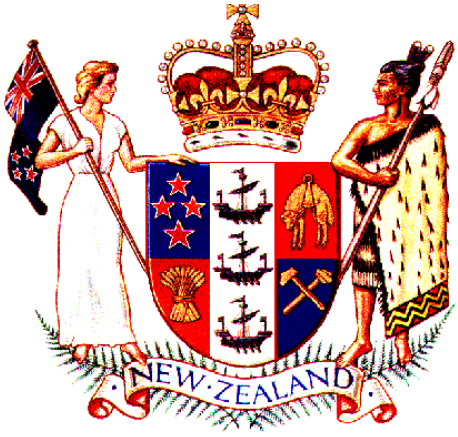


Review of Compliance
at the
Government Communications Security Bureau

Rebecca Kitteridge, March 2013

This page intentionally left blank.

Contents

This page intentionally left blank.

Executive summary

1. The Government Communications Security Bureau (GCSB) plays a vital role in New Zealand's security by obtaining, providing and protecting sensitive information. The time I have spent within GCSB has left me in no doubt that New Zealand needs this organisation now more than ever. The increasing threat of cyber attacks and the protective role GCSB plays is one part of this story, but GCSB does a wide range of other things that are essential to the well-being of New Zealand.

2. It is, however, vital that an organisation that exercises intrusive powers of the state does so in a way that is entirely lawful. Where a state organisation's internal operations must necessarily remain secret, because of their sensitivity, there need to be robust internal systems and effective external oversight so that the public can be confident in the lawfulness of those operations.

3. Concerns were raised about legal compliance within GCSB as a result of events involving Mr Kim Dotcom. I was seconded to GCSB to carry out a review of compliance systems and processes at GCSB, commencing on 2 October 2012. The review took six months. In the course of this review, I focused on two main areas:

    a. supporting the Director of GCSB to ensure that all of GCSB's activities were lawful, and in particular activities that the Director had directed be stopped at the end of September 2012, before they could be considered for resumption; and

    b. reviewing GCSB's compliance framework.

4. The Director was concerned to ensure that no other errors had occurred that were similar to that concerning Mr Dotcom. The Director's concern led to a number of other instances, in which GCSB had assisted domestic law enforcement agencies between 1 January 2009 and 26 September 2012, being referred to the Inspector-General of Intelligence and Security for review. Those cases were subsequently found to be lawful.

5. The review of activities that had stopped (involving assistance to other domestic agencies) led the Bureau to seek legal advice from the Crown Law Office on a number of issues. In relation to some assistance that GCSB has provided to the New Zealand Security Intelligence Service and (more rarely) the Police since before the enactment of the GCSB Act 2003, the Solicitor-General confirmed the difficulties in interpreting the GCSB Act and the risk of an adverse outcome if a Court were to consider

the basis of that assistance. All relevant instances of assistance (concerning 88 individuals in total), dating between 1 April 2003 and 26 September 2012, have been identified and a report has been provided to the Minister Responsible for the GCSB, in parallel with this report, so that he can determine the appropriate action to be taken.

6. I conclude, in relation to this and other legal issues, and to ensure that GCSB can carry out its work in the future with a clear understanding of the law, that legislative clarification would be desirable.

7. The second limb of my review involved considering GCSB's compliance against a standard compliance model, involving the following cycle of activity:

    a. assessing and identifying legal compliance obligations;

    b. supporting compliant behaviour and preventing non-compliance (including internal guidance, procedures, internal audit, and external oversight);

    c. responding to non-compliant behaviour;

    d. external reporting;

    e. measuring; and

    f. improving.

8. Part I of this report sets out my analysis of GCSB's compliance activity against this standard compliance model. In all these areas of compliance significant opportunities for improvement are identified. I also recommend that external oversight of GCSB be strengthened.

9. In the course of this work I concluded that the issues identified in relation to compliance were symptomatic of underlying problems within GCSB, concerning GCSB's structure, management of its information, capability and capacity. Those issues are addressed in Part II of this report.

10. A consolidated table of recommendations is attached at Appendix 1. If implemented, the changes I recommend will constitute a considerable change programme, which in my view will take more than one year to complete. It is important to note that my report represents a snapshot in time, and that a number of recommended changes have already been made or are in train.

11. Throughout my time at GCSB the staff with whom I spoke consistently expressed their commitment to the rule of law. It is my strong belief that when GCSB has addressed the issues raised in this report, it will not only be an organisation that continues to provide great public value, but also an institution in which the public can have trust and confidence.

Rebecca Kitteridge
22 March 2013

This page intentionally left blank.

Summary of key recommendations

I recommend that:

1. Legislative reform be considered, to clarify the application of the GCSB Act 2003 to GCSB's work;

2. GCSB implement a compliance framework, which will include:

    a. systems for assessing and identifying compliance obligations;

    b. risk assessment, accessible and authoritative guidance, clear procedures and training to support compliant behaviour and prevent non-compliance;

    c. monitoring compliance and detecting non-compliance, through targeted internal audit and robust external oversight;

    d. explicit and escalating internal responses to non-compliant activity;

    e. external reporting on compliance breaches to the Inspector-General of Intelligence and Security (IGIS), and on compliance statistics to the Intelligence Security Committee and to the public through the GCSB Annual Report;

    f. systems to measure the organisation's compliance state against explicit objectives, and to track trends;

    g. regular review of the compliance systems in light of compliance performance, in order to achieve continuous improvement;

3. policy work be undertaken with a view to strengthening the Office of the IGIS, including broadening the pool of candidates, increasing the resources and staff supporting the IGIS, and making the work programme, audits and reporting expectations of the IGIS more explicit;

4. organisational factors that have contributed to GCSB's compliance issues be addressed, including;

    a. reorganising GCSB in a simpler, less fragmented way;

    b. reducing the number of small units and managers;

    c. centralising some key roles and giving them Bureau-wide reach;

    d. avoiding single points of dependence;

e. reconfiguring and strengthening the compliance and operational policy resources;

f. strengthening the legal resource, and considering including it in the Intelligence Community Shared Services;

g. providing greater support to GCSB's Strategic Leadership Board so focus is on strategy, risk, workforce capability, etc;

h. improving performance management practices;

i. facilitating internal and external rotations and secondments;

j. appointing a professional Information Manager and addressing information management issues;

k. Strengthening the relationship with the Crown Law Office, and other relevant government agencies.

Introduction

Background and context

1. GCSB plays a vital role in New Zealand's security by obtaining, providing and protecting sensitive information. Some people will always be uncomfortable with the notion of intelligence organisations. Organisations of this kind, however, are found in every like-minded parliamentary democracy. In New Zealand, Parliament has placed GCSB on a statutory footing, and has set out its objectives and functions in the GCSB Act 2003.

2. The GCSB Act reflects the fact that GCSB has two main functions: information assurance (increasingly focused on protection against cyber attacks) and obtaining foreign signals intelligence ("SIGINT").

3. Successive administrations have valued what GCSB provides and have supported its work. Over many years GCSB has given information to governments to support well informed policy decisions. It has protected New Zealand government communications and (increasingly) New Zealand's critical infrastructure and intellectual property. GCSB's work has helped to save lives and has contributed meaningfully to global security.

4. The time I have spent within GCSB has left me in no doubt that New Zealand needs this organisation now more than ever. The increasing threat of cyber attacks and the protective role GCSB plays is one part of this story, but GCSB does a wide range of other things that are essential to the well-being and prosperity of New Zealand. GCSB is also highly regarded by counterpart agencies for the contribution it makes to international security. It is a great pity – and quite a big problem for GCSB, in terms of public attitudes – that security considerations prevent this positive story from being told in more detail.

5. The reason I start this report with these comments is that they provide an important backdrop to this review, which has a narrow focus on compliance. The broader story cannot be included. It is my strong belief that when GCSB has addressed the issues raised in this report, it will not only be an organisation that continues to provide great public value, but also an institution in which the public can have trust and confidence.

The New Zealand Intelligence Community

6. The core New Zealand Intelligence Community (NZIC) comprises GCSB, the New Zealand Security Intelligence Service (NZSIS), and parts of the Department of the Prime Minister and Cabinet (DPMC). The individual agencies, and the NZIC collectively, have been the subject of scrutiny, both legislative and administrative, over many years. Recent years have seen a number of reviews and improvements:

    a. In June 2009 Cabinet initiated a review of the intelligence agencies, which was conducted by Simon Murdoch on behalf of the State Services Commissioner. The review proposed a number of initiatives to improve efficiency and co-ordination of the NZIC. The review also recommended strengthening governance, management and co-ordination arrangements, including adding a governance arm to the Officials Committee for Domestic and External Security Co-ordination (ODESC(G)).

    b. Michael Wintringham led a review entitled "A National Security and Intelligence Framework for New Zealand" in September 2009. The review considered the NZIC's role in supporting a national security system. There is now 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.

7. There is no doubt that these reviews resulted in a better co-ordinated, more effective, more efficient and accountable NZIC. Real change has been evident in the way that the community operates as a collective, resulting in better use of scarce resources in the interests of New Zealand's national security. The fact that my review identifies issues and recommends changes concerning compliance at GCSB should be seen in a larger context of very significant, ongoing efforts to improve the performance of the NZIC as a whole.

My approach to the review

8. My review was not an inquiry. It is true that it was initiated as a result of the events following the discovery that GCSB had unlawfully intercepted the communications of Mr Kim Dotcom. I was not, however, asked to investigate those events. I was asked by the Director of GCSB and the Chief Executive of the Department of the Prime Minister and Cabinet to accept a secondment to GCSB, in order to provide the Director with assurance that GCSB's activities are undertaken within its

powers and that adequate safeguards are in place. In particular, I was asked to:

a. review the systems, processes and capabilities underpinning the GCSB's collection and reporting;

b. build capability and provide assurance to the GCSB Director that the compliance framework has been reviewed, improved and is fit for purpose;

c. establish new, specific approval processes for activity in support of the Police and other law enforcement agencies.

9. It should be noted that my review was focused on GCSB's operations and whether there are systems in place to ensure the lawfulness of those operations under relevant New Zealand and international law. I did not review other aspects of compliance such as financial systems, security, or the way in which GCSB works with agencies internationally.

10. I commenced the secondment on 2 October 2012, for an initial period of up to three months (later extended to the end of March 2013). The full terms of reference for this review were developed after my arrival, and are attached as Appendix 2.

11. Despite the fact that the organisation was under considerable stress when I arrived, I found that staff were very welcoming. In the course of the review I spent many hours interviewing GCSB staff; during that process I talked to well over one hundred of them. They were open, non-defensive and helpful. It was clear that they take their special roles seriously and are deeply committed to protecting and advancing New Zealand's interests in accordance with the government's priorities. They universally expressed their commitment to comply with the law as they understood it. They were frank with me that they thought their compliance systems and processes could be improved, and made useful suggestions as to how. This review reflects what they told me. A list of the teams that I spoke to is included in Appendix 3.

12. I visited the intelligence and security organisations in Australia (in particular, the Defence Signals Directorate, or DSD) and the United Kingdom (in particular, the Government Communications Headquarters, or GCHQ), to discuss compliance processes and systems in those organisations. A list of the agencies I visited is included in Appendix 3.

13. I also read a considerable amount of background material, listed in Appendix 4.

14. While I was conducting the review, I was also supporting the Director to implement change and improvements. It is therefore important to note two things in relation to this report:

    a. it represents a snapshot in time;

    b. action to remedy many of the issues identified in this report is already underway (and in some cases is complete).

15. The findings in this report are specific to GCSB, and nothing should be extrapolated from it with regard to other parts of the Intelligence Community.

16. As a final introductory point, I would note that although I have completed the tasks envisaged in paragraph 8(a) and 8(c) above, I have not been able to complete the work contemplated in paragraph 8(b) (i.e. to build capability and provide assurance to the GCSB Director that the compliance framework has been reviewed, improved and is fit for purpose). There are underlying issues that need to be addressed before those matters can be resolved (as discussed in Part II of this report). The changes required will take a considerable effort, which I estimate will take a team more than one year to implement. The recommendations in this report, once implemented, however, will result in an improved compliance framework that is fit for purpose.

Legal issues identified during the review

17. When I arrived at GCSB I found that, in response to the error regarding Mr Dotcom, the Director had taken a very conservative stance as to the activities GCSB was undertaking. On 26 September 2012, he had directed that almost all GCSB support for domestic agencies was to cease with immediate effect. The Director had stated that the cessation of support would continue until he was satisfied that GCSB had interpreted all the relevant legal issues correctly.

18. The Director was also concerned to ensure that no other errors had occurred that were similar to that concerning Mr Dotcom. On 3 October 2012 (taking account of the Inspector-General's initial findings in respect of Mr Dotcom) the Director invited the Inspector-General of Intelligence and Security to review the three other cases in which assistance had been provided to law enforcement agencies in New Zealand since January 2009 that potentially involved New Zealand citizens or permanent residents. The Inspector-General was also invited to review all the other cases of GCSB assistance to those agencies during the same

period. The Inspector-General subsequently concluded that none of these cases was in breach of GCSB's legislation.

19. While that process was continuing, other assistance to domestic agencies remained stopped. The conservative approach taken by the Director turned out to be well justified. As the newly arrived lawyers (on secondment from Crown Law) and I commenced our work, we encountered difficulty in applying aspects of the GCSB Act to some of the activities of GCSB that had ceased. Most of the difficulties were connected with section 14 of the GCSB Act, which provides that GCSB may not "take any action for the purpose of intercepting the communications of a person … who is a New Zealand citizen or a permanent resident."

20. Consideration of this prohibition, which is stated in absolute terms, raised questions regarding some long-standing (and in my view uncontroversial) practices:

    a. If GCSB wanted to test new equipment, could it do so in New Zealand? Would section 14 be breached, even if mitigating steps were taken such as choosing a remote location and intercepting the communications of GCSB employees who had volunteered to participate in the testing? Or would GCSB have to test the equipment overseas, at some considerable cost?

    b. Similarly, questions were raised about the application of section 14 to the information assurance function of GCSB. If, for example, a government agency requested GCSB to analyse the agency's network in a case of a suspected malware attack, could GCSB help? If not, how could GCSB carry out this aspect of its important protective function?

21. Determining these and other similar questions involved analysis of the word "purpose" in section 14 and other legal interpretation points. In some cases the activity resumed, on a "best interpretation" basis, but with acknowledgement that the current wording of the Act is not completely clear in its application.

22. Other activities, reflecting long-standing assumptions about the application of the Act over the course of successive administrations, were not resumed. The most significant of these concerned the exercise of the function spelled out in section 8(1)(e) of the GCSB Act, which states as one of the Bureau's functions: "to co-operate with, or to provide advice and assistance to, any public authority …"

23. The internal legal advice at GCSB (as reflected in its internal guidance) had been that it was lawful for GCSB to assist domestic agencies such as the NZSIS or the Police, under this provision, in two circumstances:

    a. Firstly, it was long-standing practice – going back to before the enactment of the GCSB Act in 2003 – for GCSB to provide assistance (i.e. its specialist capabilities) to the NZSIS on the basis of NZSIS warrants. The clear understanding within GCSB was that in such cases section 14 did not apply because GCSB was acting as the agent of the requesting agency and was therefore operating under the legal authority of the warrants. If the NZSIS, with the authority of an intelligence warrant, requested GCSB to provide assistance in cases involving New Zealand citizens or permanent residents, GCSB provided that assistance.

    b. The second situation involved metadata (information about information; for example, the kind of information that appears on a telephone bill). The understanding within the Bureau (as reflected in its internal guidance) was that metadata was not a "communication" for the purposes of the prohibition expressed in section 14 of the GCSB Act. It was the view within GCSB that GCSB could, on request, lawfully obtain and provide information about metadata involving New Zealanders, without the authority of a warrant, in accordance with its function of co-operating with and providing assistance to public authorities.

