limited. The recommended option is to amend the GCSB Act to address the identified issues and meet the objectives of the reform.

Implementation

46. The compliance review of the GCSB has a range of recommended changes to the compliance framework and operations of the GCSB. The GCSB is developing an implementation plan to respond to those recommendations, and the implementation of the amendments to the GCSB Act will be incorporated into that plan.

Monitoring, Evaluation and Review

47. The GCSB will monitor the effectiveness of the amendments and advise the Minister about any issues arising.

Item 6

Cabinet Committee on Domestic and External Security

DES (13) 11

Copy No: 15

Summary of Paper

25 March 2013

Review of the Government Communications Security Bureau Act 2003: Paper 2: Proposals

Portfolio: Minister Responsible for the GCSB

The Minister Responsible for the GCSB recommends that the Committee:

Background

1 note that in December 2012, the Cabinet Committee on Domestic and External Security (DES) agreed that a review of the Government Communications Security Bureau Act 2003 (the GCSB Act) be undertaken [DES Min (12) 4/1];

2 note that the GCSB 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 GCSB 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:

3.1 information assurance/cyber security;

3.2 foreign intelligence;

3.3 co-operating with other entities;

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

5 agree that the description of the Bureau's information assurance/cyber security function 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 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 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 that, based on the approach in paragraphs 3-7 above, section 8 of the GCSB 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 maters 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 with 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 GCSB Act continue to provide the basic tools that the Bureau requires to perform its functions, subject to some updating of the language used;

11 note that section 14 of the GCSB 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 GCSB Act 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 permitting the bureau to collect metadata in bulk and analyse foreign metadata components for foreign intelligence purposes;

13.4 permitting the Bureau to scan internet traffic for advanced cyber threats and to deal with these in a way that promotes the protection of New Zealanders and New Zealand information infrastructures in a modern telecommunications environment;

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 GCSB Act be retained;

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 GCSB Act be amended to incorporate a new mechanism to enhance Ministerial oversight of Bureau activities, through which the Minister 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 be enhanced to include assurances that the activities proposed by the Bureau are necessary, justified and reasonable, and to provide consistently across the Ministerial authorisation mechanisms;

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

18 agree that 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, in line with recent Cabinet decisions in respect of the NZSIS [DES Min (13) 1/4]:

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 the GCSB Act be amended:

21.1 in line with recent Cabinet decisions in respect of the NZSIS [DES Min (13) 1/4], 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;

21.2 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;

21.3 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;

21.4 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;

22 note that consequential amendments may be needed to the provisions governing the execution of Ministerial authorisation;

23 note that in October 2010, DES 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 [DES Min (10) 3/1];

24 note that amendments to the GCSB Act are required to give effect to the proposal in paragraph 23 above;

Legislative process

25 note that in December 2012, DES:

25.1 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);

25.2 noted that the bill would be enacted by August 2013;

[DES Min (12) 4/1-1]

26 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 GCSB, to issue drafting instructions to Parliamentary Counsel to give effect to the above proposals;

27 agree that the GCSB Act as amended bind the Crown, consistent with the present approach under section 5 of the GCSB Act;

28 authorise the Minister Response for GCSB and the Attorney-General to make any decisions on additional matters that are necessary to give effect to the above proposals, and that are consistent with Cabinet decisions.

Sam Gleisner
Committee Secretary

Distribution:
Cabinet Committee on Domestic and External Security
18 Office of the Prime Minister
19 Chief Executive, DPMC
20 Director, Security and Risk, DPMC
21 Director, Intelligence Coordination Group, DPMC
22 Director, National Assessments Bureau, DPMC
23 Director, NZSIS
24 Director, GCSB
25 Secretary to the Treasury
26 Secretary for Justice
27 Privacy Commissioner
28 Secretary of Foreign Affairs and Trade
29 Secretary of Defence
30 Chief of Defence Force
31 State Services Commissioner
32 Commissioner of Police
33 Minister of Customs
34 Comptroller of Customs
35 Chief Parliamentary Counsel

s6(a)

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.

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

Objectives and Functions

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.

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. Being unable to take part fully in this partnership – for example, if the Act hindered the Bureau from participating in joint threat analysis or from sharing its own discoveries with partners – would substantially degrade the Bureau's capability in this area, with a consequential impact on its capacity to protect New Zealand networks from cyber threats.

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

s9(2)(h)

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 s6(a) 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. s6(a) 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).

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.

Powers, Controls and Limitations

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

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);
- to collect metadata (described further below) in bulk and analyse foreign metadata components for foreign intelligence purposes;
- to scan internet traffic for advanced cyber threats and deal with these in a way that promotes the protection of New Zealanders and New Zealand information infrastructures in a modern telecommunications environment; and
- 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.

37. In the current telecommunications environment, it is generally impossible to know for certain whether a particular communication is "foreign" or "domestic" at the point of interception. Electronic communication takes place without regard for nationality or borders, and may be routed anywhere in the world before it reaches its destination (even if that destination is the same city in which it started). The information is only capable of being filtered after collection. A restriction on collection that demands to know in advance that a communication is definitely "foreign" is therefore unworkable and, indeed, virtually meaningless in the internet age.

38. The same technical constraints are hindering the Bureau in effectively carrying out its foreign intelligence function. Modern tools permit the analysis of very large volumes of data generating considerable information s6(a) and so on, in relation to foreign organisations and foreign persons without needing to touch the content of any communication (that is, without retrieving the particular conversation that was held or the particular message that was sent). This activity, known as "metadata analysis", is considered to be fundamental in the toolkit of any signals intelligence agency.

39. Because of the way digital communications are managed and routed globally, however, it is impossible to exclude metadata generated by New Zealanders at the point of collection: indeed, the metadata itself can be an important factor in determining that a particular communication is a New Zealand communication and should be disregarded. Equally, when a New Zealand selector (such as a phone number) is happened upon, it should be possible for the Bureau to continue its analysis of the broader data set for foreign intelligence purposes, provided that no specific analysis is carried out on that New Zealand selector.

40. Finally, section 14 is impeding the Bureau in its function of assisting other entities. The most compelling example may be activities which are carried out for benevolent purposes. For example, in the event that a member of New Zealand's armed forces is taken hostage while on duty overseas, the New Zealand Defence Force has a responsibility to seek the safe return of that person. s6(a) Section 14 of the Act prohibits the Bureau from intercepting the communications of New Zealanders even when assisting an agency with its lawful duties in benevolent circumstances like these, s6(a)

s6(a)

s6(a) [redacted]

42. Metadata collected incidentally by the Bureau while carrying out its foreign intelligence function can be a powerful tool to generate leads s6(a) [redacted] it is important to preserve the Bureau's ability to retain and communicate such information incidentally obtained.

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. As communication shifts inexorably towards increased use of the internet carried over fibre, these issues will intensify, continuously degrading the Bureau's ability to perform its functions.

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:

- 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)
- Permit the Bureau to collect metadata in bulk and analyse foreign metadata components for foreign intelligence purposes
- Permit the Bureau to scan internet traffic for advanced cyber threats and deal with these in a way that promotes the protection of New Zealanders and New Zealand information infrastructures in a modern telecommunications environment
- 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.

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 specified types of computer network operation, or 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

- 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. In response, NZSIS recently obtained Cabinet approval to apply principle 5 without modification; and to apply principles 1, 8 and 9, modified as necessary to achieve the effective and efficient performance by the Service of its functions [DES Min (13) 1/4]. In the interests of enhancing privacy protections for New Zealanders, it is proposed that Cabinet agree to take a similar approach to the Bureau.

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 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, as has previously been agreed by Cabinet in respect of the review of NZSIS legislation [DES Min (13) 1/4 refers], 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. Together with changes to be made to the NZSIS legislation, 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.

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;

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;

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);

s9(2)(h)

    13.4 permitting the Bureau to scan internet traffic for advanced cyber threats and to deal with these in a way that promotes the protection of New Zealanders and New Zealand information infrastructures in a modern telecommunications environment;

    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 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, in line with recent Cabinet decisions in respect of NZSIS [DES Min (13) 1/4]:

    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, in line with recent Cabinet decisions in respect of NZSIS [DES Min (13) 1/4], 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;

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.

Christopher Finlayson

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

22 / 3 /2013

REGULATORY IMPACT STATEMENT

Government Communications Security Bureau Act Review

Agency Disclosure Statement

1. This regulatory impact statement has been prepared by the Department of Prime Minister and Cabinet with the Government Communications Security Bureau.
2. It provides an analysis of options to update and amend the Government Communications Security Bureau Act 2003 (the GCSB Act) to respond to the findings and recommendations of the recent review of compliance at GCSB carried out by Rebecca Kitteridge, and to respond to changes in GCSB's operating environment.
3. The analysis of options was conducted as part of a wider New Zealand Intelligence Community Policy and Legislation Review project, which included an existing review of the New Zealand Security Intelligence Service Act 1969 and a review of legislation providing for oversight mechanisms (the Intelligence and Security Committee Act 1996 and the Inspector-General of Intelligence and Security Act 1996). The analysis of options took into account the work on these other reviews, and the compliance review.
4. The GCSB Act contains intrusive state powers. Consequently any review of the GCSB Act will involve the consideration of human rights and privacy matters. Respect for human rights, and individual privacy and traditions of free speech in New Zealand were guiding principles in undertaking the review and developing recommendations.

Rajesh Chhana
Intelligence Co-ordination Group
Department of Prime Minister and Cabinet

22 March 2013

Status quo and problem definition

5. The GCSB has a vital role to play in protecting the security and safety of New Zealanders. Together with the other New Zealand Intelligence Community agencies, the GCSB contributes to the protection of the national security of New Zealand.

6. The GCSB was continued and established as a department of State by the Government Communications and Security Bureau Act 2003 (GCSB Act). The GCSB Act has not been amended since its enactment in 2003.

7. The GCSB Act sets out the objectives and functions of the GCSB, specifies the intrusive powers Parliament has necessarily provided to the GCSB to fulfill its functions and the related authorisation processes. The ability to exercise such powers comes with responsibility – responsibility to operate within the law and consequently to maintain the confidence of everyday New Zealanders.

8. In October 2012 Rebecca Kitteridge was seconded from the Cabinet Office to the GCSB to undertake a review of compliance at GCSB to provide assurance to the GCSB Director that the GCSB's activities are undertaken within its powers and that adequate safeguards are in place. Ms Kitteridge briefed officials working on the New Zealand Intelligence Community Policy and Legislation Review project about her review, and her findings have been taken into account in developing the proposals referred to in this paper.

9. Two broad problems with the GCSB Act have been identified. First, while the GCSB Act provides for and authorises its current activities, it is not easy to determine whether any given activity falls within the scope of the prescribed functions of the GCSB or not. A considerable amount of legal analysis about the interplay of different provisions within the GCSB Act is needed to arrive at any such conclusion.

10. This situation is not satisfactory. The foundation of effective oversight is having a clearly formulated and consistent statutory framework. The lack of such a framework makes management and oversight of the GSCB very difficult, having to rely as it does on extensive and complex analysis of the meaning of the GCSB Act. The only responsible course of action when dealing with intrusive powers is to make the legislation clearer and more transparent.

11. Second, since the enactment of the GCSB Act in 2003 there have been a number of changes in the threat environment facing New Zealand, particularly in the area of cyber security, and developments in the law relating to privacy and search and surveillance. The issues that require the GCSB Act to be updated can be summarised under four headings.

Changing information security requirements

12. The cyber environment continues to innovate at a remarkable pace, fueling economic growth and international trade opportunities. Consequently, there is an increasing shift of activity, both business and government, to that environment. To counter the threat to business and government information the Government launched the New Zealand Cyber Security Strategy in June 2011 (NZCSS).

13. The GCSB currently has as one of its core functions information security and assurance. The advanced capabilities developed through GSCB's intelligence work mean it is

uniquely placed to contribute to responses to cyber security issues. That is why, as part of the NZCSS, the National Cyber Security Centre (NCSC) was created within the GCSB. The Cabinet has indicated its expectation that the GCSB will considerably enhance its cyber security capabilities and use its expertise to assist a range of organisations (government, state sector, critical national infrastructure providers, and key economic contributors). However, the implementation of the NCSC has highlighted limitations on the ability of GCSB to contribute to this work because of the provisions of the GCSB Act (for example it is not clear that the GCSB can provide advice and assistance to private sector entities in New Zealand).

14. The impact of cyber threats is difficult to quantify precisely, but the NZCSS sets out some of the potential impacts, as well as some estimates suggesting New Zealanders lose up to $500m annually due to cyber-borne frauds and scams. Recent statistics on the NCSC website indicate that in the last 12 months cyber crime against New Zealanders cost $625m, and the global cost was estimated at up to $460 billion.

15. More broadly, the monetized cost of loss of intellectual property as a result of cyber intrusions into private sector entities is exceptionally difficult to quantify, in part because companies are reluctant to report losses or may not even know their property has been stolen. However, based on the scale of intrusions and exfiltrations seen in other jurisdictions and the number of intrusions reported in New Zealand the potential costs to New Zealand of cyber-based industrial espionage are likely to be significant.

16. Internationally the trend has been described as shifting from "exploitation" to "disruption" and "destruction". In other words the cyber threat is changing from theft of personal and intellectual property, to denial of service attacks and destruction of computer networks.

17. The NCSC 2012 Incident Summary reported that there was a significant increase (from 90 to 134) in the number of reported serious attacks against New Zealand government agencies, critical national infrastructure and private sector organisations.

18. If a major attack was directed at government agencies, critical national infrastructure providers (for example telecommunications networks and water supply) or companies that drive New Zealand's economy, there could be significant disruption to commercial and personal activities. It would also put at risk New Zealand's political and business reputation.

Changing security environment

19. The security environment New Zealand faces today presents new challenges. Globalisation means that New Zealand is no longer as distant from security problems as it was in the past. Security issues are increasingly interconnected and national borders are less meaningful. The increasing level of innovation in the cyber environment and the ubiquity of internet-based services is giving rise to new security threats and vulnerabilities. The GCSB Act was enacted 10 years ago when cyber matters were less sophisticated and prominent.

Changing public law environment

20. The legal environment in which the GCSB Act is interpreted has developed since its enactment. The courts' consideration of law enforcement cases has provided further guidance about how intrusive state powers should be set out in statute, and highlight areas where powers may no longer be effective given the change in the

telecommunications environment. For law enforcement agencies these issues were reviewed comprehensively over a number of years, and were addressed in the Search and Surveillance Act 2012.

Better Public Services

21. In addition to the issues above, the GCSB plays a crucial role in the support of other government agencies, in particular the New Zealand Defence Force and the NZSIS. The GCSB also supports the New Zealand Police in the detection and investigation of serious crime. The GCSB's unique capabilities are an invaluable resource for those agencies to draw upon.

22. The GCSB Act review considered that in a small jurisdiction such as New Zealand we cannot afford to duplicate expensive and sophisticated assets, and there are limited numbers of people that can work with such assets. Consistent with the Better Public Services programme, the capabilities such as those developed or acquired by the GCSB, where appropriate and subject to necessary safeguards, should be available to assist in meeting key Government priorities. This too should be addressed in the update of the GCSB Act.

Objectives

23. The objectives of the GSCB Act review are:

- To provide for greater and more effective oversight at all levels (internally by the Director, at ministerial level by the responsible Minister and externally by the Inspector-General and the Intelligence and Security Committee).
- To enable the GCSB to respond to the changing security environment, cyber and information security environment, and the changes in the public law environment since the GCSB Act was passed in 2003.

Regulatory Impact Analysis

24. Three policy options were assessed:

- non-legislative solutions;
- amending the GCSB Act;
- repealing and replacing the GCSB Act.

Non-legislative solutions

25. As noted above the GCSB Act is a piece of legislation that sets out and provides safeguards for the use of intrusive state powers. The GCSB cannot address any new threats beyond those it is permitted to address in its legislation.

26. The difficulties associated with the interpretation of the GCSB Act could be addressed by developing detailed guidance material, but it would be of limited benefit and consume considerable time and expenditure on legal advice to develop. This would not substantially address the need to improve management and external oversight of the GSCB.

