This paper has been redacted for public release.

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

This paper has been redacted for public release.

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 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. [text removed] 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.

This paper has been redacted for public release.

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 communications 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	Other agencies will not have to duplicate technical capabilities and expertise already held by the Crown, and make effective and

expertise.	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 re-enacting 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.