24. I do not want to suggest that GCSB was in the business of routinely providing assistance to domestic agencies in cases involving New Zealanders, because that is not the case. GCSB is first and foremost a foreign intelligence organisation, and foreign intelligence is by far its greater focus. Most of the support provided to domestic agencies concerned non-New Zealanders. From time to time, however, in the two circumstances set out in the previous paragraph, GCSB provided its specialised assistance to New Zealand agencies in cases involving New Zealand citizens or permanent residents, in the belief that the assistance was provided lawfully. The assistance was provided to NZSIS to help combat threats to New Zealand's security in areas such as counter-

terrorism. The procedures for providing such assistance were carefully spelled out in GCSB's internal guidance, and compliance with that guidance was monitored.

25. In the course of this review, a question arose about whether these long-standing interpretations of the law were correct. The Inspector-General of Intelligence and Security had asked the Directors of GCSB and NZSIS the same question at the end of May 2012, and the issue had been the subject of some legal analysis and correspondence, but the matter had not been resolved and in any event assistance to domestic agencies had ceased on 26 September 2012. In October 2012 the Director of GCSB sought an opinion from the Solicitor-General on the question of whether the authority of a NZSIS warrant would override the prohibition in section 14. The Solicitor-General confirmed the difficulties of interpretation and the risk of an adverse outcome if a Court were to consider the question. (I refer to the Solicitor-General's opinion in only general terms since that advice is subject to legal professional privilege and the Attorney-General does not intend to waive that privilege.)

26. It should be noted that all of NZSIS's domestic intelligence warrants are issued jointly by the Minister in Charge of the NZSIS and the Commissioner of Security Warrants, and that it is a function of the Commissioner (who is required to be a former High Court Judge) to advise the Minister in Charge of the NZSIS on applications for domestic intelligence warrants, under section 5A of the New Zealand Security Intelligence Service Act 1969. All of those warrants were also subject to review under section 11(d) of the Inspector-General of Intelligence and Security Act 1996 by successive Inspectors-General of Intelligence and Security, a role that is also required to be held by a former High Court Judge. The Inspector-General of Intelligence and Security and the Commissioner of Security Warrants have recently each been invited to consider the legal issue concerning the effect of section 14 of the GCSB Act 2003 in relation to domestic intelligence warrants. Each has reached a conclusion similar to that of the Solicitor-General. The fact that the issue had not been identified during the preceding ten years (except for the question raised by the Inspector-General of Intelligence and Security in May 2012) reinforces the point that the interplay between the two Acts is not straightforward.

27. The legal reasoning applies by extension to GCSB's assistance to the New Zealand Police on the basis of Police warrants, although that assistance was in practice much rarer.

28. There was a similar outcome in relation to metadata. On review, it appeared that metadata would be likely to constitute a "communication" (as defined in the GCSB Act) for the purposes of section 14.

29. The consequence of these developments is that the lawfulness of some of GCSB's past assistance to domestic agencies is now called into question. In relation to NZSIS, the relevant period is between 1 April 2003, when the GCSB Act came into force, and 26 September 2012, when such assistance ceased. During that period GCSB provided 55 instances of assistance to NZSIS, which potentially involved 85 New Zealand citizens or permanent residents. In relation to the New Zealand Police, the relevant period is between 1 April 2003 and 1 January 2009, because (as already noted) every case of assistance to Police after that date has already been investigated by the Inspector-General of Intelligence and Security and determined to be lawful (with the exception of the case involving Mr Dotcom and his associate). During the relevant period, GCSB provided assistance to the Police in one instance, which potentially involved three New Zealand citizens or permanent residents.

30. It is not known as at the date of this report how many of these instances of assistance might ultimately be determined to have been undertaken in a way that is inconsistent with the GCSB Act, as there are a number of factors to consider in making that kind of determination.

31. Since becoming aware of these issues, the Director of GCSB has:

    a. confirmed that no assistance involving New Zealand citizens or permanent residents, even on the basis of warrants, will resume in the absence of a legislative amendment;

    b. ensured that all cases where GCSB's assistance is now open to question have been identified; and

    c. reported to the Minister Responsible for the GCSB on the matter, so that the Minister can determine the appropriate action to be taken.

32. Other (less significant) legal issues were also considered in parallel to my compliance review, with some interconnection between the two processes. A list of the legal issues considered in the course of this review is attached as Appendix 5, which is legally privileged and classified. Given the need to work carefully through the legal issues, and the complexity of the GCSB operation, the compliance review took longer than expected and my reporting deadline was extended to the end of March 2013.

33. Some legal issues were able to be resolved relatively quickly and the activity reinstated. Some issues required opinions from the Solicitor-General, which have either been provided or are pending.

34. What has also become very clear as a result of this process is that the GCSB Act is not (and probably has never been) completely fit for purpose. Legislative clarification would be highly desirable in a number of important areas where the Act is currently less than clear. That process will provide an opportunity for a public discussion about the powers and functions of GCSB, including the extent to which GCSB should be permitted to assist domestic law enforcement and security agencies, and (if such assistance is supported) under what legal constraints. I recommend that such legislative clarification be sought.

Structure of the report

35. While this report acknowledges the legal issues found at GCSB, those issues are not the focus of the report. This report is concerned primarily with compliance systems and processes.

36. I conclude that the problems concerning compliance at GCSB are symptomatic of broader organisational issues. For this reason, my report is divided into two parts:

    a. the first part assesses GCSB's compliance activity against a standard compliance framework model;

    b. the second part considers what organisational factors may have contributed to GCSB's compliance problems.

Part I: Compliance frameworks

Introduction

37. Legal compliance is an issue for every organisation. The level of effort and engineering that goes into compliance depends on the size and complexity of the organisation, and the type of risks it assumes. At one end of the scale, a one person start-up company may do the minimum to ensure that it complies with the law – for example, paying GST. At the other end of the scale are complex organisations for which the consequences of getting things wrong are disastrous – for example, because errors will result in loss of human life, or critical loss of reputation and public trust. Hospitals come into this category.

38. I would argue that GCSB too is at this high-risk end of the compliance spectrum. Its powerful capabilities and intrusive statutory powers may only be utilised for certain purposes. The necessarily secret nature of its capabilities and activities prevents the sort of transparency that would usually apply to a public sector organisation. It is therefore imperative that the public be able to trust that those exercising the powers are doing so only in the way authorised by Parliament. A robust compliance regime, including visibly demanding external reporting and oversight, should provide considerable assurance to the public.

The standard compliance cycle

39. There is an abundance of literature and case studies available about compliance frameworks and how they apply. Regardless of the type of organisation, robust compliance frameworks tend to include a cycle of activities, as follows:

- **Assessing and identifying compliance obligations:**

  The first step in establishing a robust compliance framework involves assessing the operating and legal environment, identifying the relevant compliance obligations and setting out the compliance objectives.

- **Supporting compliant behaviour and preventing non-compliance:**

  Once the compliance environment has been assessed and identified, the focus should shift to prevention of non-compliant activity. This involves a significant investment, and

includes risk assessment, accessible and authoritative guidance, clear procedures, and training.

- **Monitoring compliance and detecting non-compliance:**

  Preventative systems and procedures are essential, but they will never be sufficient. It is important to be able to detect non-compliance (whether accidental or deliberate) by having internal compliance audits, and external oversight such as inspectors and ombudsmen.

- **Responding to non-compliant activity:**

  Where non-compliance is identified, there needs to be an explicit and escalating internal response that is universally understood and consistently applied within the organisation. The organisation's response should encourage self-reporting of errors, at one end of the scale, and contemplate full disciplinary procedures (including dismissal) at the other.

- **External reporting:**

  Where non-compliant activities have been identified and dealt with, they should be reported to the appropriate external authority and statistics made public. Such external reporting promotes accountability and public trust.

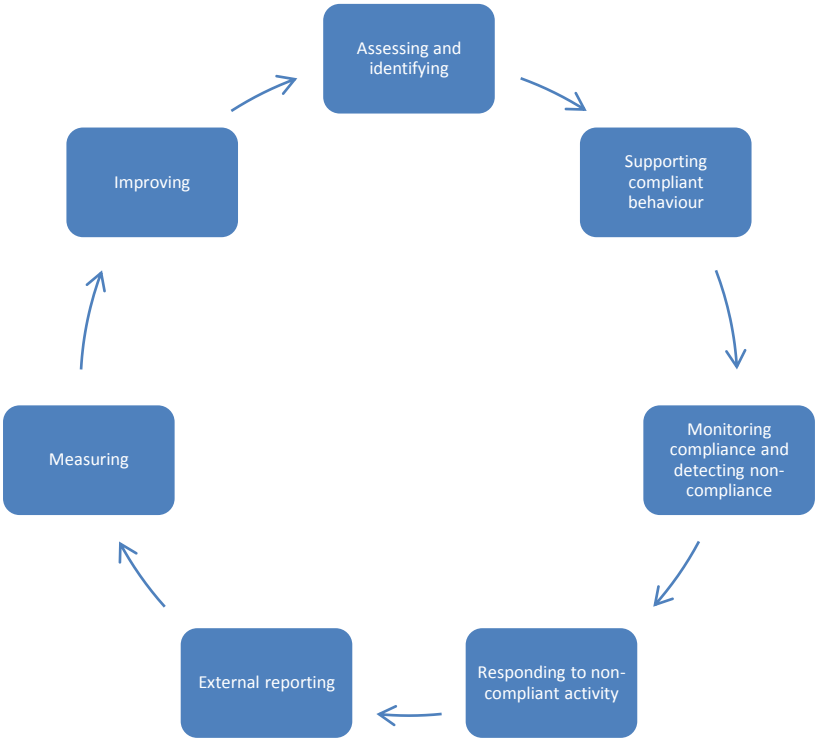
- **Measuring:**

  A robust compliance framework should include a reporting system that allows the organisation's compliance state to be measured against explicit objectives, and trends to be tracked. Information of this kind is invaluable in helping the compliance team (and ultimately the senior leadership team) to understand the compliance health of the organisation, to motivate the organisation to improve, and to promote external accountability and transparency.

- **Improving:**

  An organisation should have a compliance culture of continuous improvement. The compliance systems within the organisation need to be reviewed periodically in the light of compliance performance.

40. Ideally, these features of a compliance framework should operate in a cycle, as follows:



Compliance framework at GCSB

41. GCSB does not have a comprehensive compliance framework of this kind. It does, however, have some features of a compliance framework. This review considers each aspect of a compliance framework as it applies at GCSB, and makes recommendations for improvement where applicable.

42. It is important to note that although GCSB is a complex organisation, it is relatively small. The implementation of these recommendations must not be so heavy-handed and bureaucratic that the organisation cannot function. It must, however, be effective. Organisational structure, governance, systems and culture are all critical to an effective compliance framework, as discussed in Part II of this report.

Recommendations

43. I recommend that:

    a. a comprehensive compliance framework be developed for GCSB;

    b. the compliance framework be peer-reviewed by an external reviewer and implemented.

Assessing and identifying compliance obligations

Best practice: The first step in establishing a robust compliance framework involves assessing the operating environment, identifying the relevant compliance obligations and setting out the compliance objectives.

Assessing and identifying at GCSB

44. I have not seen any evidence of a systematic and ongoing process to identify relevant compliance obligations that apply to GCSB. I found:

    a. **GCSB Act:**

    Throughout GCSB there is a focus on the GCSB Act (as explained and interpreted through internal operational guidance) as the sole source of authority and law. Unfortunately, some aspects of the GCSB Act have recently been found to have been open to question or incorrectly applied since the legislation was enacted, as set out earlier in this report. Where appropriate, those matters have been referred to the Inspector-General of Intelligence and Security. In addition, policy work, led by DPMC, is underway to review unclear aspects of the GCSB Act and to recommend amendment.

    b. **Other legislation:**

    Other legislation relevant to GCSB has not been adequately analysed and considered in relation to its operation (for example, the Defence Act 1990 and the Privacy Act 1993), meaning that the organisation has been exposed to some legal risk; see Appendix 5 for details. These matters are subject to ongoing legal analysis. In addition, I did not find evidence of any system for scanning Bills or legislative amendments on a routine basis to assess the impact of those amendments on GCSB. A process has now been put in place to scan legislative amendments regularly.

    c. **International law:**

    I did not find any collection of relevant international conventions or treaties. In addition, over the years GCSB has entered into a number of Memoranda of Understanding (MOUs) with counterpart organisations overseas on matters of technical assistance, without reference to the Ministry of Foreign Affairs and Trade. These documents were intended by all parties to be non-binding arrangements, but some of them are written using "treaty language", which may give the misleading impression that they are intended to have the force of international law. All documents of

this kind ought to have been discussed with the Legal Division at the Ministry of Foreign Affairs and Trade, to ensure that they had proper oversight, were written in a way that made their status absolutely clear, and followed the right process. Improved practices are now in place.

d. **Jurisprudence and the public law context:**

I have seen no evidence that significant judgments (such as the Supreme Court judgment in Hamed & Ors v. R (2011) NZSC 101) or other developments in the public law domain have been systematically assessed or analysed in terms of their potential impact on GCSB's operation. In addition, it does not seem that the person who was for some years the Bureau's sole legal advisor, the Deputy Director Mission Enablement (DDME), was well connected with the public law community. He was therefore not well placed to keep in touch with legal developments and public law jurisprudence in New Zealand.

e. **Technological developments:**

Technology is changing enormously quickly, with profound impacts on the techniques and tools utilised across the whole of the Bureau. Until recently, the nature of communications media being intercepted at various stages of GCSB's existence (high frequency radio, then microwave via satellite) meant that the communications being targeted for foreign intelligence purposes could mostly be readily distinguished and intercepted. That has largely changed with the technological switch to ubiquitous use of the Internet. The GCSB Act was intended to be technology-neutral and future-proofed, but with the benefit of hindsight it looks to be rather narrowly focused on the SIGINT function as it operated in 2003. Even though the Act is only ten years old, it has not kept pace with developments, especially in relation to information assurance and cyber security. Since 2003, the Bureau has continued to constantly innovate to stay at the cutting edge of technology, which is critical for its success. There does not, however, appear to have been a process for testing how the Act might be applied to new technology at the point that projects are starting. As at the date of this report, the reality is that the Act is difficult to apply to some of the Bureau's current operation or its intended future operation. Essentially the legislation is in need of amendment if GCSB is to continue to be effective.

f. **Connection with the Crown Law Office:**

The Crown Law Office provides authoritative legal advice for the Crown, and it is very important for every public sector organisation to keep well connected with that Office. I was not able to find a collection of Crown Law opinions at GCSB, but the Crown Law Office sent over copies of all opinions they had provided to GCSB since 1988. According to Crown Law's records, 12 opinions were provided between 1988 and September 2012 (24 years), only three of which deal with operational (rather than corporate) matters. In the last six months the Bureau has obtained ten opinions from Crown Law on matters of substantive interpretation, and more are underway.