27. Non-legislative solutions cannot satisfactorily meet the two objectives.

Amending the GCSB Act

28. The GCSB Act currently provides for three functions;

    - Foreign intelligence
    - Information security and assurance
    - Co-operation and assistance to other entities

29. The two objectives could be met by updating and clarifying the current functions set out in the GCSB Act. It is not considered that any new functions need to be added, but a refresh of the way in which the functions are articulated would ensure that the functions fit the changing operational environment, as well as providing greater clarity about what GCSB's functions actually are. These changes would complement and amplify the proposals to strengthen oversight by the Inspector-General of Intelligence and Security.

30. In the case of the foreign intelligence and cooperation functions, both would need to be clarified to allow for more effective oversight, and in the case of co-operation a ministerial authorisation process could be included in the GCSB Act to provide a way of determining who GCSB can work with and under what circumstances.

31. The information security and assurance function in the GCSB Act focuses almost entirely on providing protective services to public sector entities. However, threats in the cyber environment also put at grave risk our critical infrastructure and businesses that drive our economy. This function needs to be given more prominence. So too the expectations of the GCSB in safeguarding New Zealand information, in both public and private sectors, needs to be made clear.

32. The GCSB Act currently sets out three types of powers:

    - Warrantless powers of interception and access
    - Interception warrants
    - Computer network access authorisations

33. These powers are contained in Part 3 of the GCSB Act along with other provisions that control the use of those powers.

34. The objective of greater and more effective oversight would be met by still requiring the current range of authorisations but amending the GCSB Act so the authorisation processes are more transparent and consistent.

35. In order to meet the second objective, while the range of powers available to the GCSB does not need to be expanded the GCSB Act would be amended to make it clear that the powers can be used for both the foreign intelligence function and the information security and assurance function. The powers are needed to support the information security and assurance function to give the GCSB the ability to respond effectively to emerging cyber threats against New Zealanders.

36. The basic premise underpinning the operations of the GCSB that it does not conduct foreign intelligence activities against New Zealanders will be retained (currently contained in section 14 of the GCSB Act). However, because the information security and assurance function is about protecting New Zealanders, an amendment will also be required to allow the GCSB to see who (namely New Zealand individuals and

companies) is being attacked. This would allow the GCSB to determine where the threats are being generated from and develop measures to counter those threats.

37. Finally, amendments could be made to update the description of the powers to accommodate changes in how communication are now carried and routed around the world. This would be similar to the work undertaken for law enforcement powers in the Search and Surveillance Act 2012.

38. The costs of developing and drafting the proposed amendments and implementing them fall on the Government. The GCSB Act applies to the operation of the GCSB consequently the costs are part of its core operating expenses, and no compliance costs for business arise.

39. This approach would have the following outcomes and benefits:

Outcomes	Benefits
Greater clarity of the law governing the operation and administration of the GCSB	Provides basis for more effective oversight by external oversight bodies, thereby enhancing public trust and confidence.
	Responds to changes in the public law environment so that the law reflects current jurisprudence and is relevant to the current technological environment.
	Provides clarity to the public on the functions and powers of the GCSB.
	Provides clarity to staff and enhances management oversight of GCSB activities.
GSCB functions updated to allow GCSB to meet new threats, in particular cyber security.	Enables GCSB to support private sector in addition to public sector entities to counter cyber threats, which currently have an estimated impact on New Zealanders of over $0.50 billion in terms of cyber crime alone.
	Enables GCSB to more effectively detect and respond to cyber threats by allowing it to use the powers in the GCSB Act when undertaking its information security and assurance function.
	Allow GCSB to better fulfill the functions of the NCSC and play an effective part in the delivery of the NZCSS along with the other agencies tasked with its delivery.
GCSB able to assist and advise other Government agencies fulfill their lawful functions with its technical capabilities and expertise.	Other agencies will not have to duplicate technical capabilities and expertise already held by the Crown, and make effective and efficient use of the GCSB's capabilities.

Repealing and replacing the GCSB Act

40. The two objectives could be achieved by taking a more expansive approach to updating the GCSB's establishment statute, by repealing it and replacing it with a new statute.

41. The benefit of this approach, over and above the option to amend the GCSB Act, is that it would result in a new Act that would pick up the changes described in the discussion of the option to amend the GCSB Act as well as providing an opportunity to reenact all other existing provisions with updated drafting where necessary. However, as discussed above, the number of changes required to achieve the objectives can be targeted at particular parts and sections of the GCSB Act and the basic construction of the GCSB Act does not need to change to accommodate those amendments.

42. Consequently there does not seem to be any great benefit associated with dedicating additional time and resources to redrafting and reenacting provisions that do not need to be changed.

Consultation

43. The policy development process was undertaken by the New Zealand Intelligence Community (DPMC – lead, with GCSB, and NZSIS). The agencies consulted were the Ministry of Foreign Affairs and Trade, New Zealand Defence Force, New Zealand Police, New Zealand Customs Service, Ministry of Defence, Ministry of Justice, Office of the Privacy Commissioner, State Services Commission and the Treasury.

44. Given the nature of the issues being dealt with and the national security classifications associated with the material, there was no public consultation process. Public consultation on the proposals will occur during the parliamentary consideration of the amending legislation.

Conclusions and recommendations

45. As discussed above, the identified problems do not require a change to the scheme of the GCSB Act and the objectives of the review can be met by amendments to targeted provisions. The benefits of dedicating resources to a full redrafting of the Act are consequently limited. The recommended option is to amend the GCSB Act to address the identified issues and meet the objectives of the reform.

Implementation

46. The compliance review of the GCSB has a range of recommended changes to the compliance framework and operations of the GCSB. The GCSB is developing an implementation plan to respond to those recommendations, and the implementation of the amendments to the GCSB Act will be incorporated into that plan.

Monitoring, Evaluation and Review

47. The GCSB will monitor the effectiveness of the amendments and advise the Minister about any issues arising.

File

Item 7

DES Min (13) 3/2-3

Copy No: 15

Cabinet Committee on Domestic and External Security

Minute of Decision

Review of the Government Communications Security Bureau Act 2003

Portfolio: Minister Responsible for the GCSB

On 26 March 2013, the Cabinet Committee on Domestic and External Security (DES), having taken Power to Act in accordance with its Terms of Reference:

Background

1 **noted** that in December 2012, DES agreed that a review of the Government Communications Security Bureau Act 2003 (the GCSB Act) be undertaken [DES Min (12) 4/1-1];

2 **noted** that the GCSB 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;

3 **noted** that on 26 March 2013, DES took decisions on amendments to the Intelligence and Security Committee Act 1996 and the Inspector General of Intelligence and Security Act 1996 to provide for new external oversight mechanisms [DES Min (13) 3/1];

Objective and functions

4 **agreed** that section 7 of the GCSB 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:

4.1 information assurance/cyber security;

4.2 foreign intelligence;

4.3 co-operating with other entities;

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

6 **agreed** that the description of the Bureau's information assurance/cyber security function 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;

7 **agreed** that the Bureau's foreign intelligence function 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;

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

9 **noted** that, based on the approach in paragraphs 4-8 above, section 8 of the GCSB Act (Functions of Bureau) will be amended to craft a description of the Bureau's three core functions around the following elements:

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

9.2 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;

9.3 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;

10 **noted** that officials will consult with the Responsible Minister and the Attorney-General when drafting the description of the Bureau's core functions;

Powers, controls and limitations

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

12 **noted** that section 14 of the GCSB 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;

13 **noted** 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 the government expects the Bureau to fulfil;

14 **agreed** that the approach in section 14 of the GCSB Act be modified in a way that resolves the unanticipated effects of that provision, including:

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

14.2 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);

14.3 permitting the bureau to collect metadata in bulk and analyse foreign metadata components for foreign intelligence purposes;

14.4 permitting the Bureau to scan internet traffic for advanced cyber threats and to deal with these in a way that promotes the protection of New Zealanders and New Zealand information infrastructures in a modern telecommunications environment;

15 **agreed in principle**, subject to paragraph 28 below, that the approach in section 14 of the GCSB Act be modified in a way that resolves the unanticipated effects of that provision, including 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);

16 **agreed** that:

16.1 the concept of "incidentally obtained intelligence" reflected in section 25 of the GCSB Act be retained;

16.2 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;

17 **agreed in principle**, subject to paragraph 28 below, that the GCSB Act be amended to incorporate a new mechanism to enhance Ministerial oversight of Bureau activities, through which the Minister would specify particularly sensitive or non-routine activities or classes of activities requiring explicit Ministerial authorisation;

18 **agreed** that the conditions under which Ministerial authorisation may be granted be enhanced to include assurances that the activities proposed by the Bureau are necessary, justified and reasonable, and to provide consistently across the Ministerial authorisation mechanisms;

19 **agreed** the GCSB Act be amended to reflect that the Bureau may exercise its legislated powers to fulfil any of its prescribed functions;

20 **agreed** that 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

21 **noted** 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);

22 **agreed** that, in line with recent Cabinet decisions in respect of the NZSIS [DES Min (13) 1/4]:

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

22.2 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;

23 **agreed** that the GCSB Act be amended:

23.1 in line with recent Cabinet decisions in respect of the NZSIS [DES Min (13) 1/4], 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;

23.2 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;

23.3 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;

24 **agreed in principle**, subject to paragraph 28 below, that the GCSB Act 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 **noted** that consequential amendments may be needed to the provisions governing the execution of Ministerial authorisation;

26 **noted** that in October 2010, DES 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 [DES Min (10) 3/1];

27 **noted** that amendments to the GCSB Act are required to give effect to the proposal in paragraph 26 above;

Further consideration of Ministerial authorisations

28 **directed** the Bureau, in consultation with relevant departments, to report to DES as soon as possible with further information on proposals relating to Ministerial authorisations referred to in paragraphs 15, 17 and 24 above;

Legislative process

29 **noted** that in December 2012, DES:

29.1 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);

29.2 noted that the bill would be enacted by August 2013;

[DES Min (12) 4/1-1]

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

31 **agreed** that the GCSB Act as amended bind the Crown, consistent with the present approach under section 5 of the GCSB Act;

32 **authorised** the Minister Responsible for the GCSB and the Attorney-General to make any decisions on additional matters that are necessary to give effect to the above decisions, and that are consistent with previous decisions.

Sam Gleisner
Committee Secretary

References: DES (13) 10, DES (13) 11

Present:
Rt Hon John Key (Chair)
Hon Steven Joyce
Hon Judith Collins
Hon Christopher Finlayson
Hon Dr Jonathan Coleman
Hon Anne Tolley
Hon Amy Adams

Officials present from:
Office of the Prime Minister
Department of the Prime Minister and Cabinet
New Zealand Security Intelligence Service
Government Communications Security Bureau

Distribution: (see over)

Distribution:

Cabinet Committee on Domestic and External Security
18 Office of the Prime Minister
19 Chief Executive, DPMC
20 Director, Security and Risk, DPMC
21 Director, Intelligence Coordination Group, DPMC
22 Director, National Assessments Bureau, DPMC
23 Director, NZSIS
24 Director, GCSB
25 Secretary to the Treasury
26 Secretary for Justice
27 Privacy Commissioner
28 Solicitor-General
29 Secretary of Foreign Affairs and Trade
30 Secretary of Defence
31 Chief of Defence Force
32 State Services Commissioner
33 Commissioner of Police
34 Minister of Customs
35 Comptroller of Customs
36 Chief Parliamentary Counsel
37 Legislation Coordinator

File

Cabinet

CAB (13) 175

Copy No: 24

Decisions of the Cabinet Committee on Domestic and External Security

28 March 2013

Report of the Cabinet Committee on Domestic and External Security: Part 2: Period ended 28 March 2013

Cabinet is asked, as appropriate, to confirm the decisions or approve the recommendations in the attached report on the work of the Cabinet Committee on Domestic and External Security for the period ended 28 March 2013.

Part 1 of the DES Report with items classified "Restricted" is under CAB (13) 157.

Sam Gleisner
for Secretary of the Cabinet

The Cabinet Committee on Domestic and External Security met on 26 March 2013

SECRET

1 **Review of the GCSB Act 2003**
Portfolio: Minister Responsible for the GCSB
DES Min (13) 3/2-3, DES (13) 10, DES (13) 11

On 26 March 2013, the Cabinet Committee on Domestic and External Security (DES), having taken Power to Act in accordance with its Terms of Reference:

Background

1 **noted** that in December 2012, DES agreed that a review of the Government Communications Security Bureau Act 2003 (the GCSB Act) be undertaken [DES Min (12) 4/1-1];

2 **noted** that the GCSB 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;

3 **noted** that on 26 March 2013, DES took decisions on amendments to the Intelligence and Security Committee Act 1996 and the Inspector General of Intelligence and Security Act 1996 to provide for new external oversight mechanisms [DES Min (13) 3/1];

Objective and functions

4 **agreed** that section 7 of the GCSB 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:

4.1 information assurance/cyber security;

4.2 foreign intelligence;

4.3 co-operating with other entities;

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

6 **agreed** that the description of the Bureau's information assurance/cyber security function 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;

7 **agreed** that the Bureau's foreign intelligence function 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;

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

9 **noted** that, based on the approach in paragraphs 4-8 above, section 8 of the GCSB Act (Functions of Bureau) will be amended to craft a description of the Bureau's three core functions around the following elements:

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

9.2 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;

9.3 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;

10 **noted** that officials will consult with the Responsible Minister and the Attorney-General when drafting the description of the Bureau's core functions;

Powers, controls and limitations

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

12 **noted** that section 14 of the GCSB 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;

13 **noted** 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 the government expects the Bureau to fulfil;

14 **agreed** that the approach in section 14 of the GCSB Act be modified in a way that resolves the unanticipated effects of that provision, including:

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

14.2 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);

14.3 permitting the bureau to collect metadata in bulk and analyse foreign metadata components for foreign intelligence purposes;

14.4 permitting the Bureau to scan internet traffic for advanced cyber threats and to deal with these in a way that promotes the protection of New Zealanders and New Zealand information infrastructures in a modern telecommunications environment;

15 **agreed in principle**, subject to paragraph 28 below, that the approach in section 14 of the GCSB Act be modified in a way that resolves the unanticipated effects of that provision, including 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);

16 **agreed** that:

16.1 the concept of "incidentally obtained intelligence" reflected in section 25 of the GCSB Act be retained;

16.2 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;

17 **agreed in principle**, subject to paragraph 28 below, that the GCSB Act be amended to incorporate a new mechanism to enhance Ministerial oversight of Bureau activities, through which the Minister would specify particularly sensitive or non-routine activities or classes of activities requiring explicit Ministerial authorisation;

18 **agreed** that the conditions under which Ministerial authorisation may be granted be enhanced to include assurances that the activities proposed by the Bureau are necessary, justified and reasonable, and to provide consistently across the Ministerial authorisation mechanisms;

19 **agreed** the GCSB Act be amended to reflect that the Bureau may exercise its legislated powers to fulfil any of its prescribed functions;

20 **agreed** that 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

21 **noted** 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);

22 **agreed** that, in line with recent Cabinet decisions in respect of the NZSIS [DES Min (13) 1/4]:

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

22.2 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;

23 **agreed** that the GCSB Act be amended:

23.1 in line with recent Cabinet decisions in respect of the NZSIS [DES Min (13) 1/4], 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;

23.2 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;

23.3 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;

24 **agreed in principle**, subject to paragraph 28 below, that the GCSB Act 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 **noted** that consequential amendments may be needed to the provisions governing the execution of Ministerial authorisation;

26 **noted** that in October 2010, DES 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 [DES Min (10) 3/1];

27 **noted** that amendments to the GCSB Act are required to give effect to the proposal in paragraph 26 above;

Further consideration of Ministerial authorisations

28 **directed** the Bureau, in consultation with relevant departments, to report to DES as soon as possible with further information on proposals relating to Ministerial authorisations referred to in paragraphs 15, 17 and 24 above;

Legislative process

29 **noted** that in December 2012, DES:

29.1 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);

29.2 noted that the bill would be enacted by August 2013;

[DES Min (12) 4/1-1]

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

31 **agreed** that the GCSB Act as amended bind the Crown, consistent with the present approach under section 5 of the GCSB Act;

32 **authorised** the Minister Responsible for the GCSB and the Attorney-General to make any decisions on additional matters that are necessary to give effect to the above decisions, and that are consistent with previous decisions.

Cabinet

CAB Min (13) 10/8

Copy No: 6

Minute of Decision

Report of the Cabinet Committee on Domestic and External Security: Period Ended 28 March 2013

On 2 April 2013, Cabinet made the following decisions on the work of the Cabinet Committee on Domestic and External Security for the period ended 28 March 2013.

[Not in Scope]

DES Min (13) 3/2-3 **GCSB Item** CONFIRMED

for Secretary of the Cabinet

Reference: CAB (13) 157; CAB (13) 175

Distribution (see over)

Distribution:
Cabinet Committee on Domestic and External Security
Chief Executive, DPMC
Director, Security and Risk, DPMC
Director, Intelligence Coordination Group, DPMC
Director, National Assessments Bureau, DPMC
Manager, NCPO, DPMC
Director, NZSIS
Director, GCSB
Secretary to the Treasury
Secretary for Justice
Privacy Commissioner
Secretary of Defence
Chief of Defence Force
State Services Commissioner
Secretary of Foreign Affairs and Trade
Commissioner of Police
Chief Executive, MBIE (C&IT)
Minister of Internal Affairs
Secretary for Internal Affairs
Minister of Customs
Comptroller of Customs
Chief Parliamentary Counsel
Legislation Coordinator
Secretary, DES

File

Item 8

DES (13) 12

Copy No: 15

Cabinet Committee on Domestic and External Security

Summary of Paper

8 April 2013

This paper has been distributed for the Committee's consideration by round robin.

GCSB Act Review: Alternative Proposals on Ministerial Authorisation

Portfolio Minister Responsible for the GCSB

On 26 March 2013, the Cabinet Committee on Domestic and External Security (DES) took decisions on amendments to the Government Communications Security Bureau Act 2003 [DES Min (13) 3/2-3].

DES directed the GCSB, in consultation with other departments as required, to report to DES with further information on three proposals relating to Ministerial authorisations.

The Minister Responsible for the GCSB has approved the attached memorandum that addresses the proposals relating to Ministerial authorisations.

The Minister Responsible for the GCSB recommends that the Committee:

In principle decisions

1 note that in March 2013, the Cabinet Committee on Domestic and External Security agreed in principle that the:

1.1 approach in section 14 of the Government Communications Security Bureau Act 2003 (the GCSB Act) be modified in a way that resolves the unanticipated effects of that provision, including 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);

1.2 GCSB Act be amended to incorporate a new mechanism to enhance Ministerial oversight of Bureau activities, through which the Minister would specify particularly sensitive or non-routine activities or classes of activities requiring explicit Ministerial authorisation;

1.3 GCSB Act 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;

[DES Min (13) 3/2-3]

Confirmation of in principle decisions and alternative proposals

2 confirm the decision in paragraph 1.1 above, that the approach in section 14 of the GCSB Act be modified in a way that resolves the unanticipated effects of that provision, including 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;

3 agree that, in addition to the proposal in paragraph 2 above, the GCSB Act be amended to provide that the Bureau may assist:

3.1 the New Zealand Defence Force;

3.2 the New Zealand Police;

3.3 the New Zealand Security Intelligence Service; or

3.4 any other department prescribed by regulations for the purpose, subject to such authorisation requirements or limitations that the Responsible Minister considers appropriate;

4 note that under section 8(3) of the GCSB Act, the performance of the Bureau's functions is subject to the control of the Responsible Minister;

5 agree not to proceed with the decision in paragraph 1.2 above;

6 confirm the decision in paragraph 1.3 above;

7 invite the Minister Responsible for the GCSB to confirm drafting instructions to the Parliamentary Counsel Office to give effect to the above proposals.

Sam Gleisner
Committee Secretary

Distribution: (see over)

Distribution:
Cabinet Committee on Domestic and External Security
18 Office of the Prime Minister
19 Chief Executive, DPMC
20 Director, Security and Risk, DPMC
21 Director, Intelligence Coordination Group, DPMC
22 Director, National Assessments Bureau, DPMC
23 Director, NZSIS
24 Director, GCSB
25 Manager, NCPO
26 Secretary to the Treasury
27 Secretary for Justice
28 Privacy Commissioner
29 Solicitor-General
30 Secretary of Foreign Affairs and Trade
31 Secretary of Defence
32 Chief of Defence Force
33 State Services Commissioner
34 Commissioner of Police
35 Minister of Customs
36 Comptroller of Customs

s6(a)

Office of the Prime Minister

The attached memorandum has been authorised by the Prime Minister for consideration by the Cabinet Committee on Domestic and External Security.

Paula Oliver
Deputy Chief of Staff

GCSB Act Review: Alternative Proposals on Ministerial Authorisation

1 The Cabinet paper on the Review of the GCSB Act (Paper 2) recommended amending the Act to include a requirement to seek Ministerial authorisation in two circumstances not covered by the existing legislation:

- before the Bureau could agree to a request for advice or assistance from another agency (para 29)
- before conducting particularly sensitive or non-routine activities (specified in advance by the Responsible Minister through written Ministerial directions) (para 52)

2 The rationale for this proposal was that activities such as assisting another agency by collecting information on New Zealanders, while technically lawful under the proposed new legislative framework, are nevertheless sensitive and might be at the margins of public acceptability of the Bureau's intrusive powers. The assessment was that enhanced Ministerial oversight and control was an appropriate corollary. It was envisaged that authorisation could be granted on a case-by-case basis, or on a class basis for a specified period of time, depending on the degree of sensitivity of the proposed activity.

3 The Cabinet paper on the Review of the GCSB Act (Paper 2) also recommended amending the Act to include alternative avenues for obtaining Ministerial authorisation in situations of urgency when the Responsible Minister is not readily available. The rationale for this proposal was to allow for some flexibility in circumstances where Ministerial authorisation was required within a short timeframe.

Co-operating with Other Entities

4 It is not essential for the proposals on co-operation to impose formal Ministerial authorisation requirements in order to deliver a satisfactory level of assurance that the Bureau is conducting itself in a lawful and acceptable manner.

5 As it stands, the proposal is that the Bureau would only be authorised to assist another agency with any activity that the other agency is lawfully able to conduct itself, and subject to any limitations imposed by law on that agency in performing its lawful duties. This approach sets a clear threshold for assistance by the Bureau: the activity must first and foremost be lawful for the other agency to conduct, whether under inherent powers, or statutory powers, or under an instrument such as a surveillance device warrant or an intelligence warrant duly granted by the appropriate authority. The approach also contemplates the Bureau's assistance being confined by any limitations imposed by law on the other agency in carrying out its duties. In short, the powers and the limitations that apply to the agency requesting assistance would apply equally in respect of any assistance by the Bureau.

6 A legal ability to provide assistance does not impose an obligation to assist. The decision whether or not to render assistance in any given instance would still be made by the Director of GCSB who may, depending on the particular activity being considered, choose to consult the Responsible Minister before making a final decision. While the Minister would no

longer have a statutory role in approving assistance activities, he or she nevertheless remains in formal control of the Bureau's activities in accordance with section 8(3) of the Act, which states: "The performance of the Bureau's functions is subject to the control of the Minister."

7 In performing its co-operation function, the Bureau provides support primarily to the New Zealand Defence Force, the New Zealand Police and the New Zealand Security Intelligence Service. It would be possible for the legislation to explicitly authorise assistance to these agencies on the terms outlined above, without further recourse to the Responsible Minister. For additional flexibility, the legislation could provide that the Bureau may assist any other department prescribed by regulations for the purpose, and subject to any additional authorisation process or limitations that were considered appropriate in each case. This would enable other agencies – in particular law enforcement agencies – to receive the benefit of the Bureau's expertise and capabilities in the right circumstances subject to Cabinet approval.

8 External oversight of the Bureau's co-operative activities under the approach proposed here would fall to the Inspector-General of Intelligence and Security. The clarification of the Bureau's co-operation function proposed in the Cabinet paper sits within a context of enhanced oversight by the Inspector-General, which will provide a level of assurance that the Bureau is acting strictly within the legal parameters that have been set for it.

9 The approach outlined above has implications for Recommendation 15 of DES minute (13) 3/2-3. Under the alternative approach discussed here, the Recommendation could be confirmed in the following terms:

> **confirm** that the approach in section 14 of the GCSB Act be modified in a way that resolves the unanticipated effects of that provision, including 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;

10 Two additional recommendations would provide the wider context of Cabinet and Ministerial control in the following terms:

> **agree** that the GCSB Act should be amended to provide that the Bureau may assist:
>
> - the New Zealand Defence Force;
> - the New Zealand Police;
> - the New Zealand Security Intelligence Service; or
> - any other department prescribed by regulations for the purpose, subject to such authorisation requirements or limitations that the Responsible Minister considers appropriate;

note that, under section 8(3) of the GCSB Act, the performance of the Bureau's functions is subject to the control of the Responsible Minister;

Ministerial Authorisation for Other Activities

11 The Cabinet paper also proposed a new mechanism to enable the Responsible 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.

12 After further consideration, given 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, this additional mechanism is no longer considered necessary.

13 This approach will need to be reconciled with that set out in Recommendation 17 of DES minute (13) 3/2-3, which could be done as follows:

rescind recommendation 17 of DES minute (13) 3/2-3;

Ministerial Authorisation in Situations of Urgency

14 The Cabinet paper on the Review of the GCSB Act (Paper 2) also recommended amending the Act to include alternative avenues for obtaining Ministerial authorisation in situations of urgency when the Responsible Minister is not readily available.

15 Under the GCSB Act as it stands, only the Responsible Minister has authority to grant an interception warrant or a computer access authorisation. This restriction introduces a degree of inflexibility in the authorisation process, which can result in unforeseen and awkward delays in responding to issues of national security as they arise. Sometimes delay is necessary so that appropriate consideration can be given to the issue at hand. However, it would be desirable if the authorisation process could be more flexible in situations of urgency when the Responsible Minister is not readily available. It is proposed to amend the Act to provide alternative avenues for obtaining Ministerial authorisation in these situations. 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.

16 The approach outlined above is currently captured by Recommendation 24 of DES minute (13) 3/2-3, which could be confirmed as follows:

confirm that the GCSB Act 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;

Cabinet Committee on Domestic and External Security

DES Min (13) 4/1

Copy No: 15

Minute of Decision

GCSB Act Review: Ministerial Authorisation

Portfolio: Minister Responsible for the GCSB

In April 2013, the Cabinet Committee on Domestic and External Security (DES) by round robin, and having taken Power to Act in accordance with its terms of reference:

In principle decisions

1 **noted** that in March 2013, DES agreed in principle that the:

1.1 approach in section 14 of the Government Communications Security Bureau Act 2003 (the GCSB Act) be modified in a way that resolves the unanticipated effects of that provision, including 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);

1.2 GCSB Act be amended to incorporate a new mechanism to enhance Ministerial oversight of Bureau activities, through which the Minister would specify particularly sensitive or non-routine activities or classes of activities requiring explicit Ministerial authorisation;

1.3 GCSB Act 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;

[DES Min (13) 3/2-3]

Confirmation of in principle decisions

2 **confirmed** the decision in paragraph 1.1 above, that the approach in section 14 of the GCSB Act be modified in a way that resolves the unanticipated effects of that provision, including 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;

3 **agreed** that, in addition to the decision in paragraph 2 above, the GCSB Act be amended to provide that the Bureau may assist:

3.1 the New Zealand Defence Force;

3.2 the New Zealand Police;

3.3 the New Zealand Security Intelligence Service; or

3.4 any other department prescribed by regulations for the purpose, subject to such authorisation requirements or limitations that the Responsible Minister considers appropriate;

4 **noted** that under section 8(3) of the GCSB Act, the performance of the Bureau's functions is subject to the control of the Responsible Minister;

5 **agreed** not to proceed with the decision in paragraph 1.2 above;

6 **confirmed** the decision in paragraph 1.3 above;

7 **invited** the Minister Responsible for the GCSB to confirm drafting instructions to the Parliamentary Counsel Office to give effect to the above decisions.

Sam Gleisner
Committee Secretary

Reference: DES (13) 12

Distribution:
Cabinet Committee on Domestic and External Security
18 Office of the Prime Minister
19 Chief Executive, DPMC
20 Director, Security and Risk, DPMC
21 Director, Intelligence Coordination Group, DPMC
22 Director, National Assessments Bureau, DPMC
23 Director, NZSIS
24 Director, GCSB
25 Manager, NCPO
26 Secretary to the Treasury
27 Secretary for Justice
28 Privacy Commissioner
29 Solicitor-General
30 Secretary of Foreign Affairs and Trade
31 Secretary of Defence
32 Chief of Defence Force
33 State Services Commissioner
34 Commissioner of Police
35 Minister of Customs
36 Comptroller of Customs

s6(a)

File

Cabinet

CAB Min (13) 13/6(A)

Copy No: 4

Minute of Decision

GCSB Act Review: Ministerial Authorisation

Portfolio: Minister Responsible for the GCSB

On 22 April 2013, following reference from the Cabinet Committee on Domestic and External Security, Cabinet:

In principle decisions

1 **noted** that in March 2013, DES agreed in principle that the:

1.1 approach in section 14 of the Government Communications Security Bureau Act 2003 (the GCSB Act) be modified in a way that resolves the unanticipated effects of that provision, including 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);

1.2 GCSB Act be amended to incorporate a new mechanism to enhance Ministerial oversight of Bureau activities, through which the Minister would specify particularly sensitive or non-routine activities or classes of activities requiring explicit Ministerial authorisation;

1.3 GCSB Act 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;

[DES Min (13) 3/2-3]

Confirmation of in principle decisions

2 **confirmed** the decision in paragraph 1.1 above, except the part relating to Ministerial authorisation, that the approach in section 14 of the GCSB Act be modified in a way that resolves the unanticipated effects of that provision, including 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;

3 **agreed** that, in addition to the decision in paragraph 2 above, the GCSB Act be amended to provide that the Bureau may assist:

3.1 the New Zealand Defence Force;

3.2 the New Zealand Police;

3.3 the New Zealand Security Intelligence Service; or

3.4 any other department prescribed by regulations for the purpose, subject to such authorisation requirements or limitations that the Responsible Minister considers appropriate;

4 **noted** that under section 8(3) of the GCSB Act, the performance of the Bureau's functions is subject to the control of the Responsible Minister;

5 **agreed** not to proceed with the decision in paragraph 1.2 above;

6 **confirmed** the decision in paragraph 1.3 above;

7 **invited** the Minister Responsible for the GCSB to confirm drafting instructions to the Parliamentary Counsel Office to give effect to the above decisions.

for Secretary of the Cabinet

Reference: CAB (13) 226

Secretary's note: *This minute replaces DES Min (13) 4/1. Paragraph 2 has been amended to clarify the scope of the decision.*

Distribution:

10 Prime Minister
11 Chief Executive, DPMC
12 Director, Security and Risk, DPMC
13 Director, Intelligence Coordination Group, DPMC
14 Director, National Assessments Bureau, DPMC
15 Manager, NCPO, DPMC
16 Director, NZSIS
17 Director, GCSB
18 Secretary to the Treasury
19 Secretary for Justice
20 Privacy Commissioner
21 Solicitor-General
22 Secretary of Foreign Affairs and Trade
23 Secretary of Defence
24 Chief of Defence Force
25 State Services Commissioner
26 Commissioner of Police
27 Minister of Customs
28 Comptroller of Customs
29 Min of Finance
30 Min of Justice
31 Attorney-General
32 Min of Foreign Affairs
33 Min of Defence
34 Min of Police

Item 9

Cabinet

CAB (13) 239

Copy No: 1

Summary of Paper

3 May 2013

Government Communications Security Bureau and Related Legislation Amendment Bill: Approval for Introduction

Portfolios: Minister Responsible for the GCSB / Minister in Charge of the NZSIS

On 22 April 2013, Cabinet authorised a group of Ministers (Joint Ministers), comprising the Prime Minister, Hon Bill English, Hon Steven Joyce, Hon Christopher Finlayson and Hon Amy Adams to have Power to Act to finalise the intelligence bill and the interception and network security bill for introduction, subject to final consideration by Cabinet on 6 May 2013 [CAB Min (13) 13/24].

On 2 May 2013, Joint Ministers finalised the contents of the Government Communications Security Bureau and Related Legislation Amendment Bill (the Amendment Bill).

Cabinet approval is sought for the introduction of the Amendment Bill in accordance with the decision on 22 April above.