45. The above findings confirm that there was no systematic effort at GCSB to identify relevant compliance obligations. It is unsurprising in these circumstances that there was no attempt to set out compliance objectives or goals.

Recommendations

46. I recommend that:

a. an exercise be undertaken to assess relevant laws (including common law and international law) relevant to the Bureau and to ensure that current practice is consistent with the law;

b. legal developments (new legislation, legislative amendments, relevant judgments) be systematically scanned to ensure that timely changes can be made at GCSB where necessary to ensure ongoing legal compliance;

c. systems be established to ensure that all technological developments or material changes in practice or operation be assessed to ensure legal compliance;

d. GCSB's in-house counsel be better connected with other public sector lawyers, including the Crown Law Office.

Supporting compliant behaviour and preventing non-compliance

Best practice: Once the compliance environment has been assessed and identified, the focus should shift to prevention of non-compliant activity. This involves a significant investment, and includes risk assessment, authoritative and accessible guidance, clear procedures and training.

Risk assessment at GCSB

47. A good compliance framework will be connected with an organisation's risk assessment framework.

48. GCSB has not always resourced a specific risk management position. Until recently, the Chief Financial Officer (who reported to the DDME) was responsible for risk management (among his other responsibilities). In early 2012 a Risk Management Advisor position was created at GCSB, and after some unavoidable delays the first holder of that position took up the role in September 2012. The Risk Management Advisor – whom, I should emphasise, did not have an opportunity to address these matters before this compliance review started – says that a good risk assessment framework would have identified compliance as a high priority, given the consequences of compliance failure in terms of impact on public trust, and the reputational and financial implications for the organisation.

49. The Bureau also has an Audit Committee, with an external chair. Included in its duties and responsibilities are risk management and internal control. When I arrived at GCSB, I learned that the Audit Committee had not met since June 2010. I understand that GCSB had quite an unsettled period between October 2010 and February 2012, during which time it had a number of Directors and Acting Directors, and I have been advised that this was the reason the Committee did not meet. The current Director decided soon after his appointment that the Committee should be reactivated. This has been done and the Committee, retitled the Risk and Audit Committee, was as at the date of this report scheduled to meet on 25 March 2013.

50. At its June 2010 meeting the Audit Committee considered a document entitled *Internal Audit Plan 2010-12*, which included a proposal to commission a compliance framework from a major consultancy firm at a cost of $15,000. The proposal stated: "The compliance framework … sets out a good practice model, enabling organisations to embed compliance into the business making all employees accountable as it allows for continuous improvement in an ever changing business environment." It is not clear whether the compliance framework, if commissioned and implemented, would have focused on compliance with the GCSB Act. It

is more likely in my view that it would have focused on the full spectrum of legislation that applies to GCSB – e.g. the Public Finance Act 1989, the Official Information Act 1982, the Privacy Act 1993, etc. It does, though, seem likely that a review of this kind would have identified gaps in GCSB's compliance framework, and recommended better systems and processes to manage compliance. The proposal, however, was not proceeded with, apparently for cost reasons.

Recommendations

51. I recommend that:

    a. legal compliance be included in GCSB's risk framework;

    b. the Risk and Audit Committee (which has now resumed) continue to be convened regularly;

    c. legal compliance be included in the regular reporting to the Risk and Audit Committee.

Availability of authoritative guidance and compliance tools at GCSB

52. In any robust compliance regime there needs to be ready access to relevant legal and procedural advice, and information tools that make compliance easier to achieve. What is needed will be different depending on the various positions and roles.

53. At GCSB I found:

    a. **Legal advice:**

    I expected, when I arrived at GCSB, to find easily a collection of all relevant Acts and Regulations, judicial decisions, legal commentary, journals and academic articles. I also expected there to be a collection of legal opinions (internal or provided by the Crown Law Office), kept in a centralised repository and cross-indexed. Even with the assistance of GCSB's IT and Registry staff, and other staff who had worked closely with the DDME, I could not locate this information. The lack of an accessible, centralised and comprehensive repository of legal advice created a risk for the organisation in terms of institutional knowledge, which came to fruition when the DDME went on leave in September 2012 and later resigned. The legal advisors who have arrived since October 2012 have worked to create a more accessible centralised repository of authoritative material and legal precedents.

b. **Operational guidance for the SIGINT operation:**

Within GCSB, the compliance focus is very much on the Signals Intelligence (SIGINT) operation, which collects foreign intelligence. Almost the entire compliance effort is focused on that part of the business. New Zealand Signals Intelligence Directive 7 (NZSID7) provides useful compliance advice for those in the SIGINT part of the operation. NZSID7 is well understood and is available online on the internal website. It is considered to be completely authoritative and staff rely upon it (much more than the GCSB Act, which is not commonly referred to) to ensure legal compliance in their daily work. GCSB's Compliance Advisor is well versed in NZSID7 and available to provide advice on its interpretation. Unfortunately the version of NZSID7 that was in force when I arrived incorporated some assumptions and interpretations of the GCSB Act that have since been found to be incorrect or at the very least open to serious doubt (see paragraphs 22 to 31 above). NZSID7 has since been reviewed and amended to reflect the legal advice received since the end of September 2012.

c. **Operational guidance for the rest of the Bureau:**

Parts of the organisation other than SIGINT often do not have the benefit of compliance advice that is specific to their work (unless they are required to access SIGINT tools and databases, in which case they will comply with NZSID7). For example, it is part of the information assurance function to provide expert technical assistance, in certain circumstances and on request, where a government department network appears to have been compromised. In such a situation GCSB responds to a request for assistance from the relevant agency, and provides highly valued expertise. In addition to the legal issues raised at the start of this report, the forensic work that is required may raise privacy issues. I note that there are MOUs between GCSB and the agencies that use GCSB's information assurance services, which oblige GCSB to take all reasonable steps both to protect departmental information and to safeguard the privacy of individual network users in compliance with the Privacy Act 1993. Staff undertaking this assurance work are acutely aware of the privacy issues, and do take steps to avoid unnecessarily accessing personal information where they can. The practical guidance they have to follow, however, is limited, which in my view is unsatisfactory.

d. **Precedents, examples and frequently asked questions:**

A universal theme throughout my discussions with the staff of the Bureau was an express wish for a centralised and authoritative collection of compliance precedents, examples and frequently asked questions. At the moment, information of this sort is scattered throughout the Bureau; held by individuals in personal email folders, on the intranet, in a SharePoint database, on the internal wiki and the internal blog site. Some units have developed precedents databases of their own, relevant only to their own area of operation. Some rely on institutional knowledge. GCSB's quarterly report to the Inspector-General of Intelligence and Security (IGIS) dated 26 January 2011 notes: "The absence of the Compliance Advisor overseas highlighted the need for a compliance precedents database, where information on previous compliance decisions and points of policy … could be accessed. A rudimentary database was set up in anticipation of SharePoint." Although SharePoint has been introduced, the situation is no better now. The information is not consolidated and much of it is out of date. The recent introduction of an Electronic Document and Records Management System (EDRMS) may assist but it will not be a complete answer. Staff are unclear about whether it is their job to compile such information; they are not confident about how to go about it and find it time-consuming to do. The Compliance Advisor told me that compiling and updating precedents and FAQs is on her work programme but she has not had time to address it.

e. **Consolidated database:**

One further matter was raised with me, which involves classified information. That proposal is discussed at Appendix 6.

Recommendations

54. I recommend that:

a. the legal advisors at GCSB be required to maintain an accessible, centralised repository of authoritative legal material, opinions and legal precedents for reference within the legal team;

b. NZSID7 and other operational advice be reviewed regularly to ensure that it remains current and fit for purpose, as part of the "assessing and identifying" phase of the compliance framework, and be made available to staff in one easily accessed location;

c. operational guidance be developed for the organisation beyond the SIGINT operation;

d. separately from the legal advisors' material, there be a centralised repository of useful operational compliance precedents, examples and frequently asked questions, which is authoritative and kept up to date, searchable and cross-referenced and available electronically in a user-friendly format as a resource for the whole Bureau;

e. staff not be permitted to keep precedents and compliance advice on their personal drives, because it will become out of date; if they receive a particularly useful opinion or piece of compliance advice they be directed to ask the Compliance Advisor or team to include it in the legal and compliance precedents;

f. thought be given to the costs and benefits of a consolidated database, as discussed in classified Appendix 6.

Procedures at GCSB

55. The GCSB operation is very complex. There are very many different activities that need to be regulated. There is a range of ways in which communications are intercepted and authorised for interception, and differences (depending on a number of factors) in the ways SIGINT is handled, stored, accessed, processed, produced and disseminated. In some cases under the GCSB Act warrants and authorities are required; in other cases GCSB may conduct its activities without such documentary authorisations. There are differences between the protective and intelligence functions. There is considerable operational interconnection with other agencies, and relationships with both public and private sector entities, and with other intelligence agencies within New Zealand and beyond New Zealand. All of these relationships and factors lead to an extremely complicated compliance landscape.

56. There are some areas of strength in the current systems and processes. Systems and processes tend to be stronger in the Intelligence Directorate, possibly because the more invasive powers of the Bureau (as opposed to the protective functions) have always been recognised as needing careful regulation. Additionally, it seems that GCSB's own guidance on the collection and reporting of foreign intelligence as set out in NZSID7 is accessible and clear. (The only problem is, as discussed earlier, that some basic aspects of NZSID7 were based on some interpretations of the Act that are no longer accepted.)

57. I did, however, see considerable evidence of confusion or uncertainty in relation to procedures in different parts of the Bureau. Some examples are:

a. **Requests for information (RFIs) and Requests for assistance (RFAs):**

- At the moment there is not a uniform process by which domestic agencies make RFIs or RFAs to GCSB. A number of people to whom I spoke said that there ought to be one centralised point of contact, perhaps located in the Office of the Director or somewhere central and Bureau-wide.

- RFIs and RFAs arrive in a range of ways, and it was suggested to me that there should be tighter, standardised requirements for the format in which RFIs and RFAs are lodged. The Manager Outreach has been trialling a new RFA template with customer agencies, and this trial is progressing well.

- GCSB has in the past sometimes relied on assurances provided by other agencies regarding key compliance matters. Some staff said to me that they believe that where GCSB is being asked to assist other agencies, it should always satisfy itself on important points of compliance (e.g. citizenship or residency status) based on documentation and evidence, rather than accepting assurances, even if those assurances are in writing. If GCSB obtains direct access to relevant databases as proposed above, that will also reduce the chances of error.

- The converse of having one point of connection within GCSB to deal with the RFIs and RFAs from domestic agencies is that an effort should be made to have a centralised point of contact within those agencies for such requests. Having one Bureau-wide point of contact would help to ensure consistency in terms of the processes followed, understanding of the compliance needs of GCSB, and consistency of process.

- A side benefit of having one centralised point of contact within GCSB for RFIs and RFAs is that it will allow adequate documenting, prioritising and monitoring of those requests. One unit within GCSB has developed a prioritisation matrix, and this matrix could be used as a model to prioritise all requests based on factors such as risk and benefits.

- Whatever RFI/RFA procedures are agreed, they should be applied consistently to all operations, including those that are very sensitive. Accordingly those in charge of the process would ideally have a good understanding of the whole spectrum of GCSB's business, as well as being very experienced and be able to exercise excellent judgement.

b. **Fewer assumptions, more evidence:**

It is an inherent aspect of intelligence work that one does not always have perfect information. That does not, however, mean that one is entitled to make assumptions without applying one's mind and judgement to the issue. For example, it will not always be acceptable to assume, just because an entity has a presence in a foreign country and a website with a foreign IP address, that the entity is not incorporated in New Zealand and is therefore a "foreign organisation" for the purposes of the GCSB Act. Similarly, in each case where citizenship or residency is an issue, and very little information is held about the individual, a process must be followed to answer that question which takes account of the context. It will depend on the circumstances. Judgement must be applied. Evidence should be provided wherever possible. Similarly, in relation to agents of a foreign power (the only case where New Zealand citizens' communications can be intercepted under the GCSB Act), thought needs to be given and documentary evidence provided.

c. **Broadening the compliance focus beyond nationality:**

The predominant focus of compliance on the intelligence side is in avoiding the interception of communications of New Zealanders. This concern is very deeply embedded in the culture of the organisation. There are, though, other requirements relevant to legal compliance under the GCSB Act. For example, by law foreign intelligence must be gathered in accordance with the foreign intelligence requirements. Those requirements should be properly considered and documented either electronically or on paper. It is not sufficient to copy the text of foreign intelligence requirement justifications. The system should require analysts to address their minds to this point in free text.

d. **Broadening the focus beyond SIGINT:**

While on the SIGINT side there are documented processes and systems, such is not always the case for other parts of the organisation. Staff members in GEOINT, for example, were not entirely clear about which guidance they should be following (NZSID7, adapted as required, or the operational policies of the New Zealand Defence Force). In parts of the Information Assurance Directorate (IA) there is a similar story. Some staff (for example, those involved in technical assurance of classified systems and those working with communications security equipment) have clear procedures, although sometimes their guidance is out of date. In parts of IA that have developed rapidly in recent years, such as cyber defence, there is less certainty. Staff said to me that written procedures are very incomplete. Enquiries come in from a range of organisations and are not logged or systematically coordinated or prioritised. I was told that the role of the National Cyber Security Centre (NCSC) does not seem to have made the process more systematic, and in some ways appears to have added to the difficulties. Work is underway to address these issues.

58. Before concluding this part of the report, I would like to reflect on some comments made to me by the Australian Inspector-General of Intelligence and Security when I visited Canberra. She told me that the best agencies have systems and processes or forms that require analysts to explain in their own words how they are complying with the law; they must verbalise their reasoning, and not just tick boxes. She commented that this model is very useful for training junior staff coming through the system, because they see what the thinking is behind decisions. It also helps the Australian Inspector-General, because it explains and often justifies the step that has been taken. Such processes and systems protect the agencies. If there is evidence on the systems that demonstrate that staff put their minds to an issue then they are less likely to be criticised by the Australian Inspector-General.

Recommendations

59. The range of system and process issues that I encountered at GCSB will take some time to address and should be part of a wider compliance reform process. It would be useful for the team that takes the reform project forward to consider the approach to systems and processes in similar jurisdictions.

60. I recommend that:

    a. the process for coordinating all RFIs and RFAs across the Bureau (including Information Assurance, all aspects of SIGINT, etc) be standardised, centralised and triaged through a centralised point of contact at the Bureau;

    b. processes be systematically reviewed and be made more robust, by requiring more evidence, more research, fewer assumptions, and more judgement;

    c. more use be made of free text boxes on database systems to explain thinking and reasoning;

    d. further research be done in other similar jurisdictions to see what other lessons can be applied in New Zealand with regard to processes and procedures, to support compliance while still enabling an efficient operation.

Training at GCSB

61. All new SIGINT analysts undergo training when they first arrive at the Bureau. There is an induction programme and compliance training is part of it. Training is delivered through the Compliance Advisor, but it is also provided quite carefully and systematically through close supervision of junior analysts by experienced analysts, team leaders and managers. Learning and understanding the compliance regime is complemented through experiential learning.

62. The Compliance Advisor has the job of providing formal training for intelligence analysts. She provides a 40 minute power point presentation. It is compulsory for new staff and is available as a voluntary refresher for existing staff. Those interviewed said that they found the training briefings helpful, and particularly valued the opportunity to ask questions.

63. Nobody is permitted to access SIGINT material without sitting and passing a compliance exam. Those accessing SIGINT material must take the exam every two years. The exam is provided online, and comprises a random selection of compliance questions. Out of a possible 41 questions, those sitting in the exam are required to answer 20 questions, of which they must answer 16 (80%) correctly. This exam was established in August 2011. It is maintained and administered by the Compliance Advisor. She amends the questions, and changes or adds to them as required.

64. It is reassuring that GCSB has provided briefings, training and testing for its intelligence staff over the years. I do, though, question whether a 40 minute briefing is adequate to give sufficient depth of knowledge and understanding. I note in this regard that the equivalent organisation in Australia, the Defence Signals Directorate (DSD), provides a two day course for its new staff. The training at the Government Communications Headquarters in the United Kingdom (GCHQ) is also much more extensive. Secondly, I note that only those staff that are accessing SIGINT material are required to sit the exam every two years. Managers and unit leaders of SIGINT analysts who are not themselves accessing SIGINT material are not required to complete the exam. My concern about this situation is that those who are supervising are not having their own knowledge refreshed and retested. I also question whether an exam every two years is sufficient.

65. Although SIGINT training is available for GEOINT or Information Assurance staff, it has never been part of the Compliance Advisor role to provide training that is designed specifically for them. It would be desirable for this gap in training to be filled.

66. Some staff suggested to me that the SIGINT exam could be made more demanding. Compliance testing is a fundamental aspect of all counterpart organisations, including Australia and the United Kingdom, which I visited in the course of this review. The research that I have undertaken demonstrates that training and testing is a more thorough and comprehensive process in some other jurisdictions. In addition, I understand that the Compliance Advisor relies on the analysts to notify her when they have successfully completed the test; she does not necessarily check the tests herself. In some other jurisdictions, failing three times constitutes a compliance breach and means that SIGINT data access ceases. That policy also applies at GCSB, but it relies on self-reporting.

67. There are some other ideas that might be considered in the New Zealand context, which came out of my meetings with counterpart organisations in Australia and the United Kingdom:

    a. dedicate part of the compliance resource to compliance training;

    b. have the legal team deliver training of some kind on a regular basis, as an effective way of establishing links between the business and the lawyers;

c. have a structured programme of training, including both face-to-face training for forums where questions and discussion are necessary, and e-learning where appropriate;

d. have a system whereby when a person finishes the e-training, it automatically populates the database of people who have completed the training, with the database being available to all who need that information.

Recommendations

68. I recommend that:

a. a comprehensive programme of compliance training be developed and provided for all operational staff across the Bureau (including SIGINT, Information Assurance, and cyber defence), including both face-to-face training and e-learning where appropriate;

b. all operational staff be required to sit and pass an annual compliance exam (including supervisors and managers);

c. the existing SIGINT exam be reviewed, and compliance testing be developed for other areas of operation;

d. part of the compliance resource be dedicated to training;

e. an active programme be considered, whereby the legal team delivers training and seminars.

Monitoring compliance and detecting non-compliance

Best practice: Preventative systems and procedures are essential, but they will never be sufficient. It is important to be able to detect non-compliance (whether accidental or deliberate) by having internal compliance audits, and external oversight such as inspectors and ombudsmen.

Internal operational audit at GCSB

69. There are some internal operational audit procedures at GCSB. Like so much compliance activity, however, the audit procedures are focused on the SIGINT part of the business. NZSID7 advises that audit for nationality rules compliance may be undertaken at any time by GCSB or by the Inspector-General of Intelligence and Security. The guidance also requires that any contravention is to be recorded and drawn to the attention of the GCSB Legal Advisor (at the time this review commenced,

the DDME). The GCSB Legal Advisor is responsible for ensuring that all such records, together with details of the corrective action taken, are brought to the attention of the Inspector-General of Intelligence and Security in the form of a quarterly report (see paragraphs 110 – 113).

70. More detailed guidance on the auditing of SIGINT activity is provided in Policy Procedure 2001, entitled *Database Access and Auditing Procedures*, which was promulgated on 31 May 2011. There is not a good awareness of this policy at GCSB. Despite the fact that I asked questions about audit procedures as a standard part of all of the interviews, nobody mentioned Policy Procedure 2001 to me. The Compliance Advisor was not aware of it even though it sets out requirements relevant to her role. I only located a copy of Policy Procedure 2001 some five months into this review after I saw a reference to it in some documentation and obtained it from GCSB's Policy Advisor.

71. Before I discuss further the issue of auditing of SIGINT activity, I should note that there is very close supervision of intelligence analysts. An analyst cannot take any action for the purpose of communications interception or foreign intelligence production without the approval of the analyst's team leader. This supervision means that inconsistencies and non-compliant activities should be resolved at an early point. It also means that it is difficult for an analyst to cover up a mistake. Supervision is, of course, different from audit, but it is relevant context.

72. In addition to this close supervision, there are automated audit functions built into some SIGINT tools, whereby auditors within relevant units are prompted daily to audit at least 10% of activity and required to note on the system that they have done so, indicating where further investigation is needed.

73. Detailed information about this internal audit process includes classified information about operational procedures, and accordingly is attached at Appendix 7.

74. The internal SIGINT audit regime is a good initiative, but there are a number of shortcomings with it:

    a. The automated daily audit process is not particularly deep. As required by NZSID7, audit is focused on nationality, but the information provided does not allow an auditor to understand whether a judgement has been made about nationality, and if so on what basis. Furthermore, the process does not allow an auditor to review the foreign intelligence requirement that is relevant to the query.

b. Several team leaders told me that they did not undertake any audits even though they knew they should; one said that she had received no training and did not know what to do.

c. Formal training is not available to auditors. A number of people (including the Compliance Advisor) told me they were not completely clear about the requirements.

d. Staff are not clear about whose responsibility it is to administer the SIGINT audit regime. Policy Procedure 2001 sets out audit responsibilities, including the responsibilities of the Compliance Advisor. The Compliance Advisor, however, has had little to do with audit, and the responsibilities set out in Policy Procedure 2001 have not been included in her job description or performance agreement. The Compliance Advisor told me that she has been too busy with operational queries to undertake second audits as she should (which she described as being ideally every couple of weeks). She told me there was a six month period early in 2012 where she conducted no second audit at all because she was too busy with day-to-day advice.

e. Under the current regime, auditors are auditing their own teams. I have seen no evidence that those conducting the audits are less than rigorous in reviewing the queries. Nonetheless there would be more assurance if analysts were audited by auditors from another team.

f. The audit regime does not currently extend to other databases.

75. More fundamentally, there is no internal audit function at all for many of the intelligence functions, or for the information assurance functions.

76. I am aware that internal audit can be very resource-intensive. I see it as part of an overall compliance regime, so it does not have to be over-engineered. I think if there is sufficient supervision and effective external oversight, comprehensive internal audits would not be necessary. The Bureau's activities should instead be reviewed periodically by the compliance team, so that internal audit can be targeted where it will add the most value. In some cases, it will be appropriate for regular internal audit to be ongoing. In others, occasional spot audits of areas of particular risk or significance may be appropriate. This regime should be sufficient, so long as the auditing is properly administered, monitored and documented.

Recommendations

77. I recommend that:

    a. the compliance team have overall responsibility for the operational audit regime across the whole of the Bureau (including SIGINT, information assurance and cyber defence), with responsibility for the actual conduct of the audits (whether managers or compliance advisers) to be determined;

    b. the Bureau's operational activities be reviewed periodically by the compliance team, so that internal audit can be targeted where it will add the most value (as assessed during the identification phase of the compliance cycle);

    c. spot audits look fully at an operational activity to assess all significant areas of compliance, including judgements, reasoning and documented evidence;

    d. thought be given to whether there should be a policy against auditors auditing their own teams;

    e. training be provided to auditors;

    f. auditors themselves be spot-audited;

    g. audit responsibilities be reflected in job descriptions and individual performance agreements, as appropriate;

    h. the internal guidance be updated, reissued and made accessible to staff who need it;

    i. the results of such internal audit be reported to the IGIS as part of GCSB's regular reporting.

The overall oversight regime at GCSB

78. The external oversight of intelligence agencies is essential to provide assurance to the public that the intrusive powers of the organisations are being exercised lawfully and with respect to the privacy of citizens.

79. GCSB is a public service department and, like other departments, is responsible to its Minister and subject to scrutiny and oversight from Parliament. It is also subject to review or investigation by the Office of the Controller and Auditor-General, and on some matters the Offices of the Ombudsmen and the Privacy Commissioner.

80. Because GCSB's activities include the collection and dissemination of foreign intelligence, however, the oversight regime that applies to it has some constraints and some additional strengthening. In terms of constraints, there are, for example, limits on the information that may be made public – as reflected in the Intelligence and Security Committee Act 1996 and the Public Finance Act 1989. In terms of additional strengthening, there is an Inspector-General of Intelligence and Security (IGIS), appointed under statute, who provides oversight that is additional to the usual public sector accountability mechanisms.

81. Each of these oversight mechanisms has a different focus and function, as follows:

a. **Minister Responsible for the GCSB:**

The Director is responsible to the portfolio Minister for carrying out the functions and duties of the department, tendering advice to the Minister (and other Ministers as required), for the general conduct of the department and the efficient, effective and economical management of the department. The Director is responsible for the day-to-day operations of the department, and the Minister is entitled to expect that those day-to-day operations are being conducted lawfully.

The Minister decides the direction and priorities of the department, but is not involved in the day-to-day operations of the department. In the case of GCSB, section 8(3) of the GCSB Act 2003 states: "The performance of the Bureau's functions is subject to the control of the Minister." This provision makes it clear that there is no question of the Director asserting something akin to constabulary independence. The Minister must also authorise certain activities. As with all Ministers, the Minister is accountable to the House for ensuring the proper conduct of the department, including, for example answering parliamentary questions when errors are made – regardless of whether the Minister has knowledge of the actions giving rise to the errors.

b. **Intelligence and Security Committee:**

The Intelligence and Security Committee (ISC) is a parliamentary committee established and governed by its own statute (the Intelligence and Security Committee Act 1996). The functions of the ISC include examining the policy, administration and expenditure of each intelligence and security agency, scrutinising bills, considering annual reports, and considering other matters referred to the ISC.

The functions of the ISC do not include inquiring into matters that are within the jurisdiction of the IGIS, sensitive operational matters (as defined by the Act), or complaints by individuals that can be resolved elsewhere.

c. **Inspector-General of Intelligence and Security:**

The IGIS is appointed under the Inspector-General of Intelligence and Security Act 1996, the express purpose of which is to increase the level of oversight and review of intelligence and security agencies (including GCSB). The IGIS Act provides that the functions of the IGIS include, among other things:

- inquiring (whether at his or her own motion, or at the request of the Minister) into any matter that relates to the compliance by an intelligence and security agency with the law of New Zealand;
- inquiring into any complaint by a New Zealand person (or a current or former agency employee) that that person has or may have been adversely affected by acts, omissions, practices, policies or procedures, or the propriety of particular activities of an agency;
- carrying out programmes to review the effectiveness and appropriateness of procedures relating to the issue and execution of interception warrants and computer access authorisations.

d. **Other oversight bodies:**

GCSB is subject to oversight by the Controller and Auditor-General, and is also subject to the Official Information Act 1982, the Ombudsmen Act 1975 and the Privacy Act 1993 – although complaints under the last two statutes may be referred to the IGIS if they fall within the IGIS's jurisdiction. Referral to the IGIS would not be appropriate for a complaint relating to the Official Information Act, but would, for example, be appropriate for matters of legal non-compliance, or for matters that have an adverse effect on individuals.

82. The focus of my review is on GCSB's legal compliance at the operational level, and accordingly this report focuses on the external oversight role of the IGIS.

The Inspector-General of Intelligence and Security at GCSB

83. As with many matters at GCSB, I found it difficult to find documents explaining or describing how the relationship between GCSB and the IGIS works at an operational or practical level. I reviewed all of GCSB's files relating to the IGIS. There are only three, covering the years 1996 to 2013. Although they are legal files, they contain no correspondence between the legal advisor and the IGIS, nor any file notes of meetings. They contain formal reports from the IGIS (annual reports and reports resulting from inquiries or in response to complaints).

84. I did, however, speak with the current IGIS, and with staff at GCSB who had interacted with the IGIS. I understand from these discussions and my review of the files that, consistent with the current statutory model, the long-standing pattern of interaction is that successive Inspectors-General:

    a. have operated on their own rather than managing an office of staff; they have not had much (if anything) in the way of permanent administrative, communications or legal support, although since 2004 they have had funding available to obtain such support through the Ministry of Justice, which is responsible for the support of the IGIS [POL Min (04) 12/1];

    b. have employed experts and sought outside legal advice on an "as required" basis (mostly in relation to the NZSIS);

    c. have focused on the SIGINT side of the GCSB operation, and in particular have considered technical issues concerning the issuing of interception warrants and computer access authorisations;

    d. have visited the Bureau's premises approximately quarterly to review documentation;

    e. have spoken mostly with the former DDME, and sometimes with the Compliance Advisor and other staff members directly involved in the issuing of warrants and authorisations;

    f. consistent with section 11(4) of the IGIS Act, have not looked at source information such as databases, or observed staff at work;

    g. have given their views, when asked, on the application of the GCSB Act in particular operational contexts;

    h. have, on occasion, undertaken substantive inquiries into the conduct of GCSB's business and reported publicly on the outcomes;

i. have raised legal issues from time to time and asked for explanations – including several issues listed in Appendix 5;

j. have received from GCSB periodic reports setting out matters relating to compliance, and identifying any non-compliant activity. (I understand that the DDME initiated these reports. They were focused on foreign intelligence collection and reporting rather than being Bureau-wide. Despite being described as "quarterly reports" they were produced at intervals ranging from two months to 18 months.)

85. For some years, it appears that Inspectors-General were reactive; they did not tend to initiate their own inquiries or audits, but waited for complaints to which to respond. Similarly, they equated a lack of complaints with compliance (for example, the 1999 IGIS annual report says: "The fact that there are very few complaints and little need for any inquiry into the activities of the … GCSB indicates, I believe, that the performance of their activities does not impinge adversely on New Zealand citizens").