The Minister Responsible for the GCSB and the Minister in Charge of the New Zealand Security Intelligence Service recommend that Cabinet:

Background

1 note that in December 2012, the Cabinet Committee on Domestic and External Security (DES):

1.1 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);

1.2 noted that the Bill would be enacted by August 2012;

[DES Min (12) 4/1-1]

Government Communications Security Bureau and Related Legislation Amendment Bill

2 note that the Government Communications Security Bureau and Related Legislation Amendment Bill (the Amendment Bill) is an omnibus Bill that amends the Government Communications Security Bureau Act 2003, the Inspector-General of Intelligence and Security Act 1996, and the Intelligence and Security Committee Act 1996;

3 note that on 22 April 2013, Cabinet authorised a group of Ministers (Joint Ministers), comprising the Prime Minister, Hon Bill English, Hon Steven Joyce, Hon Christopher Finlayson and Hon Amy Adams to have Power to Act to finalise the intelligence bill and the interception and network security bill for introduction, subject to final consideration by Cabinet on 6 May 2013 [CAB Min (13) 13/24];

4 note that on 2 May 2013 the Joint Ministers referred to in paragraph 3 above approved the contents of the Amendment Bill for introduction;

5 confirm the decision by the Joint Ministers to approve for introduction the Government Communications Security Bureau and Related Legislation Amendment Bill [PCO 17322/9.0];

6 agree that the Amendment Bill be introduced as soon as possible after consideration by Cabinet;

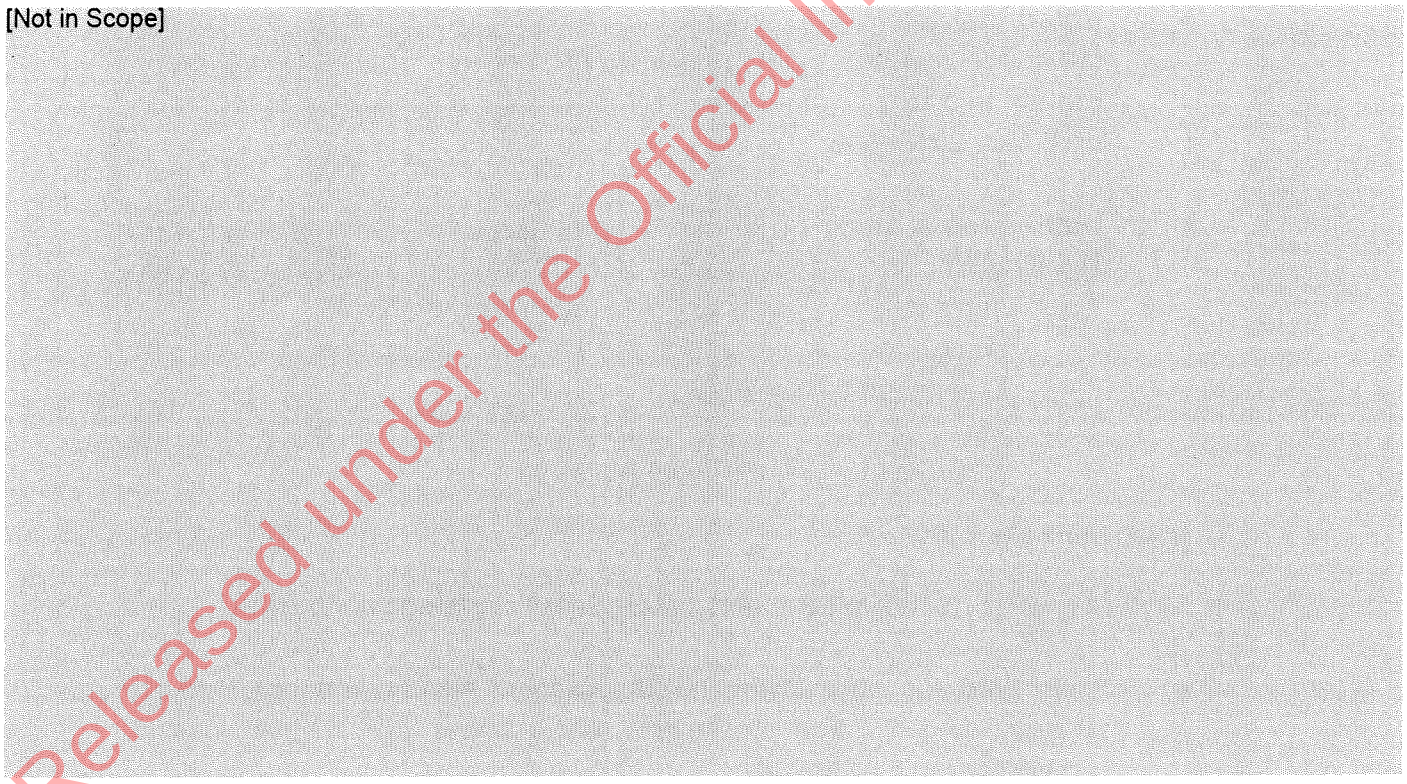
7 agree that the government propose that the Amendment Bill be:

7.1 referred to the Intelligence and Security Committee for consideration;

7.2 reported back by 26 July 2013;

7.3 enacted by August 2013;

[Not in Scope]



Sam Gleisner
for Secretary of the Cabinet

Distribution:
The Cabinet

Office of the Prime Minister

Cabinet

GOVERNMENT COMMUNICATIONS SECURITY BUREAU AND RELATED LEGISLATION AMENDMENT BILL: APPROVAL FOR INTRODUCTION

Proposal

1. It is proposed that Cabinet confirm the decision by joint Ministers to approve for introduction to the House the Government Communications Security Bureau and Related Legislation Amendment Bill; and review previous decisions relating to amendments to the New Zealand Security Intelligence Service Act 1969.

Background

2. On 22 April 2013, Cabinet:

   - **noted** that the Bills to amend the intelligence legislation, interception capability legislation and providing for network security were being drafted and that it was intended that they be available for introduction on 6 May 2013; and

   - **authorised** a group of Ministers, comprising the Prime Minister, Hon Bill English, Hon Steven Joyce, Hon Christopher Finlayson and Hon Amy Adams to have Power to Act to (among other things):
     - finalise the Bills for introduction, subject to final consideration by Cabinet on 6 May 2013;
     - make changes to proposals to achieve consistency with the New Zealand Bill of Rights Act 1990.

   [CAB Min (13) 13/24]

3. On 2 May 2013, joint Ministers met by telephone conference and:

   - **approved** for introduction the Government Communications Security Bureau and Related Legislation Amendment Bill subject to final consideration by Cabinet;

   - **agreed** that the Bill should include a safeguard provision requiring approval to be granted jointly by the Responsible Minister and the Commissioner of Security Warrants when anything is to be done by

GCSB under new section 8A or 8B for the purpose of intercepting the private communications of New Zealand citizens or permanent residents;

- **agreed** that the Bill be introduced as soon as possible after its final consideration by Cabinet;

- **agreed** that the government propose that the Bill be:
  - referred to the Intelligence and Security Committee for consideration;
  - reported back by 26 July 2013;
  - enacted by August 2013.

[Not in Scope]

Policy

GCSB and Related Legislation Amendment Bill

5. On 26 March 2013, the Cabinet Committee on Domestic and External Security (DES) approved the policy parameters for legislation amending the Government Communications Security Bureau Act 2003 (GCSB Act), the Inspector-General of Intelligence and Security Act 1996 (IGIS Act), and the Intelligence and Security Committee Act 1996 (ISC Act) [DES Min (13) 3/2-3, DES Min (13) 3/1]. This was followed in April 2013 by supplementary decisions on three matters earlier agreed by DES in principle [DES Min (13) 4/1].

6. The Government Communications Security Bureau and Related Legislation Amendment Bill retains the basic construct of the GCSB Act while amending the Act with two main objectives:

- to clarify aspects of the Act, especially relating to the Bureau's functions and powers, as well as the applicable controls and limitations, so as to provide for a clearly formulated and consistent statutory framework for the activities of GCSB; and

- to update that framework to respond to the changing security environment New Zealand is facing (particularly in relation to cyber and

information security), and to changes in the public law environment since the Act was passed in 2003.

7. The Bill also amends the IGIS Act to strengthen the office of the Inspector-General of Intelligence and Security, increasing the resourcing of the office to enable a greater range of activities to be carried out, expanding the IGIS's statutory work programme and enhancing the corresponding reporting responsibilities.

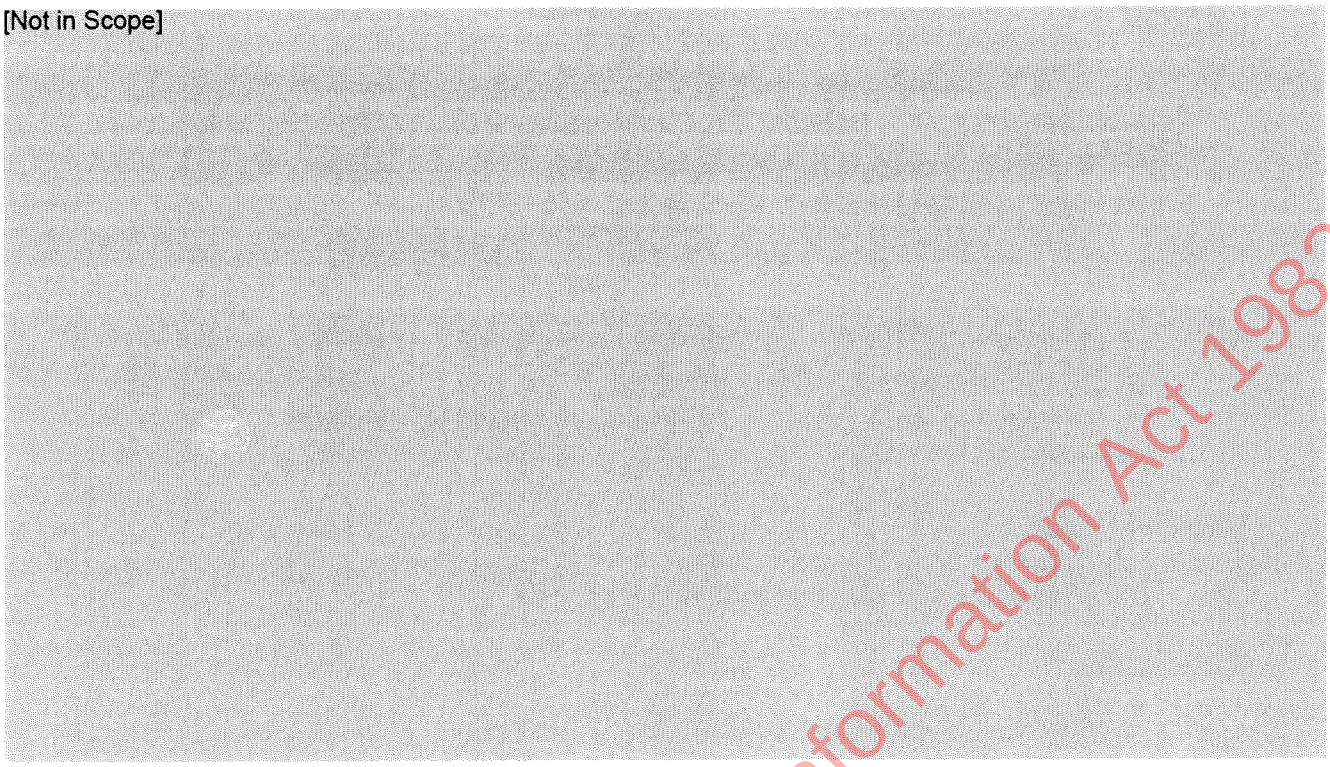
8. Finally, the Bill amends the ISC Act to improve the Committee's ability to provide effective oversight and accountability of the intelligence agencies. In particular, this involves the Prime Minister relinquishing the ISC chair if the Committee, when conducting a financial review of an intelligence agency for which the Prime Minister is the Responsible Minister, is discussing the performance of that agency.

9. The drafting in the Bill retains a basic operating premise in section 14 of the GCSB Act – that GCSB is not to conduct foreign intelligence activities against New Zealanders. The original language of section 14 has been maintained to the extent possible, with an adjustment to clarify that the restriction applies only to the Bureau's foreign intelligence function.

10. The Bill departs from the wording of the applicable DES Minutes in one way which is consistent with the substance of DES's decisions and the basic premise in section 14. As a safeguard in respect of New Zealanders' privacy, the Bill provides (in new section 15B) that anything done by GCSB under new section 8A or 8B for the purpose of intercepting the private communications of New Zealand citizens or permanent residents requires an authorisation to be granted jointly by the Responsible Minister and the Commissioner of Security Warrants (appointed under the New Zealand Security Intelligence Service Act 1969). When GCSB is assisting another entity under section 8C, the authorisation processes and any restrictions or limitations that apply to that entity will apply to the Bureau's assistance.

11. This additional safeguard, for which policy approval was not initially sought, is consistent with the process for seeking domestic security warrants under the New Zealand Security Intelligence Service Act 1969. In accordance with the Power to Act granted in CAB Min (13) 13/24, joint Ministers agreed to the inclusion of this provision to achieve consistency with the New Zealand Bill of Rights Act 1990.

[Not in Scope]



Compliance

14. The Bill complies with:

- the principles of the Treaty of Waitangi
- the New Zealand Bill of Rights Act 1990
- the Human Rights Act 1993
- the Privacy Act 1993
- relevant international standards and obligations
- the LAC Guidelines

Consultation

15. The Government Communications Security Bureau, New Zealand Defence Force, New Zealand Police, New Zealand Security Intelligence Service, and the Crown Law Office have been consulted on the Bill.

Parliamentary stages

16. In line with the timeframe previously indicated by DES [DES Min (12) 4/1-1], the Bill should be introduced to the House as soon as possible after its final consideration by Cabinet, and should be enacted by August 2013. Introduction on 6 May will enable the First Reading of the Bill to take place on Thursday 9 May.

17. It is proposed that the Bill stand referred to the Intelligence and Security Committee. To meet the timeframe for enactment by August 2013, the Bill will need to be reported back by the Committee in less than four months. Under the Standing Orders, a report-back period of less than four months is a time-unlimited debatable motion.

Publicity

18. Issues regarding GCSB's functions and powers are contentious, particularly in light of Kim Dotcom and the subsequent *Review of Compliance at the GCSB*. Media releases were issued on 9 and 15 April and briefing material has been made available. A further media release is planned on introduction of the Bill.