86. The current Inspector-General has always been assiduous in inspecting all of GCSB's formal documentation and responding to complaints. He recognised about five years ago, however, that reliance solely on complaints provides a low level of oversight of intelligence and security agencies. He observed that a prerequisite of a complaint is knowledge of what is happening or may have happened. In 2007, after the resolution of the *Zaoui* case, he was able to turn his attention to GCSB. He proposed a proactive review programme comprising regular checking of compliance with various statutory requirements, and obtained approval for it in 2008 and annually thereafter. Following the introduction of the work programme, the Inspector-General received some operational briefings, reviewed GCSB's internal guidance and recommended a number of improvements – for example on the level of detail in ministerial authorisations, and the practice regarding requests for assistance and agents of a foreign power.

87. The current IGIS also suggested to GCSB in late 2010 that it would be a good idea for the Office of the IGIS to have a website; this suggestion was not acted upon, but it is not clear why not.

88. These initiatives and ideas were all constructive. In my view, though, the current New Zealand oversight model could be strengthened further to ensure a really robust level of external oversight.

89. An alternative model for the IGIS can be found in Australia. I had the opportunity to learn about that office during a visit to Canberra in December 2012.

90. Many features of the office are the same in the two jurisdictions. For example, they both:

    a. are politically independent;

    b. have the powers of a standing Commission of Inquiry (although the Australian model has more powers);

    c. have "own motion" powers;

    d. may, under their governing statutes, consider both legality and propriety;

    e. report to the Minister.

91. There are also some differences:

    a. It is not a requirement in Australia that the IGIS be a retired Judge. The current IGIS in Canberra is a former Ombudsman, who is very familiar with the daily operation of organisations and the importance of good administration, systems and processes.

    b. The Australian IGIS is clear that determining the law for DSD is not her job; that is the job of the Australian equivalent of the Crown Law Office.

    c. The Australian IGIS has an organisational focus (reflecting her view that a well managed organisation is a compliant organisation), and will point out where poor administrative or information management practices are placing the organisation at risk.

    d. The Australian IGIS has both structured and unstructured engagement with DSD. She meets the Director every two months, and has telephone calls with him in between.

    e. The Office of the IGIS in Australia has 12 staff, including former intelligence community employees (who provide useful institutional knowledge), a legal advisor, review staff and three administrators. Taking into account the difference in the size of the organisations for which she is responsible, there remains a difference in resource. More resource allows a much more active engagement with the agencies.

f. The staff of the Office of the IGIS in Australia have a very regular audit programme, meeting DSD's compliance team monthly, and accessing a considerable amount of agency information. They visit DSD every week or two to review processes and information. They also conduct team reviews, which are ad hoc and very important. These reviews might, for example, look at a snapshot of what the team has done over the last three months and review the activity for compliance.

g. The Office of the IGIS in Australia has a website and most of the IGIS's reports are published (redacted where necessary).

h. The Australian IGIS also reports on the positives, and although she does not speak to the media she will speak about her work in public speeches in appropriate forums.

92. The overwhelming impression one gets about the Office of the IGIS in Australia is that it is very muscular. All parties to whom I spoke described it consistently as robust and assertive. Agencies reported to me that they were proactive and cooperative in their dealings with the IGIS's office. It was obvious that the agencies all saw how important the oversight was for the maintenance of public trust, and that they saw the need for proactive openness and transparency with the IGIS's Office as a vital investment to maintain that public trust.

93. In my view, incorporating elements of the Australian IGIS model would provide strengthened oversight of GCSB, which would be positive for the Bureau and welcomed by the New Zealand public.

94. I should add that these comments should not be seen as reflecting on the IGIS's relationship with the NZSIS. I understand from the IGIS and from the NZSIS that a lot of the IGIS's time and effort is taken up with the NZSIS, which has always been more time-consuming because it has a significantly higher number of formal authorisations requiring review and its focus on New Zealanders. NZSIS finds its engagement with the IGIS to be robust and meaningful.

Determination of legal issues

95. One matter has arisen in the course of this review, which could be helpfully resolved if the Office of the IGIS were reformed and strengthened. That matter relates to the determination of the law as it applies to GCSB.

96. The Cabinet Directions for the Conduct of Crown Legal Business 2012 state:

"The Law Officers, the Attorney-General and the Solicitor-General, have constitutional responsibility for determining the Crown's view of what the law is …"

97. GCSB, as a public service department, is bound by that position and must apply the law as determined by the Solicitor-General.

98. As noted elsewhere in this report, in the past the DDME did not often seek advice from Crown Law. He was more inclined to discuss legal issues with the IGIS. The IGIS, for his part, was happy to provide his views on the application of the law to GCSB.

99. The fact that the Solicitor-General and the Inspector-General might reach different views on the interpretation and application of the GCSB Act potentially puts GCSB in a difficult position. I think a better solution would be for GCSB to seek opinions where necessary from the Crown Law Office (rather than the IGIS) in relation to legal issues concerning its operational activities. GCSB could share those opinions with the IGIS. The IGIS would, however, continue to conduct inquiries and to deal with complaints, applying the law in those matters as he or she sees fit. This kind of approach would seem consistent with other oversight agencies such as the Office of the Ombudsmen.

100. It would be useful to clarify the roles of the respective institutions in relation to the provision of legal advice, whether through discussions with the various institutions or through legislative clarification.

Other external oversight matters

101. In order to provide greater assurance to the ISC and the public, GCSB could do more to report externally on statistics concerning compliance and compliance trends. When GCSB has implemented a compliance framework, this information could be included in GCSB's Annual Report and could also be reported to the ISC, thus strengthening that Committee's ability to ask questions of the Director regarding organisational performance and improvement. I make recommendations in this regard in the section of this report regarding external reporting.

102. It was noted to me during the course of this review that, when compliance systems and oversight are tightened, it is likely that the reported incidence of non-compliance will increase initially. That is not to be seen as a negative sign, but rather that the system is working.

Recommendations

103. I recommend that policy work be undertaken with a view to strengthening the Office of the IGIS in New Zealand, including:

    a. broadening the pool of candidates for the position, by considering whether it is necessary for the IGIS to be a retired Judge, or whether independence and the ability to conduct the inquiry functions might also be found in very experienced and senior public servants and administrators;

    b. increasing the resources and staff supporting the IGIS;

    c. considering what other aspects of the Australian legislative model might translate well into the New Zealand context;

    d. making the work programme, audits and reporting expectations more explicit;

    e. much more regular visits to GCSB, access to all information, team reviews, and spot audits;

    f. continuing the existing self-reporting by GCSB to the IGIS via more timely quarterly reports;

    g. clarifying the relationship between GCSB, the IGIS and the Crown Law Office, in relation to legal advice;

    h. establishing a website for the Office of the IGIS.

Responding to non-compliant activity

Best practice: Where non-compliance is identified, there needs to be an explicit and escalating internal response that is universally understood and consistently applied within the organisation. The organisation's response should encourage self-reporting of errors, at one end of the scale, and contemplate full disciplinary procedures (including dismissal) at the other.

Responding to non-compliant activity at GCSB

104. In the course of the review I asked GCSB staff how compliance errors are identified and how non-compliance activity is dealt with. Again, there is no written guidance on this point. However, the SIGINT analysts I spoke to were quite clear about the process that would be followed.

105. As I say elsewhere in this report, GCSB employees are deeply indoctrinated so as not to intercept the communications of New

Zealanders except in very limited authorised circumstances. Nonetheless, as with all human activity, occasionally mistakes are made. For example, a number might be copied incorrectly. Given that analysts often do not have perfect information about targets, it is not always possible to exclude the possibility that a target may have New Zealand citizenship (for example if the target has a common foreign surname and the analyst does not have a date of birth). Additional information may be learned about citizenship in the course of an operation – perhaps that a target has dual citizenship.

106. In circumstances such as these, the error must be reported. While the process is only partially documented (in Policy Procedure 2001), I was advised that the following process would occur once an error has been detected:

    a. the analyst will inform the team leader;

    b. the analyst and the team leader will talk to the Compliance Advisor;

    c. the matter will possibly be then escalated to the Manager Outreach or the DDME, depending on the nature and seriousness or the error;

    d. the collection will cease immediately;

    e. if there has been any reporting, that will be cancelled immediately;

    f. the information concerning the target will be deleted within GCSB if it has not already "aged off" the system;

    g. if any information on the target has been provided to an agency outside the Bureau, a request will be made for the information to be purged;

    h. the team leader will send the Compliance Advisor a reporting email telling her exactly what happened, what has been done to fix it, and how to ensure that it does not happen again;

    i. the error will be included in the quarterly report to the IGIS.

107. The goal is to encourage analysts to self-report. Accordingly, minor, inadvertent errors are not punished. Errors of that kind would result in the analyst being spoken to, and being required to undertake further briefings or remedial training as required. A deliberate breach of the Act or wilful failure to comply with NZSID7 must be reported to the Director and the staff member will face disciplinary action.

108. I think GCSB's approach to incidents of non-compliance seems appropriate, graduated and proportionate. The procedures should, however, be fully explicit and transparent, and Bureau-wide.

Recommendations

109. I recommend that:

a. procedures in the event of non-compliance be developed for all staff for whom compliance is an issue;

b. procedures in the event of non-compliance be made explicit in writing for staff.

External reporting

Best practice: Where non-compliant activities have been identified and dealt with, they should be reported to the appropriate external authority and statistics made public. Such external reporting promotes accountability and public trust.

External reporting at GCSB

110. At the moment there is some limited collating of compliance information and reporting. I have been told that GCSB is required to provide quarterly reports to the IGIS that disclose and address all compliance matters and breaches that have occurred during the reporting period. This requirement is referred to in Policy Procedure 2001 although the practice predates that guidance. Policy Procedure 2001 states that quarterly reporting is part of the Compliance Advisor's responsibilities, but it is not reflected in the Compliance Advisor's job description or Individual Performance Agreement.

111. I have reviewed the file containing the quarterly reports to the IGIS since their inception. As mentioned above, the reports have not always been provided on a quarterly basis. When I arrived at the Bureau, I found that no report had been provided since the end of May 2011. I was advised by the Compliance Advisor that the pressure of providing day-to-day advice had meant that there was no time to complete them. Since the commencement of this review, the Compliance Advisor has provided a report detailing compliance matters, which covers the period 1 June 2011 to 31 December 2012.

112. The Compliance Advisor told me that nobody – including the DDME (her manager) or the IGIS – ever asked where the missing quarterly reports were.

113. The IGIS's reports include information on compliance, based on his visits to the Bureau and the quarterly reports provided by the Compliance Advisor. The IGIS's reports are published annually. They are not, however, available on-line on an official website. It is therefore difficult for the public to find or read the information.

114. Reporting on compliance statistics is not included in GCSB's Annual Report, and nor is it reported to the Intelligence and Security Committee (ISC). It seems unsatisfactory that the ISC receives insufficient statistical information to enable that committee to question the Director of GCSB on whether GCSB is meeting its compliance objectives.

Recommendations

115. I recommend that:

    a. the IGIS's requirements regarding compliance reporting be made explicit and provided in writing;

    b. responsibility for the quarterly reports be clearly allocated within the compliance team, and reflected in the relevant performance agreements;

    c. compliance statistics be reported on in the IGIS report and the GCSB Annual Report, and be made available to the ISC;

    d. the IGIS's reports be made available on an official website (perhaps the GCSB website or the DPMC website until an IGIS website is established).

Measuring

Best practice: A robust compliance framework should include a reporting system that allows the organisation's compliance state to be measured against explicit objectives, and trends to be tracked. Information of this kind is invaluable in helping the compliance team, and ultimately the senior leadership team, to understand the compliance health of the organisation, to motivate the organisation to improve, and to promote external accountability and transparency.

Measuring at GCSB

116. As noted above, an effective compliance framework will include mechanisms for tracking, measuring and reporting information about compliance breaches. Such statistical and qualitative information ensures:

a. accountability to the Inspector-General and the public; and

b. valuable business information to inform system improvement.

117. As I noted under the section about assessment and identification of compliance issues, GCSB has no explicit compliance objectives against which to measure its performance. Neither does it track historical information against which to measure its progress. It does not monitor its compliance statistics at all.

118. Accordingly, the Senior Leadership Board does not have visibility of trends in the compliance area, or business information that would assist in determining where to direct compliance effort.

119. Similarly, external oversight agencies (such as the IGIS and the ISC) do not have information that would be useful in their roles.

Recommendations

120. I recommend that:

a. GCSB develop explicit compliance objectives, collect statistics, assess performance against those statistics, and track historical information;

b. the compliance team be allocated the responsibility to support and monitor this process and report to the Senior Leadership Board;

c. Compliance statistics, assessed against compliance objectives, be provided annually to the IGIS and the ISC, and be included in the GCSB Annual Report.

Improving

Best practice: An organisation should have a compliance culture of continuous systems improvement. The compliance systems within the organisation need to be reviewed periodically in the light of compliance performance information to drive on-going change and improvement. There should be a compliance team work programme that sets out improvement projects as well as day-to-day business.

Improving compliance at GCSB

121. At GCSB:

a. compliance is very much focused on day-to-day advice;

b. there is no evidence of systems being consciously reviewed with an eye to improving compliance;

c. statistical trends are not monitored, which hampers the ability of the organisation to see where problems are arising that might need to be addressed through improved training, guidance and procedures;

d. there is no agreed compliance work programme aimed at improving compliance at GCSB.

Recommendations:

122. I recommend that:

a. the compliance team and senior leaders use monitoring information, together with risk assessment, to focus and prioritise improvement activity;

b. a work programme be developed accordingly;

c. resource be allocated within the compliance team to ensure that there is a conscious and systematic effort (preferably informed by best practice in other operational departments or agencies) to continuously improve systems, training, guidance and procedures.

Part II : Organisational factors that have contributed to GCSB's compliance problems

Introduction

123. The gaps identified in the course of my compliance review have arisen to some extent because of issues within GCSB concerning organisational structure, culture, systems and capabilities. Those issues have contributed to the problems to date, and will continue to be impediments to an effective compliance regime unless they are addressed.

124. I commented at the beginning of this report that compliance issues within GCSB are symptomatic of a broader problem. This part identifies what I see as some of the wider organisational issues, and so has a broader scope than simply compliance matters.

125. It is important to note that the issues identified in this part of the report have evolved over many years.

GCSB's organisational structure

126. GCSB's current structure reflects its history. In particular, it reflects the fact that GCSB is modelled on similar organisations in other, larger jurisdictions. Its structure also reflects its diverse functions. Given GCSB's small size in relative terms, the consequence is that GCSB has ended up with a very complicated structure with many very small units. It struck me as rather extraordinary that in order to gain an understanding of an organisation with fewer than 300 staff, I had to interview 23 separate teams or units and eight individuals; even then I did not speak with every part of the organisation (for example, I did not interview Information Technology (IT), Human Resources (HR) or Registry staff).

127. The reason that I mention the complex nature of GCSB's structure is that it is significant in terms of compliance. The complexity of the operation creates real difficulties for compliance in relation to matters such as information management, guidance and record keeping.

128. In addition, the information assurance function has grown very quickly in recent years because of the growth of cyber attacks emanating from around the world, which are threatening New Zealand's security and prosperity. The organisation has not, however, adjusted to the growth on the Information Assurance side. Some of the roles that should cover the whole organisation, such as the Compliance Advisor or the Manager

Outreach, are in fact solely or mostly focused on the intelligence side of GCSB rather than Information Assurance and cyber security.

129. The organisation is very widely spread and in places very thin. The Deputy Director Mission Enablement (DDME), who was at the time my review commenced responsible for compliance, is the most extreme example of this. At the time I commenced this review, he had approximately 16 direct reports, many of whom had no staff reporting to them. Some of his responsibilities conflicted with one another and inhibited effective internal challenge.

130. It is my view that the organisational structure of GCSB, at a fundamental level, makes compliance a difficult exercise. It may be that the Director and the Senior Leadership Board wish to consider whether a simpler arrangement, with fewer managers, would be more appropriate for an organisation of this size. Perhaps, although it is beyond the remit of this review, different structural models should be considered.

131. The complexity of the organisational structure also means that there is a lack of clarity about which staff deal with exactly which procedural and compliance issues. The Compliance Advisor, the legal advisor (a role held by the DDME in addition to his other responsibilities), the Policy Advisor, the Manager Outreach and the Access Management Centre all have roles to play in compliance, but are located in different parts of the organisation in a way that is not at all coherent. Thought needs to be given into how these different parts of the organisation inter-relate (and in some, but not all cases, combine) to make a much more coordinated compliance capability. In particular, it is my view that compliance advice and operational policy should be combined into a team, placed (at least in the interim) under the aegis of a second tier manager such as the Associate Director, in the centre, and located separately from (although working closely with and freely available to) the legal team and operational directorates. Similarly, as mentioned earlier in this report, consideration should be given to the idea of having one centralised point of contact within the Bureau to deal with all Requests for Information and Requests for Assistance from external agencies.

132. Before moving on from the issue of GCSB's structure, I should add that it would be desirable to clarify the status of GEOINT and the NCSC in relation to the Bureau.

Recommendations:

133. I recommend that:

a. some innovative thought be given to reorganising GCSB in a simpler, less fragmented way that is suitable for its relatively small size but acknowledges the complexity of the business;

b. consideration be given to reducing the number of small units and managers;

c. roles that should really be Bureau-wide (compliance, outreach, etc) be placed centrally within the Bureau and reconfigured;

d. the scope of the Bureau's activities be scrutinised closely and systematically to work out whether capability can be less widely spread, focused more deeply on the things that matter, and that any low priority work be identified and eliminated;

e. effort be made to avoid single points of dependence;

f. compliance advice and operational policy be combined in a team, placed (at least in the interim) under the aegis of a second tier manager such as the Associate Director, located centrally within the Bureau, and located separately from – although working closely with – the legal team and operational staff;

g. roles (e.g. legal advisors, compliance advisors) be configured so as to avoid combining functions that conflict, and to encourage internal challenge;

h. there be one centralised point of contact within the Bureau for all day-to-day engagement with external agencies;

i. the place of NCSC and GEOINT within the Bureau be clarified.

Governance

Internal governance

134. GCSB has standard public sector governance structures. It has a senior leadership team, the name, size and membership of which has changed over the years for various reasons (and which is currently called the Board). That group has met regularly over the years. I was advised by the DDME that from October 2010 a legal and compliance report prepared by the DDME was a standing item on the agenda for all Board meetings.

135. As already mentioned, GCSB has a Risk and Audit Committee, which is able to provide independent scrutiny of matters concerning compliance and risk.

136. I do not consider that the governance structure needs to be changed at GCSB. The challenge, in a heavily operational department, is for the Board to keep focused on the big issues facing GCSB: strategic direction, risk, opportunities, the overall work programme, major projects, the departmental budget, workforce capability and capacity, etc. This review shows that in the past this is unlikely to have been the case.

137. It is likely that more active secretariat support for the Board would assist it to maintain its focus on the high level issues facing GCSB.

ODESC(G)

138. There is also the Officials Committee for Domestic and External Security Co-ordination (Governance), referred to as ODESC(G). The members of ODESC(G) are the Chief Executive of DPMC (Chair), the Secretary to the Treasury, the State Services Commissioner, the Chief of Defence Force, the Commissioner of Police, and the Secretary of Foreign Affairs and Trade. The Directors of GCSB and NZSIS are not members, but attend most meetings.

139. ODESC(G)'s role (as agreed by Cabinet in February 2010) is to focus on systemic governance including performance monitoring, oversight, priority setting and allocation of resources across the New Zealand Intelligence Community (NZIC).

140. ODESC(G)'s focus is on the NZIC as a whole. The Committee provides a mechanism to ensure that there is full and effective co-ordination and co-operation within the NZIC, and that there is no unnecessary overlap of activities or responsibilities. ODESC(G) oversees the management and conduct of New Zealand's international intelligence relationships in respect of the NZIC as a whole.

141. ODESC(G) does not seem an appropriate body to review operational compliance matters at GCSB, although it does have an interest in GCSB's performance more generally. It will, for example, take an interest in the outcome of the Performance Improvement Framework review process, which both GCSB and NZSIS intend to undertake later this year.

Recommendations

142. I recommend that:

    a. GCSB's Board agree on a Board Charter that makes it clear that the Board's focus is strategic direction, risk, opportunities, the overall work programme, major projects, the departmental budget, workforce capability and capacity, etc;

    b. secretariat support be provided for the Board to assist it to achieve this focus.

GCSB's culture

143. As noted at the start of this report, GCSB staff express a strong commitment to comply with the law. All staff that I encountered talked about their work in a way that clearly showed that unlawful activity – whether by error or deliberate act – is abhorrent to them.

144. Those involved in SIGINT operations have for many years faithfully followed the guidance that they believed to be correct. It has been quite devastating for them to learn recently that Crown Law has concluded that NZSID7 is not in all aspects entirely consistent with the law – with consequences for some activities undertaken in reliance on that guidance.

145. I have seen no evidence that GCSB staff believe that the end justifies the means or that they have acted in bad faith. In many ways it appears that they have been let down by aspects of the organisation that they have relied upon. And yet I think there are some aspects of the culture at the Bureau, caused by its special work and isolation, that have allowed the compliance situation described in this report to develop:

    a. organisational emphasis is mostly on the operation and the mission rather than corporate matters and roles;

    b. compliance, while important to staff, has been viewed by some in a rather compartmentalised and procedural way; there has been a bit of a tendency to tick boxes and make assumptions, instead of asking questions, seeking evidence, and applying thoughtful judgement (I note that quite a lot of rigour has been introduced in these areas since the start of my review);

    c. the units are very specialised, which means that staff may not be accustomed to thinking about issues (whether compliance or otherwise) in terms of GCSB as a whole;

d. there is something of a "family culture", in which poor performance tends to be tolerated, and problematic staff are redeployed internally instead of being held accountable;

e. there is an organisational aversion to performance-managing and potentially exiting poor performing staff, partly because of misplaced loyalty, partly because of difficulties associated with disgruntled former employees (who may pose a security risk), and partly because security vetting processes often makes recruitment a very long process. One consequence of this is that considerable funding may be tied up with under- or non-performing staff, which could be freed up;

f. specialised knowledge is sometimes valued at the expense of other important matters such as refreshment and succession planning. The consequence is that some staff stay too long in one job, so that in places blind spots are not addressed, fresh thinking does not occur and there is some (passive) resistance to change;

g. the "need to know" principle has eased considerably in most parts of the organisation, but it still appears in pockets, creating some silos in terms of people, ideas and technology;

h. much of the organisation is isolated and disconnected from most of the regular public service. This disconnection means that GCSB's responsiveness to public sector changes and its adoption of new norms is often very slow. Approaches and frameworks that are mainstream elsewhere have yet to filter through into the Bureau.

146. I understand how these cultural factors have developed, given the very sensitive capabilities and assets at play. Nonetheless, in my view GCSB's isolation from the regular public service is problematic. I note that in the United Kingdom, the CVs of many senior public servants include a stint in one of the intelligence agencies. Such secondments result in a good understanding of intelligence concerns in the general public service community, and an understanding of public service norms within the intelligence community. There is a need in this country to create good connections between people in different parts of the system. That is lacking presently within GCSB, and it matters very much.

Recommendations

147. I recommend that:

a. a concerted effort be made within GCSB to improve performance management practices, to ensure that all roles are regularly refreshed without losing institutional knowledge, and that persistent non-performers who cannot demonstrate improvement are exited (subject to a proper employment process) to allow for fresh recruitment;

b. thought be given to targeted rotations and secondments between the operational and central parts of GCSB (for example, rotating promising analysts through the compliance and policy team as part of their professional development);

c. thought be given to a structured programme of secondments between GCSB and other public service departments, in order to increase knowledge of the NZIC and to increase the Bureau's connection with mainstream public service thinking and developments.

Information management at GCSB

148. An issue identified in Part I of this report, concerning access to authoritative compliance information, is symptomatic of a broader issue at GCSB. That issue concerns the management of information and IT systems, and documentation and record keeping.

149. There are some staff who are designated as Knowledge Service Managers or Knowledge Services Administrators, but those positions relate either to specific projects, or positions in the GCSB Registry. There are no professional information managers despite the fact that the organisation is an information enterprise.

150. In addition, many staff members are highly knowledgeable and sophisticated in their use of information technology for their work. The combination of many IT experts and no professional Information Managers is that there has been a proliferation of very specific databases or other information management (IM) tools developed for different parts of the organisation. Some IM tools are intended to be Bureau-wide and are developed enthusiastically – such as SharePoint – but there is a lack of follow-through so that once the initial enthusiasm has passed, uptake of the tool is patchy and ultimately staff move on to something else.

151. An example of this issue is that GCSB has only in the last few months introduced its first electronic document records management system (EDRMS). It had not previously had a centralised electronic document management system of any kind. Records were kept in hardcopy (and the files maintained by a very effective Registry), but electronic records such as emails were kept in people's personal drives. The introduction of the EDRMS is a very positive step for GCSB, although the transition to it is not yet complete.

152. It is hard to imagine that an organisation would have been able to develop so many databases, and in particular so many purpose-built applications, if there were a professional Information Manager in charge of the information business needs of the Bureau. The status quo must be extremely expensive to maintain. An experienced and professional Information Manager would ensure that:

    a. proper programme methodology is used on IM projects;

    b. all IM projects are justified in terms of business need;

    c. requests for IM solutions are assessed together;

    d. risks are identified and understood;

    e. IM solutions are found for as many people as possible;

    f. IM projects are completed and fully implemented; and

    g. taxpayers' dollars are spent as efficiently as possible.

153. At a more detailed level, staff identified the following problems with information management during my discussions with them:

    a. staff have not yet been required to move all of their information onto the EDRMS, so that data is still being stored in inappropriate places (for example, there are significant volumes of business-related files stored in personal folders and email archives);

    b. there is a large amount of duplication;

    c. information management practices are inconsistent and largely dependent on the unit and the manager (for example, access control and permissions are inconsistently applied);

    d. there is a large amount of information locked down and not shared with those who need it;

e. some staff see the EDRMS as the authoritative record for the Bureau and are filing everything onto it; others are continuing to use paper files for record keeping;

f. staff are able to create their own files in the EDRMS which means that the file plan is very likely to soon become out of control (some staff think it already is);

g. there is no EDRMS on the unclassified system. Accordingly, there is no centralised repository for the electronic records of staff (such as the information assurance staff) who conduct business regularly with external agencies outside the intelligence community.

154. From what I have seen, in the past, when all record keeping was paper-based, there were good systems at GCSB (and the Registry still seems very well organised). The development of electronic systems, websites, and email, however, have presented a huge challenge to GCSB's record keeping. I should add that this is not an issue that is unique to GCSB by any means. All organisations, whether private or public, have grappled with the same challenge.

155. It must be said, however, that an institution that exercises the intrusive powers of the state has a greater obligation than most organisations to keep adequate records of its activities for the purposes of audit and oversight.

156. That has not been my experience at GCSB. There have been many basic documents that I have been unable to find and that others have struggled to find for me. Legal opinions, memoranda of understanding between GCSB and other organisations, Cabinet minutes – these are all basic authorising documents that ought to be kept in an accessible place for those who need to rely upon them.

157. I should add that some parts of GCSB are very thorough in their record keeping. For example, my review of warrants and authorisations revealed a good level of record keeping. The reason is likely to be because these files are reviewed by the Inspector-General on a regular basis. Other parts of the organisation, however, are less clear about their obligations, and use adjectives like "variable" to describe their record-keeping practices. All said that they hoped the EDRMS would assist with centralised filing, and I am sure it will. There are questions, however, about how important business information is recorded and filed, especially considering the classified and unclassified systems, and the plethora of databases and information tools. An Information Manager would help to assess this issue and to address it.

158. I think it is unlikely that GCSB complies fully with the Public Records Act 2005 although the move to the EDRMS is a big step forward. The current situation also presents challenges in terms of meeting statutory obligations relating to the Official Information Act 1982 and the Privacy Act 1993. In my view, in order to support good business practices across the board, including compliance, it is essential that this part of the business be properly supported with the right information management strategy and business disciplines.

159. I note, finally, that the Inspector-General of Intelligence and Security in Australia remarked to me: "record keeping is not just about having an EDRMS. It is about the will to record in a way that can be found and assessed. Very significant problems occur where there is poor record keeping."

Recommendations

160. I recommend that:

a. a professional Information Manager be appointed to review GCSB's business information needs and to rationalise and align the current systems as much as possible;

b. the Information Manager be expressly tasked with rationalising databases and other information management applications in a way that does not impact on the operational work of the Bureau;

c. the Information Manager have the authority to develop and implement an information management strategy with associated guidelines;

d. the Information Manager address the issue of record keeping, as a matter of urgency;

e. all staff should be required to operate in accordance with that information management strategy and those guidelines.

Capability and capacity issues within GCSB

Background

161. As mentioned above, GCSB is an organisation that is spread very thinly. A number of staff expressed the view that the Bureau (in common with all other government agencies, especially following the global financial crisis) faced a consistent challenge over the years in remaining within its

appropriation, with the result that decisions had to be taken to commit funds to the organisation's operational delivery functions at the expense of corporate and support functions such as legal and compliance advice. I agree that there is an issue (both past and present) about how resources are allocated within the Bureau. But I think there have always been choices about how the resources are allocated (i.e. between the operational delivery functions and the support functions) and nobody "had" to make those choices in any particular way. I also think that the underlying organisational issues described in this part of this report, which have not been addressed for many years but are being addressed now, have contributed quite significantly to the resource problem.

162. The result of the resourcing choices made over the years is that there are a number of single points of dependence (for example, legal advice, compliance advice, operational policy, risk management). In some cases important organisational capability is missing altogether (for example, information management).

163. Additionally, it is difficult to bring in short-term expertise (communications, change management, legal peer review) because those with the requisite skills and attributes are unlikely to have an adequate security clearance.

164. There are a number of staff members in the Bureau who have roles with a particular connection with compliance. I will discuss each role in turn.