Recommendations

19. The Prime Minister recommends that Cabinet:

Background

1. **note** that in December 2012, DES:

   1.1 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);

   1.2 noted that the bill would be enacted by August 2013;

   [DES Min (12) 4/1-1]

GCSB and Related Legislation Amendment Bill

2. **note** that the Government Communications Security Bureau and Related Legislation Amendment Bill is an omnibus Bill that amends the Government Communications Security Bureau Act 2003 (GCSB Act), the Inspector-General of Intelligence and Security Act 1996 (IGIS Act), and the Intelligence and Security Committee Act 1996 (ISC Act);

3. **note** that, on 2 May 2013, a group of Ministers having been authorised with Power to Act [CAB Min (13) 13/24] approved the Bill for introduction to the House;

4. **confirm** the decision by joint Ministers to approve for introduction the Government Communications Security Bureau and Related Legislation Amendment Bill;

5. **agree** that the Bill be introduced as soon as possible after its final consideration by Cabinet;

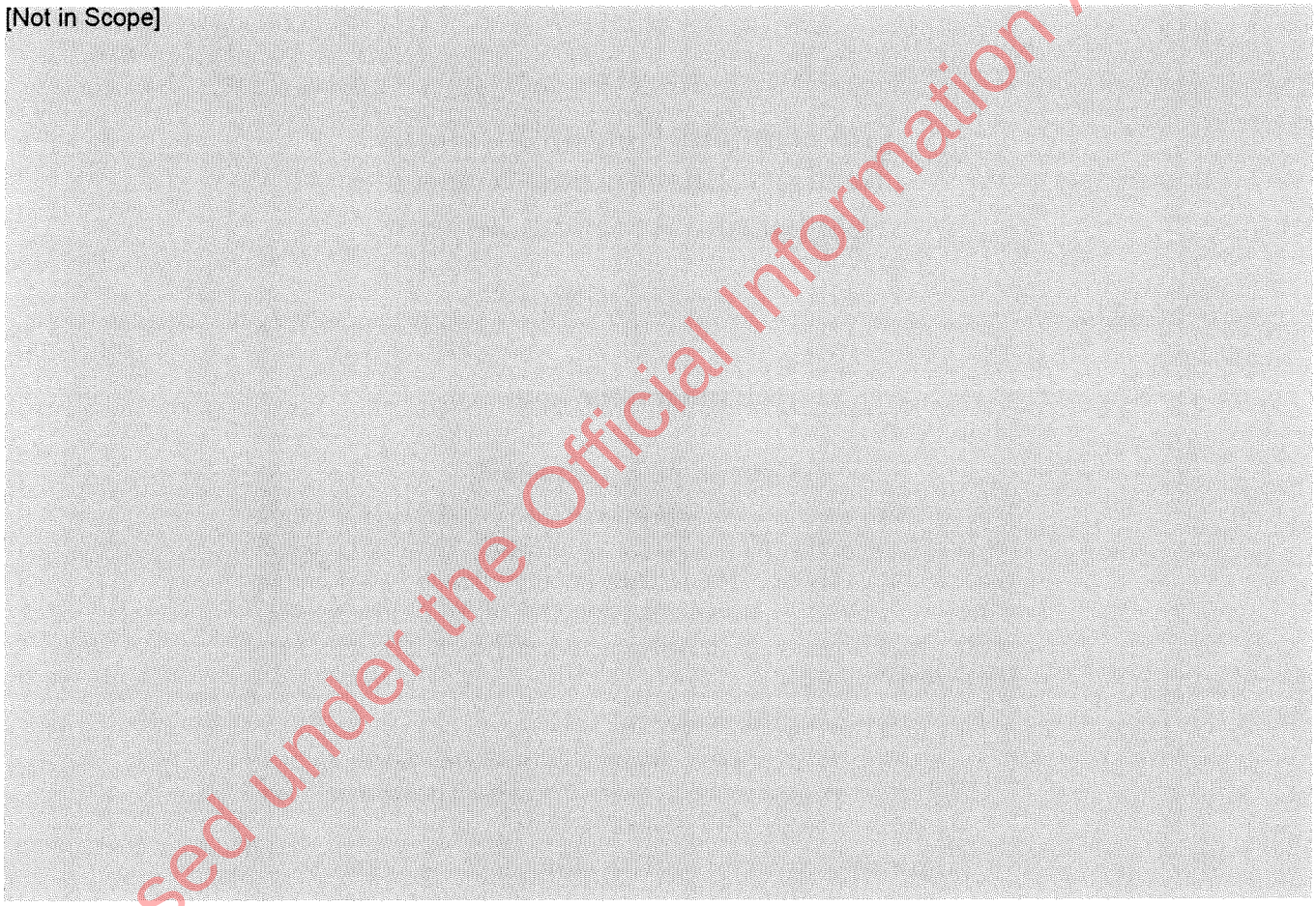
6. **agree** that the government propose that the Bill be:

   6.1 referred to the Intelligence and Security Committee for consideration;

   6.2 reported back by 26 July 2013;

   6.3 enacted by August 2013;

[Not in Scope]



Rt Hon John Key
Prime Minister

PCO 17322/9.0
Drafted by PCO
SENSITIVE

Government Communications Security Bureau and Related Legislation Amendment Bill

Government Bill

Explanatory note

General policy statement

This Bill is an omnibus Bill that amends the Government Communications Security Bureau Act 2003, the Inspector-General of Intelligence and Security Act 1996, and the Intelligence and Security Committee Act 1996. It is proposed (at the close of the Bill's committee of the whole House stage in Parliament) to divide the Bill into 3 separate amending Bills.

The purposes of the Bill are to—

- provide for a clearly formulated and consistent statutory framework governing the activities of the Government Communications Security Bureau (**GCSB**); and
- update that framework to respond to the changing security environment (particularly in relation to cybersecurity and information security), and to changes in the public law environment since the GCSB Act was passed in 2003; and
- enhance the external oversight mechanisms that apply to the intelligence agencies by strengthening the office of the Inspector-General of Intelligence and Security and by improving

the operation of Parliament's Intelligence and Security Committee.

Amendments to Government Communications Security Bureau Act 2003

It is crucial that an agency exercising intrusive powers, as GCSB does, is governed by a consistent statutory framework that articulates the agency's functions and powers, as well as the applicable controls and limitations, in the clearest possible terms. This promotes robust internal management and effective external oversight of the agency's activities.

The March 2013 *Review of Compliance at the Government Communications Security Bureau* by Rebecca Kitteridge highlighted difficulties in interpreting the GCSB Act when the Bureau was providing assistance to other agencies, notably the New Zealand Security Intelligence Service. In a small jurisdiction like New Zealand, it is essential that specialised capabilities developed or acquired by agencies like GCSB should be available to meet key government priorities, where appropriate and subject to necessary safeguards. The Bill amends the GCSB Act to clarify this important support role as well as other aspects of the Bureau's functions.

At the same time, New Zealand faces a changing security environment in which threats are increasingly interconnected and national borders are less meaningful. Globalisation means New Zealand is no longer as distant from security threats as it once was. This changed environment means the legislation governing GCSB needs updating, to enable it to address the security challenges posed by the increasing importance of cyberspace.

The Bill retains the basic construct of the GCSB Act and the core principles underpinning GCSB's operations. Amendments to the objective, functions, powers, and limitation provisions are designed to address the issues above—namely, to improve clarity about the legal parameters for GCSB's activities; and to accommodate changes in the prevailing security environment.

Objective and functions of GCSB

The Bill replaces the objective of GCSB with a simple statement that it strives, through its functions, to contribute to New Zealand's national security, international relations, and economic well-being.

The Act currently provides for 3 core functions of GCSB:

- information assurance and cybersecurity:
- foreign intelligence:
- co-operation with and assistance to other entities.

These 3 functions will be retained in substance. How they are articulated will be changed to improve transparency and facilitate external oversight of GCSB's activities.

The statement of the 3 functions will be split into separate provisions (*new sections 8A, 8B, and 8C*). The information assurance and cybersecurity function will be given greater prominence, reflecting the key role GCSB plays in the wider cybersecurity domain—including its hosting of New Zealand's National Cyber Security Centre, and its responsibility to use its cybersecurity capabilities to assist a range of public entities as well as private sector organisations such as critical national infrastructure providers and organisations of national significance.

The foreign intelligence function will be described in a way that provides transparency about the nature and scope of this role, without expressly legislating the range of activities involved or the skills required in pursuit of this function.

The Act will be changed to provide a sounder basis for GCSB to offer expert advice and assistance to other entities. The Bureau will have clear legal authority to assist the New Zealand Defence Force, New Zealand Police, and New Zealand Security Intelligence Service (as well as any other department that may be specified by Order in Council) in performing their lawful functions. In providing such assistance, GCSB will be confined to activities that the other entity is lawfully able to undertake itself (though it may not have the capability), and will be subject to any limitations and restrictions that apply to the other entity.

Powers, controls, and limitations

The Act confers 3 powers of interception on GCSB:

- 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):
- interception of communications by an interception device under an interception warrant granted by the responsible Minister (section 17):
- access to a computer system under a computer access authorisation granted by the responsible Minister (section 19).

This construct continues to provide the basic tools that GCSB needs to perform its functions, and it will be retained.

At present, section 13 of the Act dictates that the Bureau's powers are available for the purpose of obtaining foreign intelligence. While much of GCSB's work (including in the cybersecurity 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. The Act will be amended to make it clear that the powers can be used for both the foreign intelligence function and the information assurance and cybersecurity function, subject to appropriate controls and limitations.

The basic premise underpinning GCSB's operations is that it is not to conduct foreign intelligence activities against New Zealanders. This premise predated the GCSB Act, and was incorporated in the GCSB Act (in section 14) because of its importance. However, the way this basic premise was incorporated into the Act meant that it applied not only to the foreign intelligence function of the Bureau, but also to its other 2 functions: information assurance and assisting other entities. This has resulted in a growing number of difficulties, and is restricting GCSB's ability to effectively carry out its other 2 functions.

The basic premise in section 14 will be retained, with an adjustment to clarify that it only applies to the foreign intelligence function. As a safeguard in respect of New Zealanders' privacy, any activity under *new section 8A or 8B* that might involve intercepting the communications of New Zealanders will require an authorisation to be granted

jointly by the responsible Minister and the Commissioner of Security Warrants (appointed under the New Zealand Security Intelligence Service Act 1969). When GCSB is assisting another entity under *new section 8C*, the authorisation processes and any restrictions or limitations that apply to that entity will apply to the Bureau's assistance.

Other amendments

A range of amendments designed to complement other changes, or in the interests of updating the Act generally, includes the following:

- to enable the Inspector-General of Intelligence and Security to have access to the best possible information, the Act will be amended to require GCSB to maintain a written record of all warrants and authorisations in a form readily available for inspection:
- in line with the recommendation of the Law Commission in June 2011, principles 1, 5, 8, and 9 of the Privacy Act 1993 will apply to GCSB, modified if necessary to achieve the effective and efficient performance by the Bureau of its functions:
- the appointment framework for the Director of GCSB will be modified to codify the State Service Commissioner's support for that process, as currently set out in the Cabinet Manual:
- in situations of urgency where the responsible Minister is not readily available, the Attorney-General, the Minister of Foreign Affairs or the Minister of Defence will be empowered to issue an interception warrant or an access authorisation:
- the maximum penalty for unauthorised disclosure of information will be increased to align it with the penalty for similar types of offending, for example in the Crimes Act 1961.

Amendments to Inspector-General of Intelligence and Security Act 1996

Effective and credible oversight of the intelligence agencies is crucial to provide assurance that those agencies' powers are being used in accordance with the law and with respect for New Zealanders' right to privacy. The Inspector-General of Intelligence and Security (**IGIS**) is a source of independent external oversight, responsible for examining issues of legality and propriety, efficacy and efficiency, and human rights and privacy compliance.

The Bill amends the Inspector-General of Intelligence and Security Act 1996 to strengthen the office of the IGIS, increasing the resourcing of the office to enable a greater range of activities to be carried out, expanding the IGIS's statutory work programme, and enhancing the corresponding reporting responsibilities.

The changes to the Act include the following:

- the statutory work programme of the IGIS, which includes a focus on warrants and authorisations issued to the intelligence agencies, will be extended to require regular examination of system-wide issues that impact on operational activities:
- the IGIS will be required to certify each year in his or her annual report whether the compliance systems of the intelligence agencies are sound:
- the IGIS will be able to initiate inquiries into matters of propriety without requiring the concurrence of the responsible Minister. This will enable the IGIS to undertake independent inquiries:
- the responsible Minister will be given explicit responsibility to respond to IGIS reports within a reasonable time frame. The Minister may choose to provide those responses also to the Intelligence and Security Committee:
- the IGIS will be expected to make unclassified versions of his or her reports publicly available, with appropriate precautions being taken in respect of any privacy or security concerns:
- the legislative requirement that the IGIS be a retired High Court Judge will be removed, broadening the pool of potential candidates. The 3-year term of office will remain, with the possibility of reappointment for a maximum of 1 additional term:
- a Deputy IGIS will be appointed.

Amendments to Intelligence and Security Committee Act 1996

The Intelligence and Security Committee (**ISC**) is the parliamentary mechanism for oversight of the intelligence agencies. It examines issues of efficacy and efficiency, budgetary matters, and policy-setting.

The Bill amends the Intelligence and Security Committee Act 1996 to improve the ISC's ability to provide effective oversight and accountability of the intelligence agencies.

The changes to the Act involve the following:

- the Prime Minister will be required to relinquish the ISC chair if the Committee, when conducting a financial review of an intelligence agency for which the Prime Minister is the responsible Minister, is discussing the performance of that agency:
- the Prime Minister will be permitted to nominate either the Deputy Prime Minister or the Attorney-General to act as an alternate chair in circumstances where that alternate is not already a member of the ISC:
- subject to restrictions on the publication of sensitive information, the ISC will be required to table its reports in the House and make them publicly available on an Internet site.

Regulatory impact statement

The Department of the Prime Minister and Cabinet with the Government Communications Security Bureau produced a regulatory impact statement on 22 March 2013 to help inform the main policy decisions taken by the Government relating to the contents of this Bill.

A copy of this regulatory impact statement can be found at—

- http://www.gcsb.govt.nz/about-us/legislation.html
- http://www.treasury.govt.nz/publications/informationreleases/ris

Clause by clause analysis

Clause 1 states the title of the Bill. When the Bill is divided, as noted earlier, the title of each Part will refer to the principal Act being amended.

Clause 2 is the commencement clause and provides that the Bill comes into force on the day that is 1 month after the date on which it receives the Royal assent. When the Bill is divided, as noted earlier, this commencement clause will be repeated in each separate Bill.

Part 1
Amendments to Government Communications Security Bureau Act 2003

Clause 3 provides that this Part amends the Government Communications Security Bureau Act 2003.

Clause 4 amends section 3, which specifies the purpose of the Act. The amendments substitute *new paragraphs (c) to (e)*. They have been recast to be consistent with changes in terminology being made.

Clause 5 amends section 4, which defines terms used in the Act. The amendments repeal certain definitions, amend other definitions, and insert new definitions.

The new definition of incidentally obtained intelligence is important in relation to *new section 14* inserted by *clause 12* and to *new section 25* inserted by *clause 24*.

The new definition of information infrastructure is inserted to take the place of the repealed definition of computer system. The new definition includes any medium through or in which communications are carried or stored and includes the communications themselves.

Clause 6 replaces sections 7 and 8 with *new sections 7 to 8D*.

New section 7 states the objective of the Government Communications Security Bureau (the **Bureau**).

New section 8 provides that the functions of the Bureau set out in *new sections 8A to 8C* are not to be taken as specifying any order of importance or priority. It also clarifies that the performance of the Bureau's functions, and the relative importance and priority of the functions, if any, are to be determined from time to time by the Director, subject to the control of the Minister.

New section 8A sets out the function of the Bureau in relation to information assurance and cybersecurity.

New section 8B sets out the function of the Bureau in relation to gathering and analysing intelligence about the capabilities, intentions, and activities of foreign persons and foreign organisations, and in relation to gathering and analysing intelligence about information infrastructures.

New section 8C sets out the function of the Bureau in relation to co-operation with certain other entities to facilitate the performance

of their functions. *New subsection (2)* provides limits on the extent of the co-operation provided, but clarifies that the co-operation may be provided even though the advice and assistance provided might involve the exercise of powers by, or the sharing of the capabilities of, the Bureau that the Bureau is not, or could not be, authorised to exercise or share in the performance of its other functions.

New section 8D gives the Director all the powers that are necessary or desirable for the purpose of performing the functions of the Bureau, but this is subject to the Act, any other enactment, and the general law.

Clause 7 replaces section 9 with *new sections 9 to 9D* dealing with the appointment of the Director, the appointment process, remuneration and conditions of appointment, removal from office, and review of the Director's performance.

Clause 8 amends section 11, which makes it an offence for current or past employees of the Bureau to unlawfully disclose information gained in connection with the Bureau. The amendments increase the maximum penalties from 2 years' to 3 years' imprisonment and from a $2,000 to a $5,000 fine.

Clause 9 amends section 12, which provides for the Bureau's annual report. The amendments are drafting amendments.

Clause 10 replaces the Part 3 heading to update terminology and reflect that the Part deals with both intercepting communications and accessing information infrastructures.

Clause 11 replaces section 13, which sets out the purpose of Part 3. The purpose is recast to be consistent with the recasting of the Bureau's functions and with amendments made to other provisions in Part 3.

Clause 12 replaces section 14, which provides that interceptions are not to target New Zealand citizens or permanent residents of New Zealand. The *new section 14* is expressly linked to the Bureau's intelligence-gathering function in *new section 8B* and provides that any incidentally obtained intelligence is not obtained in breach of *new section 8B*, but must not be retained or disclosed except in accordance with section 23 and *new section 25*.

Clause 13 amends section 15, which prohibits, unless authorised, the connecting or installing of interception devices. The amendments are

technical to reflect the change in terminology from computer systems to information infrastructures.

Clause 14 inserts *new sections 15A and 15B*.

New section 15A provides for the Director, for the purpose of performing the Bureau's functions under *new section 8A or 8B*, to apply to the Minister for an interception warrant to intercept communications or an access authorisation to access information infrastructures. The new section sets out the matters that the Minister must be satisfied about before issuing a warrant or an authorisation.

New section 15B requires the Commissioner of Security Warrants (appointed under the New Zealand Security Intelligence Service Act 1969) to be involved if anything that may be done under a warrant or an authorisation issued under *new section 15A* is for the purpose of intercepting the private communications of a New Zealand citizen or permanent resident of New Zealand under *new section 8A* or *new section 8B* to the extent that intercepting the person's private communications under that section is not precluded by *new section 14*.

Clause 15 amends section 16, which permits certain interceptions without an interception warrant or an access authorisation.

The amendments—

- specify that the section applies to interceptions for the purposes of the Bureau's functions in *new sections 8A and 8B*:
- specify that it does not authorise the interception of private communications of New Zealand citizens or permanent residents of New Zealand.

Clause 16 repeals section 17 and the cross-heading above section 17. Section 17 has been assimilated into *new section 15A* inserted by *clause 14*.

Clause 17 amends section 18, which provides for certain matters about interception warrants. The amendments widen the application of the section to include access authorisations.

Clause 18 replaces section 19 with *new sections 19 and 19A*. *New section 19* requires the Director to keep a register of interception warrants and access authorisations that have been issued. *New section 19A* provides for the urgent issue of interception warrants or access authorisations by the Attorney-General, the Minister of Defence, or the Minister of Foreign Affairs if the Minister is unavailable and it is necessary to issue them before the Minister is available.

Clause 19 makes a drafting amendment to section 20.

Clause 20 replaces section 21 with a new section that confers immunity from civil and criminal liability for certain things done under the Act if done in good faith and in a reasonable manner.

Clauses 21 to 23 make drafting amendments to sections 22, 23, and 24 respectively.

Clause 24 replaces section 25. The new section specifies when and to whom incidentally obtained intelligence about New Zealand citizens or permanent New Zealand residents may be retained and communicated. The ground in the current section 25 of preventing or detecting serious crime in New Zealand or any other country is retained and the following 2 new grounds are added:

- preventing or responding to threats to human life in New Zealand or any other country:
- identifying, preventing, or responding to threats or potential threats to the national security of New Zealand or any other country.

Clause 25 inserts *new sections 25A and 25B* dealing with the protection and disclosure of personal information. *New section 25A* requires the Director, in consultation with the Inspector-General of Intelligence and Security and the Privacy Commissioner, to formulate a policy on the protection and disclosure of personal information that complies with the principles set out in *new section 25B*. *New section 25B* sets out the principles about collecting, using, storing, and retaining personal information.

Clause 26 makes consequential amendments to other Acts as set out in the *Schedule*.

Part 2
Amendments to Inspector-General of Intelligence and Security Act 1996

Clause 27 provides that this Part amends the Inspector-General of Intelligence and Security Act 1996.

Clause 28 amends section 2(1), which contains definitions of terms, and inserts a definition of Deputy Inspector-General.

Clause 29 replaces section 5 with *new section 5*, which provides for the appointment of an Inspector-General of Intelligence and Se-

curity and a Deputy Inspector-General of Intelligence and Security. The Deputy Inspector-General has all the powers and functions of the Inspector-General, subject to the control and direction of the Inspector-General. The Deputy Inspector-General has all the powers and functions of the Inspector-General if there is a vacancy in the office of the Inspector-General or if the Inspector-General is absent from duty for any reason.

Clause 30 amends section 6, which provides for the Inspector-General's term of office. The amendments—

- add a reference to the Deputy Inspector-General:
- provide a maximum term of appointment of 3 years for each:
- provide that each can be reappointed, but in the case of the Inspector-General only once.

Clause 31 amends section 11, which specifies the functions of the Inspector-General. The amendments replace subsection (1)(c), (d), and (da) with new paragraphs. Paragraph (c) is replaced with 2 new paragraphs. The effect of this is to permit the Inspector-General to inquire into the propriety of particular activities of an intelligence and security agency without needing the agreement of the Minister.

Paragraphs (d) and (da) are replaced with 2 new paragraphs. *New paragraph (d)* requires the Inspector-General to review, at intervals of not more than 12 months,—

- the effectiveness and appropriateness of procedures adopted by each intelligence and security agency to ensure compliance with its governing legislation in relation to the issue and execution of warrants and authorisations:
- the effectiveness and appropriateness of compliance systems concerning operational activity, including supporting policies and practices of each intelligence and security agency relating to certain matters, including risk management and legal compliance generally.

New paragraph (da) requires the Inspector-General to conduct unscheduled audits of the procedures and compliance systems described in *new paragraph (d)*.

This clause also repeals section 11(2). That subsection placed limitations on the ability of the Inspector-General to do anything of his or her own motion in relation to a complaint about any activity of an intelligence and security agency.

Clause 32 amends section 12, which authorises the Inspector-General to consult certain public office holders and disclose information necessary for that purpose.

The effect of the amendments is to add a reference to the Independent Police Conduct Authority as one of the public offices that may be consulted.

Clause 33 amends section 15 consequential on the amendments to section 12.

Clause 34 amends section 25, which specifies what the Inspector-General must do on completing an inquiry. The amendments—

- require the Minister to provide his or her response to the report to the Inspector-General and the chief executive of the intelligence and security agency concerned:
- permit the Minister to provide his or her response to the Intelligence and Security Committee.

These amendments do not apply to the extent that a report relates to employment matters or security clearance issues.

Clause 35 inserts *new section 25A*, which requires the Director-General, as soon as practicable after forwarding a report as required under section 25(1), to make a copy of the report publicly available on an Internet site maintained by the Inspector-General. The new section specifies matters that must not be disclosed in the report made available under this section.

Clause 36 amends section 27, which provides for the Inspector-General's annual report. The amendments—

- require the Inspector-General to certify whether each intelligence and security agency's compliance systems are sound:
- require the Inspector-General, as soon as practicable after his or her annual report is presented to Parliament, to make a copy of his or her report (as presented to Parliament) publicly available on an Internet site maintained by the Inspector-General.

Part 3
Amendments to Intelligence and Security Committee Act 1996

Clause 37 provides that this Part amends the Intelligence and Security Committee Act 1996.

Clause 38 amends section 6, which specifies the functions of the Committee. Section 6(1)(e) specifies one of the Committee's functions to be to report to the House of Representatives on the activities of the Committee. The amendment substitutes a *new paragraph (e)*, which requires the Committee to present an annual report to the House of Representatives and to make an annual report publicly available on the Internet site of the New Zealand Parliament.

Clause 39 inserts *new section 7A*, which contains further provisions about the chairperson of the Committee. The new section provides—

- that the Prime Minister is not to chair a meeting of the Committee while it is discussing, in the course of a financial review of an intelligence and security agency, any matter relating to the performance of the intelligence and security agency if the Prime Minister is the responsible Minister of the agency. In that case, one of the members of the Committee appointed under section 7(1)(c) must act as chairperson:
- that the chairperson of the Committee may appoint either the Deputy Prime Minister or the Attorney-General (if not already a member of the Committee) to act as chairperson in the absence of the chairperson.

Clause 40 makes amendments to section 18 that are consequential on the amendment made by *clause 38*.

Rt Hon John Key

Government Communications Security Bureau and Related Legislation Amendment Bill

Government Bill

Contents

The Parliament of New Zealand enacts as follows:

1 Title

This Act is the Government Communications Security Bureau and Related Legislation Amendment Act **2013**.

2 Commencement

This Act comes into force on the day that is 1 month after the date on which it receives the Royal assent.

Part 1
Amendments to Government Communications Security Bureau Act 2003

3 Principal Act

This **Part** amends the Government Communications Security Bureau Act 2003 (the **principal Act**).

4 Section 3 amended (Purpose)

Replace section 3(c) to (e) with:

"(c) specify the circumstances in which the Bureau requires an interception warrant or access authorisation to intercept communications:

"(d) specify the conditions that are necessary for the issue of an interception warrant or access authorisation and the matters that may be authorised by a warrant or an authorisation:

"(e) specify the circumstances in which the Bureau may use interception devices to intercept communications without a warrant or an authorisation."

5 **Section 4 amended (Interpretation)**

(1) This section amends section 4.

(2) Repeal the definitions of **computer access authorisation** or **authorisation**, **computer system**, **foreign communications**, **foreign intelligence**, and **network**.

(3) Insert in their appropriate alphabetical order:

"**access authorisation** means an authorisation issued under **section 15A(1)(b)**

"**incidentally obtained intelligence** means intelligence—

"(a) that is obtained in the course of gathering intelligence about the capabilities, intentions, or activities of foreign organisations or foreign persons; but

"(b) that is not intelligence of the kind referred to in **paragraph (a)**

"**information infrastructure** includes electromagnetic emissions, communications systems and networks, information technology systems and networks, and any communications carried on, contained in, or relating to those emissions, systems, or networks".

(4) In the definition of **access**, replace "computer system" with "information infrastructure".

(5) In the definition of **communication**, after "sounds,", insert "information,".

(6) In the definition of **foreign organisation**, paragraph (d), replace "exclusively" with "principally".

(7) In the definition of **interception warrant**, replace "section 17" with "**section 15A(1)(a)**".

6 **Sections 7 and 8 replaced**

Replace sections 7 and 8 with:

"7 **Objective of Bureau**

The objective of the Bureau, in performing its functions, is to contribute to—

"(a) the national security of New Zealand; and

"(b) the international relations and well-being of New Zealand; and

"(c) the economic well-being of New Zealand.

"8 **Functions of Bureau**

"(1) **Sections 8A to 8C** set out the functions of the Bureau.

"(2) The order in which the functions are set out is not to be taken as specifying any order of importance or priority.

"(3) The performance of the Bureau's functions and the relative importance and priority of the functions, if any, are to be determined, from time to time, by the Director, subject to the control of the Minister.

"(4) Without limiting **subsection (3)**, the performance of the Bureau's functions under **section 8A** (information assurance and cybersecurity) and **section 8C** (co-operation with other entities to facilitate their functions) is at the discretion of the Director.

"(5) In addition to the functions set out in **sections 8A to 8C**, the Bureau has the functions (if any) conferred on it by or under any other Act.

"8A **Information assurance and cybersecurity**

This function of the Bureau is—

"(a) to co-operate with, and provide advice and assistance to, any public authority whether in New Zealand or overseas, or to any other entity authorised by the Minister, on any matters relating to the protection, security, and integrity of—

"(i) communications, including those that are processed, stored, or communicated in or through information infrastructures; and

"(ii) information infrastructures of importance to the Government of New Zealand; and

"(b) without limiting **paragraph (a)**, to do everything that is necessary or desirable to protect the security and integrity of the communications and information infrastructures referred to in **paragraph (a)**, including identifying and responding to threats or potential threats to

those communications and information infrastructures; and

"(c) to report to the following on anything done under **paragraphs (a) and (b)** and any intelligence gathered as a result:

"(i) the Minister; and

"(ii) any person or office holder (whether in New Zealand or overseas) authorised by the Minister to receive the report.

"**8B Intelligence gathering and analysis**

"(1) This function of the Bureau is—

"(a) to gather and analyse intelligence (including from information infrastructures) in accordance with the Government's requirements about the capabilities, intentions, and activities of foreign persons and foreign organisations; and

"(b) to gather and analyse intelligence about information infrastructures; and

"(c) to communicate any intelligence gathered and any analysis of the intelligence to—

"(i) the Minister; and

"(ii) any person or office holder (whether in New Zealand or overseas) authorised by the Minister to receive the intelligence.

"(2) For the purpose of performing its function under **subsection (1)(a) and (b)**, the Bureau may co-operate with, and provide advice and assistance to, any public authority (whether in New Zealand or overseas) and any other entity authorised by the Minister for the purposes of this subsection.

"**8C Co-operation with other entities to facilitate their functions**

"(1) This function of the Bureau is to co-operate with, and provide advice and assistance to, the following for the purpose of facilitating the performance of their functions:

"(a) the New Zealand Police; and

"(b) the New Zealand Defence Force; and

"(c) the New Zealand Security Intelligence Service; and

"(d) any department (within the meaning of the Public Finance Act 1989) specified for the purposes of this section by the Governor-General by Order in Council made on the recommendation of the Minister.

"(2) To avoid doubt, the Bureau may perform its function under **subsection (1)**—

"(a) to the extent that the advice and assistance is provided for the purpose of activities that the entities may lawfully undertake; and

"(b) subject to any limitations, restrictions, and protections under which those entities perform their functions and exercise their powers; and

"(c) even though the advice and assistance might involve the exercise of powers by, or the sharing of the capabilities of, the Bureau that the Bureau is not, or could not be, authorised to exercise or share in the performance of its other functions.

"8D Director has full powers for purpose of performing Bureau's functions

"(1) The Director has all the powers that are necessary or desirable for the purpose of performing the functions of the Bureau.

"(2) **Subsection (1)** applies subject to this Act, any other enactment, and the general law."

7 Section 9 replaced (Director of Bureau)

Replace section 9 with:

"9 Appointment of Director

"(1) The Director of the Bureau is appointed by the Governor-General, on the recommendation of the Prime Minister, for a term not exceeding 5 years, and may from time to time be reappointed.

"(2) To avoid doubt, the mere fact that a person holds the position of Director does not entitle the person to be reappointed or to expect to be reappointed.

"9A Appointment process

The State Services Commissioner—

"(a) is responsible for managing the process for the appointment of the Director; and

"(b) must provide advice on the nominations for Director to the Prime Minister.

"**9B Remuneration and conditions of appointment of Director**

"(1) The Director is paid the remuneration and allowances determined by the Remuneration Authority.

"(2) The other terms and conditions of the Director's appointment are determined from time to time by the State Services Commissioner.

"**9C Removal from office**

"(1) The Governor-General may at any time for just cause, on the recommendation of the Prime Minister, remove the Director from office.

"(2) The removal must be made by written notice to the Director.

"(3) The notice must—

"(a) state the date on which the removal takes effect, which must not be earlier than the date on which the notice is received; and

"(b) state the reasons for the removal.

"(4) The State Services Commissioner is responsible for advising the Prime Minister on any proposal to remove the Director from office.

"(5) In this section, **just cause** includes misconduct, inability to perform the functions of office, and neglect of duty.

"**9D Review of performance of Director**

"(1) The Minister may direct the State Services Commissioner or another person to review, either generally or in respect of any particular matter, the performance of the Director.

"(2) The person conducting a review under **subsection (1)** must report to the Minister on the manner and extent to which the Director is fulfilling all of the requirements imposed on the Director, whether under this Act or otherwise.

"(3) No review under this section may consider any security operations undertaken, or proposed to be undertaken."

8 Section 11 amended (Prohibition on unauthorised disclosure of information)

In section 11(2),—

(a) replace "2 years" with "3 years"; and

(b) replace "$2,000" with "$5,000".

9 Section 12 amended (Annual report)

(1) In section 12(2), replace "without delay" with "as soon as practicable".

(2) In section 12(3)(c), delete "computer".

10 Part 3 heading replaced

Replace the Part 3 heading with:

"**Part 3**

"**Intercepting communications and accessing information infrastructures**".

11 Section 13 replaced (Purpose of Part)

Replace section 13 with:

"**13 Purpose of Part**

The purpose of this Part is—

"(a) to authorise the Bureau to intercept communications and access information infrastructures for the purpose of performing its functions under **sections 8A and 8B**; and

"(b) to place restrictions and limitations on—

"(i) the interception of communications and the accessing of information infrastructures; and

"(ii) the retention and use of information derived from the interception of communications and the accessing of information infrastructures."

12 Section 14 replaced (Interceptions not to target domestic communications)

Replace section 14 with:

"14 **Interceptions not to target New Zealand citizens or permanent residents for intelligence-gathering purposes**

"(1) In performing the Bureau's function in **section 8B**, the Director, any employee of the Bureau, and any person acting on behalf of the Bureau must not authorise or do anything for the purpose of intercepting the private communications of a person who is a New Zealand citizen or a permanent resident of New Zealand, unless (and to the extent that) the person comes within the definition of foreign person or foreign organisation in section 4.

"(2) Any incidentally obtained intelligence obtained by the Bureau in the performance of its function in **section 8B**—

"(a) is not obtained in breach of **section 8B**; but

"(b) must not be retained or disclosed except in accordance with sections 23 and **25**."

13 Section 15 amended (Interceptions for which warrant or authorisation required)

(1) In section 15(1)(a), replace "a network" with "an information infrastructure".

(2) In section 15(2),—

(a) replace "a computer access authorisation" with "an access authorisation"; and

(b) replace "a computer system" with "an information infrastructure".