Legal advice

165. For a number of years there has been only one source of legal advice at GCSB, which was the DDME, a second tier manager. When appointed in 1988 he was a full-time legal advisor, but when he was appointed to the position of Executive Director in 1996 he assumed additional duties, which gradually increased over the years. As at the time this review commenced, in addition to legal advice, the DDME had responsibility for governance and performance, strategy and policy, risk management, the Liaison Officers, the Compliance Advisor, strategic relationships, the Chief Financial Officer, knowledge services, the registry, the Chief Information Officer, technology infrastructure, security (physical, personnel, and IT) and mission capability (IT) development. Until fairly recently he also had responsibility for HR, finance and logistics, procurement and property services. He was for some periods also Acting Director of GCSB.

166. In my interviews and discussions across the whole Bureau, those interviewed told a very consistent story about the provision of legal advice at GCSB, as follows:

a. The DDME was the only GCSB legal advisor, without legal backup, for almost all of the time from his appointment in 1988. Even where legally qualified intelligence analysts were seconded to work with the DDME as lawyers (which happened twice), they were inexperienced and required considerable supervision. The DDME raised the issue of additional legal support at the senior management level on a number of occasions over the years, but no other lawyers were appointed. He was, therefore, a single point of dependence in terms of the provision of legal advice.

b. The DDME had too many hats. His multiple roles meant that there was insufficient internal debate and challenge. He was solely responsible for policy and legislative development, providing drafting instructions, interpreting the resulting law and overseeing its implementation and operation. These were conflicting roles. It is essential in an organisation that exercises intrusive powers of the state that there be robust challenge and the ability for contesting views to be expressed and explored. As the chief architect of the legislation he spoke confidently and authoritatively about the legislation and staff were not in a position to challenge that.

c. It seems unlikely that the DDME had sufficient time to devote to the important task of providing legal advice. His own estimate is that he devoted at the most between 5% and 10% of his time to legal work.

d. It appears that he was not strongly connected with the public service legal community, although he was in regular contact with other lawyers in the intelligence community and did, from time to time, discuss with them legal issues relating to particular operational matters.

e. The DDME's seniority, as a Deputy Director, contributed to reluctance on the part of staff to question his judgement. Staff were unanimous in stating to me that the DDME's view was seen as completely authoritative.

f. There appears to have been little peer review of the DDME's advice from the Crown Law Office, although he did raise some legal issues with the IGIS. I am not sure why more issues do not seem to have been referred to the Crown Law Office for an opinion – especially

considering the matters at stake and the Crown Law Office's role in providing authoritative legal advice to government departments. A contributing factor may have been that no budget was allocated for this kind of advice. In addition, the DDME commented that the culture of the Bureau during his 24 year tenure was to keep its business in classified channels, and this contributed over many years to a reluctance to seek external contact or assistance. Whatever the reason, it meant that some legal advice provided by the DDME has not been supported, on review, by the Crown Law Office. I note in this regard that the Defence Signals Directorate in Canberra (DSD) has its in-house lawyers provided from the Australian Government Solicitor (AGS). The benefit of this arrangement is that there is strong legal oversight that is well connected to experienced public lawyers. In addition over time the AGS has built up a body of cleared expertise. That may not be the best model for GCSB, but in my mind it is imperative that stronger links are developed with the Crown Law Office.

167. The legal advice in GCSB has not been sufficiently documented or, if it has been documented, it is not easily accessible. One of the problems that hampered both this compliance review and the provision of legal advice after the DDME's departure was the fact that we were not able to find any obvious precedent files or any methodical system (either electronic or hardcopy) of recording advice for the purposes of precedent files or audit. What I was told in many discussions with staff in the course of this review is that the DDME regularly gave advice informally, often in emails that were not able to be accessed when he was absent. This may have worked while the DDME was present at GCSB, but it created a very significant risk for the organisation when he was not available – a risk that was fully realised following his departure at the end of September 2012 and subsequent resignation. I note in this regard that I was told at DSD that every piece of compliance and legal advice must be documented, and that there is meticulous record keeping. If an urgent problem is posed orally, and advice is given orally, that advice must later be provided in writing, including the question and facts as understood by the compliance or legal advisor, and recorded centrally. I note, for completeness, that the DDME's perspective on this issue is that better documentation and record keeping would have been desirable, but he simply did not have time to do it.

168. It is beyond the scope of this review to investigate or determine why the role of the DDME evolved the way that it did. Contrasting views were expressed to me on that subject. What is clear is that the position was in need of review and reform. That has now happened.

Compliance Advisor

169. There is only one Compliance Advisor at GCSB (i.e. another single point of dependence). She reported to the DDME until his departure. The Compliance Advisor has no legal training or formal background in compliance.

170. The compliance role at GCSB is filled through an internal process. The Compliance Advisor and one of her predecessors told me that there was little interest by other GCSB staff in the position at the time that they expressed an interest in the role.

171. From the many discussions I had in the course of my review and from the material I have read, I make the following observations:

    a. Compliance Advisors at GCSB have had insufficient training. The current Compliance Advisor told me that she was fortunate to have a week or so of overlap with her predecessor. She received some handover notes which appear to be a list of current areas of work rather than a comprehensive desk file note.

    b. As noted above, there is no accessible record of advice from the Compliance Advisor, and up-to-date compliance precedents and FAQs are not centrally located and accessible.

    c. The scope of the job is unclear, and heavily focused on the SIGINT operation. While the Compliance Advisor herself is clear that her job covers the Information Assurance directorate (IA), the IA staff said that the Compliance Advisor sees GCSB very much through an intelligence lens, which does not always apply to IA. This focus is reinforced by the Compliance Advisor's physical co-location with the SIGINT production analysts at GCSB.

    d. Some important requirements of the Compliance Advisor's job do not seem to be properly documented – for example, audit and quarterly reporting to the Inspector-General.

    e. It is clear that the Compliance Advisor role is seen as something of a backwater. It is not a management position and so relies on influence and cooperation rather than management authority. Senior staff are not attracted to the position because it is not seen as a route for advancing within the organisation.

    f. Given that it is not a management position, the role in my view is too autonomous. The current Compliance Advisor told me that she takes 90% of decisions without reference to the legal advisor, or any

other person in a supervisory capacity. It is important to note that as well as considering what might technically be lawful, the Compliance Advisor must always consider propriety and proportionality. For this reason, in my view, the Compliance Advisor must have wide experience at a senior level to inform his or her judgement, or have regular interaction with a dedicated supervisor who has that level of experience. I conclude that too much responsibility is being placed on the shoulders of the Compliance Advisor, exposing her to risk.

g. There is insufficient monitoring and accountability in relation to the position. It is the Compliance Advisor's role to complete second audits and quarterly reports to the Inspector-General, although these responsibilities do not appear in her job description. As mentioned above, the Compliance Advisor had not completed these aspects of her role, because she was too busy with day-to-day advice. Nobody appears to have raised these matters with her.

h. Every person that I interviewed said that there was insufficient capacity in the compliance area. That lack of capacity has resulted in a number of problems for the Compliance Advisor and GCSB as a whole, relating to cover, back-up, ability to take leave, being overwhelmed by technological developments, ability to spend time doing anything other than providing day-to-day advice (such as filing, quarterly reports, audits, developing FAQs, working on training and examining analysts, contributing to new operational policies, etc). In the Compliance Advisor's view she does not have sufficient time and resources to do the job justice, and I agree.

Manager Outreach

172. The Manager Outreach has an important role in terms of compliance because most Requests for Assistance and Requests for Information pass through him. In addition, at the time this review commenced he was the only person authorised to speak to the Department of Internal Affairs and Immigration New Zealand about citizenship and nationality questions. Accordingly, he too was until recently another single point of dependence.

173. I think that consideration should be given to how the Bureau engages with other domestic agencies on a day-to-day basis. As mentioned above, there may be merit in establishing a central liaison point to which day-to-day enquiries, Requests for Assistance and Requests for Information should be directed in relation to the Bureau as a whole (not just the Intelligence Directorate). This day-to-day liaison unit could complement

a more strategic stakeholder relations role or unit. I suggest also that thought should be given as to how some compliance aspects of the Manager Outreach's role, such as reviewing of product, are connected with the compliance team.

Operational Policy Advisor

174. The role of the Policy Advisor, who is responsible for coordinating and managing all of GCSB's operational policy, is yet another "sole trader" position. The position was established in May 2012. There is clearly a strong connection between this role and the work of the Compliance Advisor, but the way the roles work together is not currently clear.

175. I suggest that the Operational Policy and Compliance Advisors be combined in a team to ensure that there is sufficient cross-fertilisation between the development of operational policy advice and compliance thinking. I recommend also that the Operational Policy and Compliance Advisors be able to provide backup for one another, perhaps by taking a more flexible approach to the way they work and either combining the roles or rotating the staff within the unit around the different compliance and policy functions.

Integrating compliance and operational policy as part of career development and performance expectations

176. There is currently no expectation that staff in the operational parts of the Bureau should spend any professional development time working in areas such as compliance or operational policy (partly because there are only currently two roles).

177. A number of those I spoke to were very positive about the notion that rotations into a compliance and operational policy team should be part of a career development plan for analysts. Such an arrangement would:

    a. provide a Bureau-wide view of the business that would otherwise be difficult to get;

    b. ensure that compliance knowledge goes back out into the business at the end of the rotation;

    c. provide fresh thinking and updated knowledge of the operation into the compliance team.

178. The Senior Leadership Board might wish to make a rotation of this kind into the centre a positive factor in terms of promotions to team leader positions – thus providing incentives to staff.

179. In addition, expectations regarding legal and operational compliance should be built in explicitly to all relevant job performance requirements (as they are in some cases). I suggest that specific compliance or operational policy experience be encouraged as part of career progression within the Bureau.

Future legal, compliance and operational policy teams

180. It is my clear conclusion that there needs to be more capacity in both the legal and compliance areas at GCSB.

Recommendations

181. I recommend that:

Legal advice:

a. GCSB increase its legal capability, by creating a Senior Counsel position and, at least for the next 12-24 months, two junior/intermediate legal advisor positions (the latter, in the short term, to be filled through secondments – and possibly able to be reduced to one when the changes required as a result of this review are fully implemented);

b. GCSB consider sharing the additional legal capability with other agencies in the Intelligence Community – perhaps through the Intelligence Community Shared Services;

c. there be stronger links with the Crown Law Office, through formal secondments or short term exchanges of staff, and/or systematically seeking Crown Law opinions on all significant legal matters;

d. the Crown Law Office maintain a cadre of suitably cleared senior Crown Counsel to provide peer review and opinions across a range of areas.

Compliance and operational policy:

e. the compliance resource be expanded to a small team, closely linked but not part of the legal team and ideally, at least in the interim, reporting to a second tier manager such as an Associate Director;

f. the compliance resource be combined with the operational policy functions in the organisation, to strengthen the links between them and to create greater flexibility, resilience and mutual back-up;

g. the compliance team have a Bureau-wide focus;

h. there be a Compliance Manager and at least one other Compliance Advisor (I recommend two during the change process);

i. the Compliance Manager be a relatively senior position, with (initially at least) a change management focus;

j. the focus of the compliance team be Bureau-wide, but the team be physically located near to the operational teams that are the biggest internal customers of compliance advice (perhaps with some hot-desking around the different parts of the Bureau to ensure that there is a rich two way dialogue about current compliance and operational issues);

k. the job descriptions and individual performance agreements of staff employed in the compliance team be developed to ensure that all aspects of the compliance framework are reflected;

l. the Compliance Manager, in consultation with the legal team, provide close supervision of the Compliance Advisors' advice.

Outreach

m. consideration be given to centralising this day-to-day liaison role (as recommended in Part I), and ensuring that it complements a more strategic stakeholder relations role or unit;

n. some consideration be given as to how some compliance aspects of the Manager Outreach's role, such as reviewing of product, connect with the compliance team.

Conclusion

182. As is evident from the length of this report and the number of recommendations, there will need to be a really solid effort at GCSB over the next year or so to strengthen the compliance systems and – more importantly – to address some of the underlying organisational issues. I have no doubt that the Director and the Bureau as a whole are determined to see that process through.

183. My belief in the importance of the work carried out by the men and women at GCSB has only increased as this review has proceeded. The world is becoming more complex, and physical borders are less relevant. The nature of the threats to national security is shifting so rapidly that keeping up with them is a challenge – let alone getting ahead.

184. In this context, it will be important to get the balance right between addressing the important internal issues and, at the same time, ensuring that GCSB can carry on protecting New Zealand and advancing our interests. The processes put in place to ensure good compliance must not be so heavy-handed that the place grinds to a halt.

185. I am sure that the right balance can be struck so that GCSB can continue its work, in the interests of New Zealand, and that the public can be confident that systems are in place to ensure that its work is being conducted lawfully. If the oversight regime can be strengthened, that too will make a significant contribution to the rebuilding of public trust.

Appendix 1

Consolidated recommendations

Legislative Reform	
1.	Legislative reform be considered, to clarify the application of the GCSB Act 2003 to GCSB's work;
Part I: Compliance Frameworks: compliance framework at GCSB	
2.	A comprehensive compliance framework be developed for GCSB;
3.	The compliance framework be peer-reviewed by an external reviewer and implemented
Part I: Compliance Frameworks: assessing and identifying at GCSB	
4.	An exercise be undertaken to assess all relevant laws (including common law and international law) relevant to the Bureau and to ensure that current practice is consistent with the law
5.	Legal developments (new legislation, legislative amendments, relevant judgments) be systematically scanned to ensure that timely changes can be made at GCSB where necessary to ensure ongoing legal compliance
6.	Systems be established to ensure that all technological developments or material changes in practice or operation be assessed to ensure legal compliance
7.	GCSB's in-house counsel be better connected with other public sector lawyers, including the Crown Law Office
Part I: Compliance Frameworks: risk assessment at GCSB	
8.	Legal compliance be included in GCSB's risk framework
9.	The Risk and Audit Committee (which has now resumed) continue to be convened regularly
10.	Legal compliance be included in the regular reporting to the Risk and Audit Committee

Part I: Compliance Frameworks: availability of authoritative guidance and compliance tools at GCSB	
11.	The legal advisors at GCSB be required to maintain an accessible, centralised repository of authoritative legal material, opinions and legal precedents for reference within the legal team
12.	NZSID7 and other operational advice be reviewed regularly to ensure that it remains current and fit for purpose, as part of the "assessing and identifying" phase of the compliance framework, and be made available to staff in one easily accessed location
13.	Operational guidance be developed for the organisation beyond the signals intelligence (SIGINT) operation
14.	Separately from the legal advisors' material, there be a centralised repository of useful operation compliance precedents, examples and frequently asked questions, which is authoritative and kept up to date, searchable and cross-referenced and available electronically in a user-friendly format as a resource for the whole Bureau
15.	Staff not be permitted to keep precedents and compliance advice on their personal drives, because it will become out of date; if they receive a particularly useful opinion or piece of compliance advice they be directed to ask the Compliance Advisor or team to include it in the legal and compliance precedents
16.	Thought be given to the costs and benefits of a consolidated database, as discussed in classified Appendix 6
Part I: Compliance Frameworks: procedures at GCSB	
17.	The process for coordinating all Requests for Information and Requests for Assistance across the Bureau (including Information Assurance, all aspects of SIGINT, GEOINT etc) be standardised, centralised and triaged through one centralised point of contact at the Bureau
18.	Processes be systematically reviewed and be made more robust, by requiring more evidence, more research, fewer assumptions, and more judgement
19.	More use be made of free text boxes on database systems to explain thinking and reasoning
20.	Further research be done in other similar jurisdictions to see what other lessons can be applied in New Zealand with regard to processes and procedures, to support compliance while still enabling an efficient operation