14 New sections 15A and 15B and cross-heading inserted

After section 15, insert:

"*Authorisations to intercept communications or access information infrastructures*

"**15A Authorisation to intercept communications or access information infrastructures**

"(1) For the purpose of performing the Bureau's functions under **section 8A or 8B**, the Director may apply in writing to the Minister for the issue of—

"(a) an interception warrant authorising the use of interception devices to intercept communications not otherwise

lawfully obtainable by the Bureau of the following kinds:

"(i) communications made or received by 1 or more persons or classes of persons specified in the authorisation or made or received in 1 or more places or classes of places specified in the authorisation:

"(ii) communications that are sent from, or are being sent to, an overseas country:

"(b) an access authorisation authorising the accessing of 1 or more specified information infrastructures or classes of information infrastructures that the Bureau cannot otherwise lawfully access.

"(2) The Minister may grant the proposed interception warrant or access authorisation if satisfied that—

"(a) the proposed interception or access is for the purpose of performing a function of the Bureau under **sections 8A and 8B**; and

"(b) the outcome sought to be achieved under the proposed interception or access justifies the particular interception or access; and

"(c) the outcome is not likely to be achieved by other means; and

"(d) there are satisfactory arrangements in place to ensure that nothing will be done in reliance on the warrant or authorisation beyond what is necessary for the proper performance of a function of the Bureau; and

"(e) there are satisfactory arrangements in place to ensure that the nature and consequences of acts done in reliance on the warrant or authorisation will be reasonable, having regard to the purposes for which they are carried out.

"(3) Before issuing a warrant or an authorisation, the Minister must consult the Minister of Foreign Affairs about the proposed warrant or authorisation.

"(4) The Minister may issue a warrant or an authorisation subject to any conditions that the Minister considers desirable in the public interest.

"(5) This section applies despite anything in any other Act.

"**15B Involvement of Commissioner of Security Warrants**

"(1) An application for, and issue of, an interception warrant or access authorisation under **section 15A** must be made jointly to, and issued jointly by, the Minister and the Commissioner of Security Warrants if anything that may be done under the warrant or authorisation is for the purpose of intercepting the private communications of a New Zealand citizen or permanent resident of New Zealand under—

"(a) **section 8A**; or

"(b) **section 8B**, to the extent that intercepting the person's private communications under that section is not precluded by **section 14**.

"(2) For the purposes of **subsection (1)**, **section 15A** applies—

"(a) as if references to the Minister were references to the Minister and the Commissioner of Security Warrants; and

"(b) with any other necessary modifications.

"(3) In this section, **Commissioner of Security Warrants** means the Commissioner of Security Warrants appointed under section 5A of the New Zealand Security Intelligence Service Act 1969."

15 Section 16 amended (Certain interceptions permitted without interception warrant or computer access authorisation)

(1) In the heading to section 16, delete "**computer**".

(2) In section 16, before subsection (1), insert:

"(1A) This section—

"(a) applies to the interception of communications for the purpose of the Bureau's functions in **sections 8A and 8B**; but

"(b) does not authorise anything to be done for the purpose of intercepting the private communications of a New Zealand citizen or permanent resident of New Zealand."

(3) In section 16(1), delete "foreign".

(4) Replace section 16(2) with:

"(2) The Director, or an employee of the Bureau, or a person acting on behalf of the Bureau may, without an interception warrant,

or, as the case requires, without an access authorisation, intercept communications by using an interception device or by accessing an information infrastructure, but only if—

"(a) the interception does not involve any activity specified in section 15(1); and

"(b) any access to an information infrastructure is limited to access to 1 or more communication links between computers or to remote terminals; and

"(c) the interception is carried out by the Director or with the authority of the Director for the purpose of performing the Bureau's function in **section 8A or 8B**."

16 Section 17 and cross-heading repealed

Repeal section 17 and the cross-heading above section 17.

17 Section 18 amended (Persons acting under warrant)

(1) In the heading to section 18, after "**warrant**", insert "**or access authorisation**".

(2) Replace section 18(1) with:

"(1) Every interception warrant and access authorisation must specify the person or class of persons who may make the interception or obtain the access authorised by the warrant or the authorisation."

(3) In section 18(2),—

(a) after "A warrant", insert "or an authorisation"; and

(b) after "the warrant", insert "or authorisation".

(4) In section 18(3), after "warrant", insert "or authorisation".

(5) In section 18(4),—

(a) after "a warrant", insert "or an authorisation"; and

(b) after "the warrant", insert "or the authorisation".

18 Section 19 and cross-heading replaced

Replace section 19 and the cross-heading above section 19 with:

"Register of interception warrants and access authorisations

"19 Register of interception warrants and access authorisations

"(1) The Director must keep a register of interception warrants and access authorisations issued under this Part.

"(2) The following information must be entered in the register in relation to each interception warrant and access authorisation issued under this Part:

"(a) the date of issue:

"(b) the period for which the warrant or authorisation is issued:

"(c) the function or functions of the Bureau to which the warrant or authorisation relates:

"(d) in the case of a warrant, the interception device or interception devices specified:

"(e) in the case of an authorisation,—

"(i) any person specified in the authorisation:

"(ii) any place specified in the authorisation:

"(iii) the information infrastructure or information infrastructures specified in the authorisation:

"(iv) any conditions specified in the authorisation.

"(3) The Director must make the register available to the Minister or the Inspector-General of Intelligence and Security as and when requested by the Minister or the Inspector-General.

"Urgent issue of warrants and authorisations

"19A Urgent issue of warrants and authorisations

"(1) This section applies if—

"(a) the Minister is unavailable to issue an interception warrant or access authorisation; and

"(b) circumstances make it necessary to issue a warrant or an authorisation before the Minister is available to do so.

"(2) Any of the following may issue a warrant or an authorisation:

"(a) the Attorney-General:

"(b) the Minister of Defence:

"(c) the Minister of Foreign Affairs.

"(3) A person issuing a warrant or an authorisation under **subsection (2)** may do so only to the same extent and subject to the same terms and conditions as apply to the issue of a warrant or an authorisation by the Minister."

19 Section 20 amended (Director's functions in relation to warrants and authorisations not to be delegated)

In section 20, replace "section 17 or section 19" with "**section 15A**".

20 Section 21 replaced (Action taken in accordance with warrant or authorisation justified)

Replace section 21 with:

"**21 Immunity from civil and criminal liability**

"(1) Every person is immune from civil or criminal liability—

"(a) for any act done in good faith in order to obtain a warrant or an authorisation under this Act:

"(b) for anything done in good faith under a warrant or an authorisation under this Act or under section 16, if done in a reasonable manner.

"(2) Every person is immune from civil and criminal liability for any act done in good faith and in a reasonable manner in order to assist a person to do anything authorised by a warrant or an authorisation under this Act or under section 16.

"(3) In any civil proceeding in which a person asserts that he or she has an immunity under this section, the onus is on the person to prove the facts necessary to establish the basis of the claim.

"(4) Section 86 of the State Sector Act 1988 applies to the Director and any employee of the Bureau subject to this section."

21 Section 22 amended (Term of warrant or authorisation)

In section 22(1), delete "computer".

22 Section 23 amended (Destruction of irrelevant records obtained by interception)

(1) In section 23(1), delete "computer".

(2) In section 23(1), after "except to the extent", insert "permitted by **section 25** or to the extent".

(3) In section 23(1)(a), replace "section 7(1)(a)" with "**section 7**".

(4) In section 23(1)(b), replace "section 8" with "**section 8A or 8B**".

23 Section 24 amended (Duty to minimise impact of interception on third parties)

In section 24, replace "a computer" with "an".

24 Section 25 replaced (Prevention or detection of serious crime)

Replace section 25 with:

"**25 When incidentally obtained intelligence may be retained and communicated to other persons**

"(1) Despite section 23, the Director may—

"(a) retain incidentally obtained intelligence that comes into the possession of the Bureau for 1 or more of the purposes specified in **subsection (2)**; and

"(b) communicate that intelligence to the persons specified in **subsection (3)**.

"(2) The purposes are—

"(a) preventing or detecting serious crime in New Zealand or any other country:

"(b) preventing or responding to threats to human life in New Zealand or any other country:

"(c) identifying, preventing, or responding to threats or potential threats to the national security of New Zealand or any other country.

"(3) The persons are—

"(a) any employee of the New Zealand Police:

"(b) any member of the New Zealand Defence Force:

"(c) the Director of Security under the New Zealand Security Intelligence Service Act 1969:

"(d) any other person that the Director thinks fit to receive the information."

25 New sections 25A and 25B and cross-heading inserted

After section 25, insert:

"Protection and disclosure of personal information

"25A Formulation of policy on personal information

"(1) As soon as is reasonably practicable after the commencement of this section, the Director must, in consultation with the Inspector-General of Intelligence and Security and the Privacy Commissioner, formulate a policy that applies to the Bureau (in a manner compatible with the requirements of national security) the principles set out in **section 25B**.

"(2) The policy must require—

"(a) all employees and persons acting on behalf of the Bureau to comply with the policy; and

"(b) the level of compliance with the policy to be regularly audited; and

"(c) the Director to advise the Privacy Commissioner of the results of audits conducted under the policy.

"(3) The Director must regularly review the policy and, if he or she considers it appropriate to do so, revise the policy in consultation with the Inspector-General of Intelligence and Security and the Privacy Commissioner.

"25B Principles to protect personal information

The principles referred to in **section 25A(1)** are as follows:

"(a) the Bureau must not collect personal information unless—

"(i) the information is collected for a lawful purpose connected with a function of the Bureau; and

"(ii) the collection of the information is reasonably necessary for that purpose, having regard to the nature of intelligence gathering:

"(b) the Bureau must ensure—

"(i) that any personal information it holds is protected by such security safeguards as it is reasonable in the circumstances to take against—

"(A) loss; and

"(B) access, use, modification, or disclosure, except with the authority of the Bureau; and

"(C) other misuse; and

"(ii) that if it is necessary for any personal information that it holds to be given to a person in connection with the provision of a service to the Bureau, everything reasonably within the power of the Bureau is done to prevent unauthorised use or unauthorised disclosure of the information:

"(c) the Bureau must not use personal information without taking such steps (if any) as are, in the light of the interests and constraints of national security and the nature of intelligence gathering, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, relevant, and not misleading:

"(d) the Bureau must not keep personal information longer than is required for the purposes for which the information may be lawfully used."

26 **Consequential amendments**

The Acts listed in the **Schedule** are consequentially amended in the manner indicated in that schedule.

Part 2
Amendments to Inspector-General of Intelligence and Security Act 1996

27 **Principal Act**

This **Part** amends the Inspector-General of Intelligence and Security Act 1996 (the **principal Act**).

28 **Section 2 amended (Interpretation)**

In section 2(1), insert in its appropriate alphabetical order:

"**Deputy Inspector-General** means the Deputy Inspector-General of Intelligence and Security holding office under **section 5**".

29 **Section 5 and cross-heading replaced**

Replace section 5 and the cross-heading above section 5 with:

"Inspector-General and Deputy Inspector-General of Intelligence and Security

"5 Inspector-General and Deputy Inspector-General of Intelligence and Security

"(1) There must be—

"(a) an Inspector-General of Intelligence and Security; and

"(b) a Deputy Inspector-General of Intelligence and Security.

"(2) The Inspector-General and Deputy Inspector-General must be appointed by the Governor-General on the recommendation of the Prime Minister following consultation with the Intelligence and Security Committee established by section 5 of the Intelligence and Security Committee Act 1996.

"(3) The Deputy Inspector-General has and may exercise and perform the powers and functions of the Inspector-General (whether under this Act or any other enactment), but subject to—

"(a) the control and direction of the Inspector-General; and

"(b) to avoid doubt, the same duties, obligations, restrictions, and terms under which the Inspector-General exercises and performs his or her powers and functions.

"(4) Sections 7 to 9 and 18 apply to the Deputy Inspector-General as if references in those sections to the Inspector-General were references to the Deputy Inspector-General.

"(5) If there is a vacancy in the office of the Inspector-General, or if the Inspector-General is absent from duty for any reason, the Deputy Inspector-General has and may exercise and perform all the powers, functions, and duties of the Inspector-General for as long as the vacancy or absence continues.

"(6) The fact that the Deputy Inspector-General exercises or performs any power, function, or duty of the Inspector-General is, in the absence of proof to the contrary, conclusive evidence of the Deputy Inspector-General's authority to do so."

30 Section 6 amended (Term of office)

(1) Replace section 6(1) with:

"(1) Every person appointed as the Inspector-General or Deputy Inspector-General—

"(a) is to be appointed for a term not exceeding 3 years; and

"(b) may be reappointed, but in the case of the Inspector-General only once."

(2) In section 6(2) and (3), after "Inspector-General", insert "or Deputy Inspector-General" in each place.

31 Section 11 amended (Functions of Inspector-General)

(1) Replace section 11(1)(c), (d), and (da) with:

"(c) to inquire at the request of the Minister or the Prime Minister or of the Inspector-General's own motion, but subject to the concurrence of the Minister, into any matter where it appears that a New Zealand person has been or may be adversely affected by any act, omission, practice, policy, or procedure of an intelligence and security agency:

"(ca) to inquire at the request of the Minister or the Prime Minister or of the Inspector-General's own motion into the propriety of particular activities of an intelligence and security agency:

"(d) without limiting paragraph (a), to review at intervals of not more than 12 months—

"(i) the effectiveness and appropriateness of the procedures adopted by each intelligence and security agency to ensure compliance with its governing legislation in relation to the issue and execution of warrants and authorisations; and

"(ii) the effectiveness and appropriateness of compliance systems concerning operational activity, including all supporting policies and practices of an intelligence and security agency relating to—

"(A) administration; and

"(B) information management; and

"(C) risk management; and

"(D) legal compliance generally:

"(da) to conduct unscheduled audits of the procedures and compliance systems described in **paragraph (d)**:".

(2) Repeal section 11(2).

(3) In section 11(3), replace "(1)(c)(ii)" with "**(1)(ca)**".

32 Section 12 amended (Consultation)

Replace section 12(2) with:

"(2) The Inspector-General may—

"(a) consult any of the persons specified in **subsection (3)** about any matter relating to the functions of the Inspector-General under section 11; and

"(b) despite section 26(1), disclose to any of the persons consulted any information that the Inspector-General considers necessary for the purpose of the consultation.

"(3) The persons are—

"(a) the Controller and Auditor-General:

"(b) an Ombudsman:

"(c) the Privacy Commissioner:

"(d) a Human Rights Commissioner:

"(e) the Independent Police Conduct Authority."

33 Section 15 amended (Jurisdiction of courts and other agencies not affected)

In section 15(3), replace "or of the Privacy Commissioner" with ", the Privacy Commissioner, a Human Rights Commissioner, or the Independent Police Conduct Authority".

34 Section 25 amended (Reports in relation to inquiries)

After section 25(5), insert:

"(6) As soon as practicable after receiving a report from the Inspector-General, the Minister—

"(a) must provide his or her response to the Inspector-General and the chief executive of the intelligence and security agency concerned; and

"(b) may provide his or her response to the Intelligence and Security Committee established under section 5 of the Intelligence and Security Committee Act 1996.

"(7) **Subsection (6)** does not apply to the extent that a report relates to employment matters or security clearance issues."

35 New section 25A inserted (Publication of Inspector-General's reports under section 25)

After section 25, insert:

"25A Publication of Inspector-General's reports under section 25

"(1) As soon as practicable after forwarding a report as required by section 25(1), the Inspector-General must make a copy of the report publicly available on an Internet site maintained by or on behalf of the Inspector-General.

"(2) However, the Inspector-General must not, in the copy of a report made publicly available under **subsection (1)**, disclose—

"(a) information the public disclosure of which would be likely to prejudice the entrusting of information to the Government of New Zealand on a basis of confidence—

"(i) by the government of any other country or any agency of such a government; or

"(ii) by any international organisation; or

"(b) information the public disclosure of which would be likely to endanger the safety of any person; or

"(c) the identity of any person who is or has been an officer, employee, or agent of an intelligence and security agency other than the chief executive, or any information from which the identity of such a person could reasonably be inferred; or

"(d) information the public disclosure of which would be likely to prejudice—

"(i) the continued discharge of the functions of an intelligence and security agency; or

"(ii) the security or defence of New Zealand or the international relations of the Government of New Zealand; or

"(e) any information about employment matters or security clearance issues."