Part I: Compliance Frameworks: training at GCSB	
21.	A comprehensive programme of compliance training be developed and provided for all operational staff across the Bureau (including SIGINT, Information Assurance, and cyber defence), including both face-to-face training and e-learning where appropriate
22.	All operational staff be required to sit and pass an annual compliance exam (including supervisors and managers)
23.	The existing SIGINT exam be reviewed, and compliance testing be developed for other areas of operation
24.	Part of the compliance resource be dedicated to training
25.	An active programme be considered, whereby the legal team delivers training and seminars
Part I: Compliance Frameworks: internal audit at GCSB	
26.	The compliance team have overall responsibility for the operational audit regime across the whole of the Bureau (including SIGINT, information assurance and cyber defence), with responsibility for the actual conduct of the audits (whether managers or compliance advisers) to be determined
27.	The Bureau's operational activities be reviewed periodically by the compliance team, so that internal audit can be targeted where it will add the most value (as assessed during the identification phase of the compliance cycle)
28.	Spot audits look fully at an operational activity to assess all significant areas of compliance, including judgements, reasoning and documented evidence
29.	Thought be given to whether there should be a policy against auditors auditing their own teams
30.	Training be provided to auditors
31.	Auditors themselves be spot-audited
32.	Audit responsibilities be reflected in job descriptions and individual performance agreements, as appropriate
33.	The internal guidance be updated, reissued and made accessible to staff who need it
34.	The results of such internal audit be reported to the Inspector-General of Intelligence and Security (IGIS) as part of GCSB's regular reporting

Part I: Compliance Frameworks: the Inspector-General of Intelligence and Security at GCSB	
35.	Policy work be undertaken with a view to strengthening the Office of the IGIS in New Zealand, including: a. broadening the pool of candidates for the position, by considering whether it is necessary for the IGIS to be a retired Judge, or whether independence and the ability to conduct the inquiry functions might also be found in very experienced and senior public servants and administrators; b. increasing the resources and staff supporting the IGIS; c. considering what other aspects of the Australian legislative model might translate well into the New Zealand context; d. making the work programme, audits and reporting expectations more explicit; e. much more regular visits to GCSB, access to all information, team reviews, and spot audits; f. continuing the existing self-reporting by GCSB to the IGIS via more timely quarterly reports; g. clarifying the relationship between GCSB, the IGIS and the Crown Law Office; in relation to legal advice; h. establishing a website for the Office of the IGIS
Part I: Compliance Frameworks: responding to non-compliant activity at GCSB	
36.	Procedures in the event of non-compliance be developed for all staff for whom compliance is an issue
37.	Procedures in the event of non-compliance be made explicit in writing for staff
Part I: Compliance Frameworks: external reporting at GCSB	
38.	The IGIS's requirements regarding compliance reporting be made explicit and provided in writing
39.	Responsibility for the quarterly reports be clearly allocated within the compliance team, and reflected in the relevant performance agreements

40.	Compliance statistics be reported on in the IGIS report and the GCSB Annual Report, and be made available to the Intelligence and Security Committee
41.	The IGIS's reports be made available on an official website (perhaps the GCSB website or the DPMC website until an IGIS website is established)
Part I: Compliance Frameworks: measuring at GCSB	
42.	GCSB develop explicit compliance objectives, collect statistics, assess performance against those statistics, and track historical information
43.	The compliance team be allocated the responsibility to support and monitor this process and report to the Senior Leadership Board
44.	Compliance statistics, assessed against compliance objectives, be provided annually to the IGIS and the ISC, and included in the GCSB Annual Report
Part I: Compliance Frameworks: improving compliance at GCSB	
45.	The compliance team and senior leaders use monitoring information, together with risk assessment, to focus and prioritise improvement activity
46.	A work programme be developed accordingly
47.	Resource be allocated within the compliance team to ensure that there is a conscious and systematic effort (preferably informed by best practice in other operational departments or agencies) to continuously improve systems, training, guidance and procedures
Part II: Organisational factors that have contributed to GCSB's compliance problems: organisational structure	
48.	Some innovative thought be given to reorganising GCSB in a simpler, less fragmented way that is suitable for its relatively small size but acknowledges the complexity of the business
49.	Consideration be given to reducing the number of small units and managers
50.	Roles that should really be Bureau-wide (compliance, outreach etc) be placed centrally within the Bureau and reconfigured
51.	The scope of the Bureau's activities be scrutinised closely and systematically to work out whether capability can be less widely spread, focused more deeply on the things that matter, and that any low priority work be identified and eliminated

52.	Effort be made to avoid single points of dependence
53.	Compliance advice and operational policy be combined in a team, placed (at least in the interim) under the aegis of a second tier manager such as an Associate Director, located centrally within the Bureau, and located separately from – although working closely with – the legal team and operational staff
54.	Roles (e.g. legal advisors, compliance advisors) be configured so as to avoid combining functions that conflict, and to encourage internal challenge
55.	There be one centralised point of contact within the Bureau for all day-to-day engagement with external agencies
56.	The place of the National Cyber Security Centre and GEOINT within the Bureau be clarified
Part II: Organisational factors that have contributed to GCSB's compliance problems: Governance, Internal Governance and ODESC(G)	
57.	GCSB's Board agree on a Board Charter that makes it clear that the Board's focus is strategic direction, risk, opportunities, the overall work programme, major projects, the departmental budget, workforce capability and capacity, etc
58.	Secretariat support be provided for the Board to assist it to achieve this focus
Part II: Organisational factors that have contributed to GCSB's compliance problems: GCSB's culture	
59.	A concerted effort be made within GCSB to improve performance management practices, to ensure that all roles are regularly refreshed without losing institutional knowledge, and that persistent non-performers who cannot demonstrate improvement are exited (subject to a proper employment process) to allow for fresh recruitment
60.	Thought be given to targeted rotations and secondments between the operational and central parts of GCSB (for example, rotating promising analysts through the compliance and policy team as part of their professional development)
61.	Thought be given to a structured programme of secondments between GCSB and other public service departments, in order to increase knowledge of the Intelligence Community and to increase the Bureau's connection with mainstream public service thinking and developments

Part II: Organisational factors that have contributed to GCSB's compliance problems: information management at GCSB	
62.	A professional information manager be appointed to review GCSB's business information needs and to rationalise and align the current systems as much as possible
63.	The information manager be expressly tasked with rationalising databases and other information management applications in a way that does not impact on the operational work of the Bureau
64.	The information manager have the authority to develop and implement an information management strategy with associated guidelines
65.	The information manager address the issue of record keeping, as a matter of urgency
66.	All staff be required to operate in accordance with that information management strategy and those guidelines
Part II: Organisational factors that have contributed to GCSB's compliance problems: capability and capacity issues within GCSB (legal advice)	
67.	GCSB increase its legal capability, by creating a Chief Legal Advisor position and, at least for the next 12-24 months, two junior/intermediate legal advisor positions (the latter, in the short term, to be filled through secondments - and possibly able to be reduced to one when the changes required as a result of this review are fully implemented)
68.	GCSB consider sharing the additional legal capability with other agencies in the Intelligence Community - perhaps through the Intelligence Community Shared Services
69.	There be stronger links with the Crown Law Office, through formal secondments or short term exchanges of staff, and/or systematically seeking Crown Law opinions on all significant legal matters
70.	The Crown Law Office maintain a cadre of suitably cleared senior Crown Counsel to provide peer review and opinions across a range of areas
Part II: Organisational factors that have contributed to GCSB's compliance problems: capability and capacity issues within GCSB (compliance and operational policy)	
71.	The compliance resource be expanded to a small team, closely linked but not part of the legal team and ideally, at least in the interim, reporting to a second tier manager such as an Associate Director

72.	The compliance resource be combined with the operational policy functions in the organisation, to strengthen the links between them and to create greater flexibility, resilience and mutual back-up
73.	The compliance team have a Bureau-wide focus
74.	There be a Compliance Manager and at least one other Compliance Advisor (I recommend two during the change process)
75.	The Compliance Manager be a relatively senior person, with (initially at least) a change management focus
76.	The focus of the compliance team be Bureau-wide, but the unit be physically located near to the teams that are the biggest internal customers of compliance advice (perhaps with some hot desking around the different parts of the Bureau to ensure that there is a rich two way dialogue about current compliance and operational issues)
77.	The job descriptions and individual performance agreements of staff employed in the compliance unit be developed to ensure that all aspects of the compliance framework are reflected
78.	The Compliance Manager, in consultation with the legal team, provide close supervision of the Compliance Advisors' advice
Part II: Organisational factors that have contributed to GCSB's compliance problems: capability and capacity issues within GCSB (Outreach)	
79.	Consideration be given to centralising this day to day liaison role (as recommended in Part I), ensuring that it complements a more strategic stakeholder relations role or unit
80.	Some consideration be given as to how some compliance aspects of the Outreach Manager's role, such as sensi-checking and reviewing product, connect with the compliance team

This page intentionally left blank.

Compliance review – terms of reference

Objective

1. The objective of the review is to provide the Director with assurance that GCSB's activities are undertaken within its powers and that adequate assurance and safeguards are in place. Where the review identifies gaps or risks, changes will be recommended to address them.

Problem / opportunity

2. In the aftermath of the Police operation "Operation Debut" it became apparent (and was acknowledged publicly) that GCSB had undertaken unauthorised surveillance of Mr Kim Dotcom, his family and an associate. The case raised questions as to how such unlawful activity has been able to occur, and whether GCSB has undertaken any other unlawful surveillance in the past. That situation is the catalyst for this review.

3. Rebecca Kitteridge ("the reviewer") has been seconded to GCSB as Associate Director and has been asked to review the systems, processes and capabilities underpinning GCSB's operations. The review needs to be undertaken in the context of the future direction of GCSB (as articulated by GCSB's Director) and the Intelligence Community (IC) as a whole. That future direction is set out in accountability documents such as the four year plan and workforce strategy, and is consistent with the aspirations of the Better Public Services strategy. This review will support the Director's goal of re-founding the organisation to position it (and the IC as a whole) for the future.

Deliverable

4. The reviewer will deliver a report to the Director that will address the following matters:
   - 4.1. whether the Bureau has been conducting its activities within its statutory powers, and whether there are any areas of ambiguity or difficulties of interpretation in relation to the legislative framework;
   - 4.2. whether the structure and capabilities of GCSB have contributed to GCSB carrying out any of its functions without clear legal authority (e.g. lack of capability or capacity, lack of checks and balances in the organisation's structure);
   - 4.3. whether the systems and processes within GCSB (e.g. compliance resources and procedures, IT systems, documentation and record-keeping, internal legal scrutiny and challenge, internal audit) are adequate;

4.4. whether the oversight regime and other accountability mechanisms (e.g. Inspector-General of Intelligence and Security, Intelligence and Security Committee, Audit Office, Office of the Ombudsmen) are sufficiently robust to ensure that GCSB is operating lawfully and in accordance with the government's objectives; and how to make best use of these mechanisms;
4.5. the culture of the organisation and its role in the way that GCSB conducts its activities;
4.6. public trust in GCSB (and the IC generally) and what changes may be required to build it.

5. The report will recommend actions to address the issues identified in the review, aligned as much as possible with GCSB's and the IC's objectives and future direction. Recommendations may include suggested changes to GCSB's and/or the IC's:
   5.1. structures, capability and capacity;
   5.2. internal procedures, systems, documentation, audit, governance;
   5.3. oversight regime;
   5.4. organisational culture;
   5.5. transparency and public communication regarding its activities;
   5.6. legislation (see also 7.6 below).

Scope

6. The review will be limited to the matters set out above, and will not:
   6.1. be an inquiry into GCSB's participation in Operation Debut; or
   6.2. focus on the performance of individual GCSB staff members (except to the extent that it is necessary to describe the organisational structures, systems, and processes relevant to compliance).

Related projects

7. This review is connected with, but separate from:
   7.1. the legal action against the Crown by Kim Dotcom;
   7.2. the Inspector-General's inquiry into assistance provided by GCSB to law enforcement agencies since 2009;
   7.3. any internal investigations relating to individual staff members, or the Police investigation, resulting from GCSB's participation in Operation Debut;
   7.4. GCSB's/the IC's four year planning and workforce strategy;
   7.5. the proposal to share some corporate services;
   7.6. the policy and legislative review being led out of ICG.

Resources

8. The resources provided for the review are:
   - Project support: Senior Advisor, GCSB; Executive Assistant, GCSB

- Legal support: Legal Advisors on secondment to GCSB

Advisory Group

9. The reviewer will report to the Director of GCSB in relation to the review.

10. An Advisory Group will meet periodically in the course of the review to consider the progress of the review, draft findings and recommendations. The Advisory Group will comprise:

    - the Chief Executive of DPMC (Chair)
    - the Solicitor-General
    - the Director NZSIS
    - the Director of the Intelligence Coordination Group
    - the SSC Assistant Commissioner responsible for the Domestic and External Security Sector

11. The Director of GCSB and the reviewer will attend meetings of the Advisory Group.

12. The final conclusions and recommendations in the report will not be subject to direction from either the Director or the Advisory Group and will be the reviewer's own.

Approach, process and timeframe

13. It is acknowledged that the commencement of the structured review has been delayed by the number of immediate issues facing the Bureau since the reviewer's arrival. In her role as Associate Director, her initial focus has been on supporting the Director by assisting him to establish interim teams (legal, policy, communications, project), and dealing with other urgent issues such as legal issues, media and public requests for information, and unauthorised disclosures of GCSB information. These issues have taken precedence over the formal review that is the purpose of the secondment.

14. The timeline and milestones for the completion of the compliance review are:

Completion date	**Milestone**
31 Jan	**Phase 1(a):** Complete information gathering: (1) read foundation documents – strategic direction, accountability documents (four year plan, workforce strategy, statement of intent, annual reports, etc), Foreign Intelligence Requirements etc; (2) speak to all areas of the GCSB business; (3) speak to key people within IC, customers, and central agencies; (4) obtain comparative information on compliance, assurance and oversight from counterparts as required.
31 Jan	**Phase 1(b): Urgent legal issues** Legal team to tackle urgent legal compliance issues.
14 Feb 28 Feb	**Phase 2: engaging with staff and external stakeholders to test preliminary conclusions** Provide preliminary conclusions to staff and external stakeholders (other agencies) to test thinking and ensure robustness of analysis. Obtain responses from staff and external stakeholders.
8 March 15 March 29 March	**Phase 3: Write up** Provide draft report and recommendations to Director and Advisory Group. Discuss with Advisory Group. Finalise and deliver report.

Note: Whether this timeline can be adhered to depends on:

- the number and significance of compliance issues identified; and
- whether the reviewer is able to focus solely on the review, or whether she is required to support other aspects of the business.

15. Any change to the reporting and implementation timeline will be discussed and agreed between the reviewer, the Director and the Advisory Group.