36 Section 27 amended (Reports by Inspector-General)

(1) After section 27(2)(b), insert:

"(ba) certify whether each intelligence and security agency's compliance systems are sound; and".

(2) In section 27(3), replace "lay a copy of the report before" with "present a copy of the report to".

(3) In section 27(4) and (6), replace "laid before" with "presented to".

(4) After section 27(6), insert:

"(6A) As soon as practicable after a copy of the report is presented to the House of Representatives under subsection (3), the Inspector-General must make a copy of the report (as presented to the House of Representatives) publicly available on an Internet site maintained by or on behalf of the Inspector-General."

Part 3
Amendments to Intelligence and Security Committee Act 1996

37 Principal Act

This **Part** amends the Intelligence and Security Committee Act 1996 (the **principal Act**).

38 Section 6 amended (Functions of Committee)

Replace section 6(1)(e) with:

"(e) subject to section 18,—

"(i) to present an annual report to the House of Representatives on the activities of the Committee; and

"(ii) to make an annual report publicly available on the Internet site of the New Zealand Parliament."

39 New section 7A inserted (Further provisions relating to chairperson)

After section 7, insert:

"7A **Further provisions relating to chairperson**

"(1) **Subsection (2)** applies if—

"(a) the Committee is, in the course of conducting a financial review of an intelligence and security agency, discussing any matter relating to the performance of the intelligence and security agency; and

"(b) the Prime Minister is the responsible Minister under the legislation governing the intelligence security agency.

"(2) If the Prime Minister is chairing the meeting of the Committee at which the matter is discussed,—

"(a) the Prime Minister must not act as chairperson of the Committee; and

"(b) another member of the Committee nominated by the Prime Minister, being one of the 2 members appointed under section 7(1)(c), must act as chairperson.

"(3) The chairperson of the Committee may appoint either of the following (if not already a member of the Committee) to be an alternate chairperson to act as chairperson at the discretion of the chairperson in the absence of the chairperson at a meeting of the Committee:

"(a) the Deputy Prime Minister:

"(b) the Attorney-General."

40 Section 18 amended (Restrictions on reports to House of Representatives)

In section 18(1), replace "reporting" with "presenting an annual report or other report".

Schedule

s 26

Consequential amendments

Radiocommunications Act 1989 (1989 No 148)

In section 133A(2)(c)(ii), replace "foreign intelligence" with "intelligence about the capabilities, intentions, and activities of foreign persons and foreign organisations".

Repeal section 133A(3)(a).

Search and Surveillance Act 2012 (2012 No 24)

In section 47(1)(c)(ii), replace "17" with "**15A(1)(a)**".

Telecommunications (Interception Capability) Act 2004 (2004 No 19)

In section 3(1), definition of **interception warrant**, paragraph (c), replace "17" with "**15A(1)(a)**".

In section 3(1), definition of **other lawful interception authority**, replace paragraph (a)(ii) with:

> "(ii) to access an information infrastructure (within the meaning of the Government Communications Security Bureau Act 2003) that is granted under **section 15A(1)(b)** of that Act; and".

Cabinet

CAB Min (13) 14/1

Copy No: 6

Minute of Decision

Government Communications Security Bureau and Related Legislation Amendment Bill: Approval for Introduction

Portfolios: Minister Responsible for the GCSB / Minister in Charge of the NZSIS

On 6 May 2013, Cabinet:

Background

1 **noted** that in December 2012, the Cabinet Committee on Domestic and External Security (DES):

1.1 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);

1.2 noted that the Bill would be enacted by August 2012;

[DES Min (12) 4/1-1]

Government Communications Security Bureau and Related Legislation Amendment Bill

2 **noted** that the Government Communications Security Bureau and Related Legislation Amendment Bill (the Amendment Bill) is an omnibus Bill that amends the Government Communications Security Bureau Act 2003, the Inspector-General of Intelligence and Security Act 1996, and the Intelligence and Security Committee Act 1996;

3 **noted** that on 22 April 2013, Cabinet authorised a group of Ministers (Joint Ministers), comprising the Prime Minister, Hon Bill English, Hon Steven Joyce, Hon Christopher Finlayson and Hon Amy Adams to have Power to Act to finalise the intelligence bill and the interception and network security bill for introduction, subject to final consideration by Cabinet on 6 May 2013 [CAB Min (13) 13/24];

4 **noted** that on 2 May 2013, Joint Ministers approved the contents of the Amendment Bill for introduction;

5 **confirmed** the decision by Joint Ministers to approve for introduction the Government Communications Security Bureau and Related Legislation Amendment Bill [PCO 17322/9.0];

6 **agreed** that the Amendment Bill be introduced under urgency in the week of 6 May 2013;

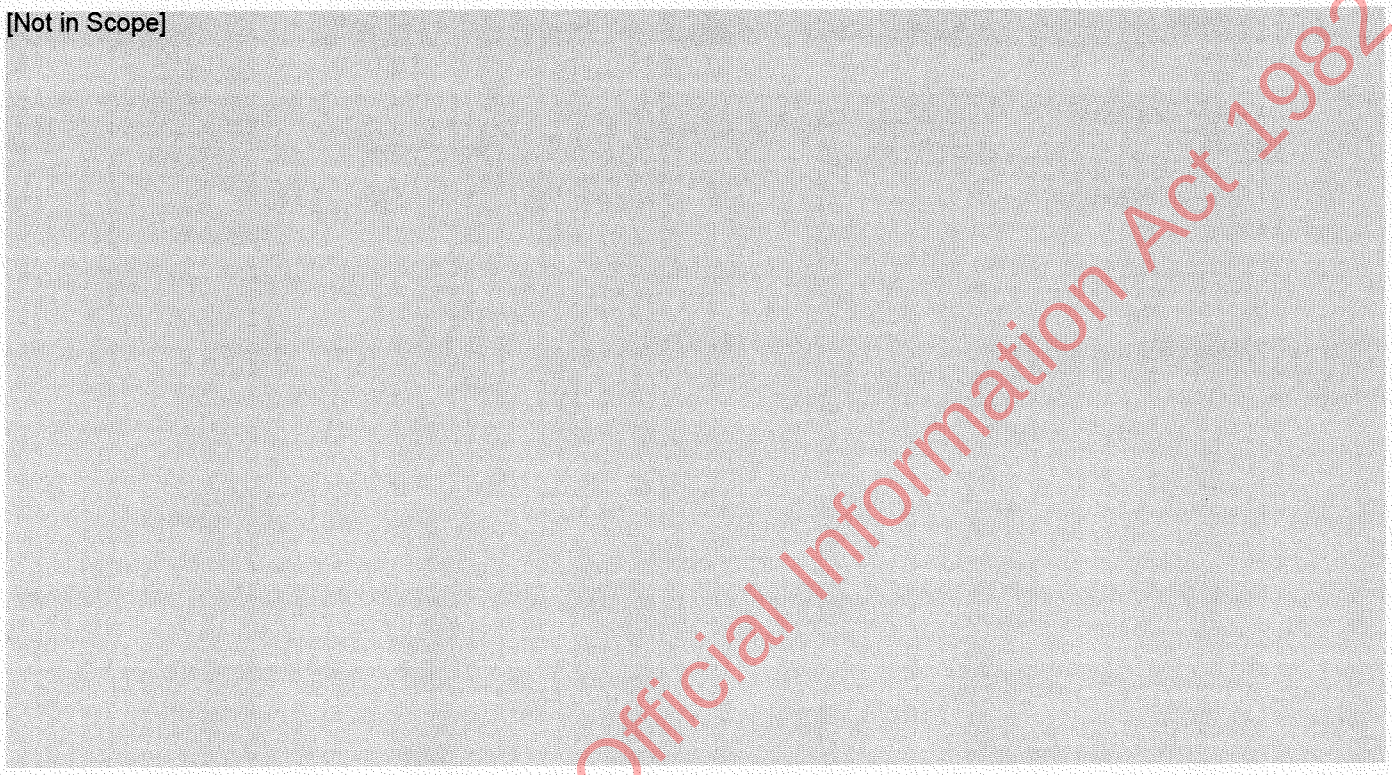
7 **agreed** that the government propose that the Amendment Bill be:

7.1 referred to the Intelligence and Security Committee for consideration;

7.2 reported back by 26 July 2013;

7.3 enacted by August 2013;

[Not in Scope]



Rebecca Kitteridge
Secretary of the Cabinet

Reference: CAB (13) 239

Distribution (see over):

Distribution:

Prime Minister
- Chief Executive, DPMC
- Director PAG, DPMC
- Director, ICG, DPMC
- Director, NAB, DPMC
- Director, GCSB
- Director, NZSIS

Minister of Finance
- Secretary to the Treasury

Minister of Justice
- Secretary for Justice

Attorney-General
- Solicitor-General

Minister of Defence
- Secretary of Defence
- Chief of Defence Force

Minister of Foreign Affairs and Trade
- Secretary of Foreign Affairs and Trade

Minister of Police
- Commissioner of Police

Minister for Communications and Information Technology
- Chief Executive, MBIE (Communications and IT)

Chief Parliamentary Counsel

Legislation Coordinator

Secretary, DES

Item 10

Cabinet

CAB (14) 324

Copy No: 24

Summary of Paper

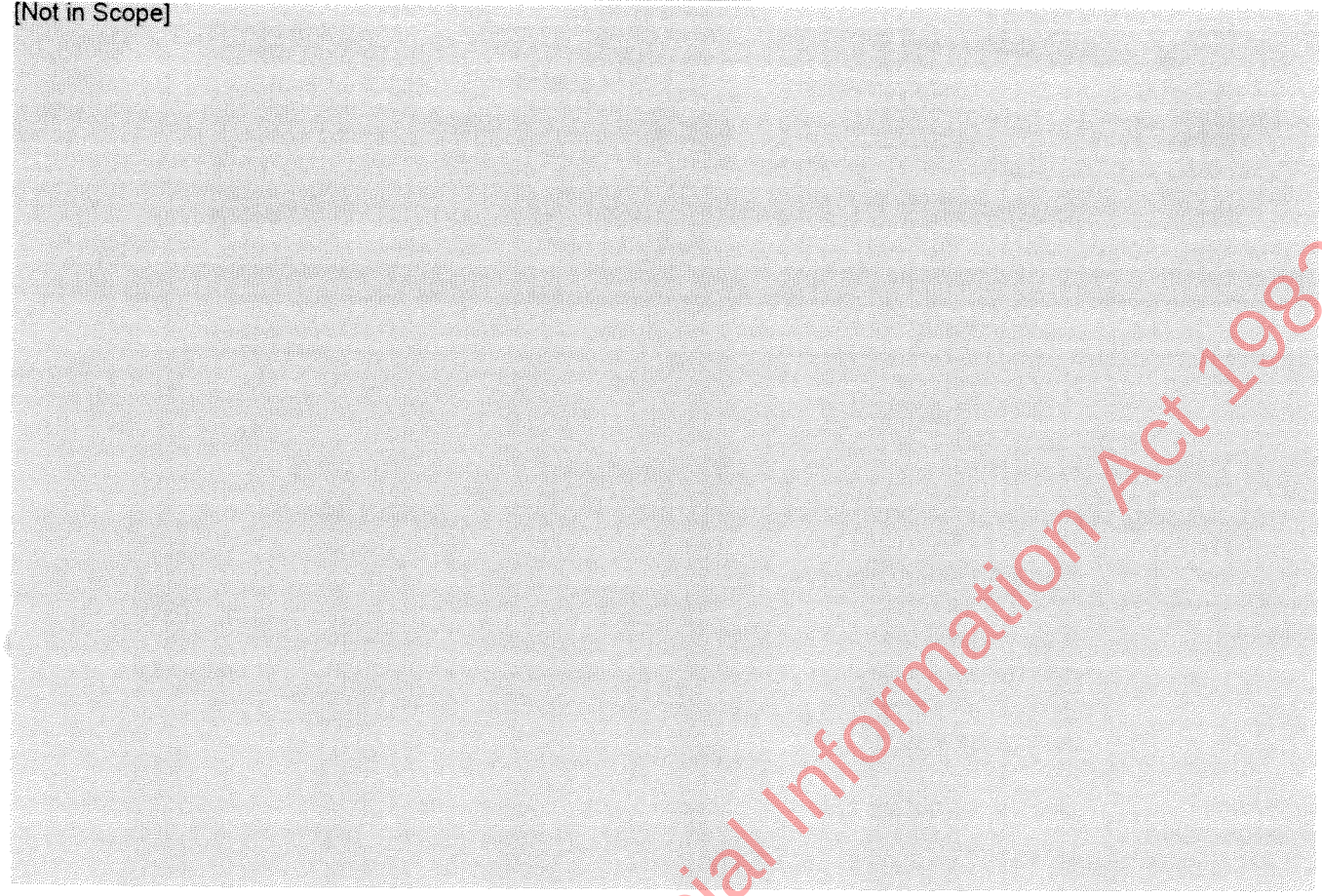
20 June 2014

New Zealand Intelligence Community Strategy, Capability and Resourcing Review: Commencement and Policy Expectations

Portfolios	Prime Minister / Finance
Purpose	This paper notes that the New Zealand Intelligence Community (NZIC) has commenced a Strategy, Capability and Resourcing Review (SCRR), and seeks agreement to endorse provisional policy expectations for the NZIC for the purposes of the SCRR.
Previous Consideration	See the summary below.

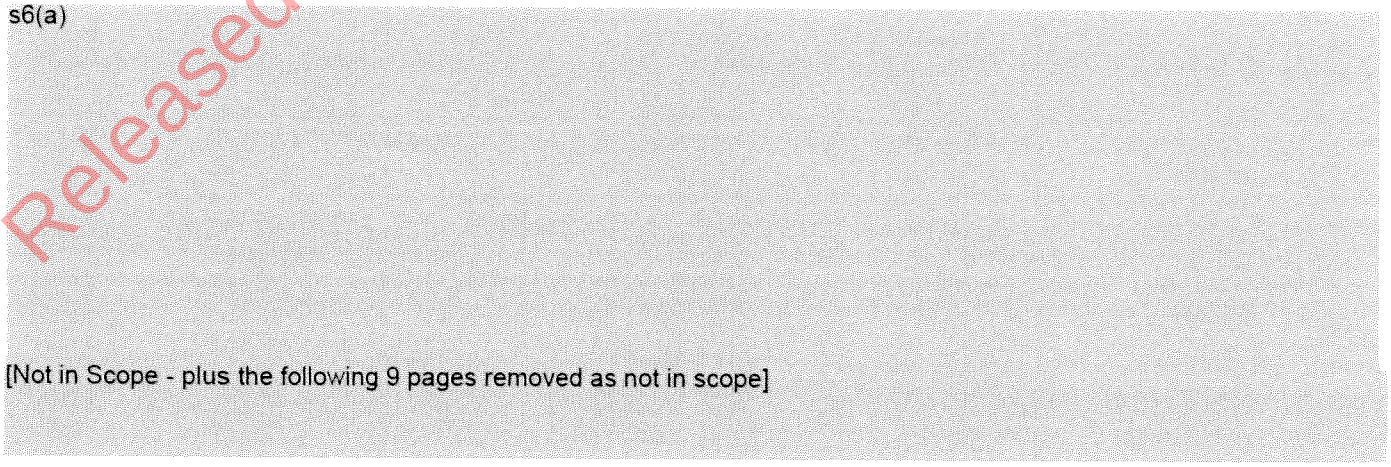
[Not in Scope - plus the following 6 pages removed as not in scope]

[Not in Scope]



12. The March 2013 *Review of Compliance at the GCSB* by Rebecca Kitteridge highlighted the difficulties in interpreting the GCSB Act and the need to improve the compliance framework for the GCSB to ensure that it is acting in accordance with the law. This led to a range of legislative amendments to the GCSB Act and changes to the GCSB's compliance framework. In addition amendments were made to the Inspector-General of Intelligence and Security Act 1996 (IGIS Act) and the ISC Act to strengthen the external oversight of the GCSB and NZSIS. Under the Telecommunications (Interception, Capability and Security) Act 2013 (TICSA), the GCSB was also given a regulatory role for the first time. The financial impact of the changed GCSB Act, enhanced oversight and the GCSB's new regulatory role were to be met from existing NZIC baselines; the NZIC has consequently reprioritised expenditure from its intelligence and security outputs to meet these new needs.

s6(a)



[Not in Scope - plus the following 9 pages removed as not in scope]