GCSB Compliance Review – Progress Report 1

June 2013

This is the first report on the Government Communications Security Bureau's (GCSB) activities and change programme since the Compliance Review conducted by Rebecca Kitteridge was released on 9 April 2013.

The GCSB has a major change programme underway that reflects the recommendations of the Compliance Review.

The Review made 80 recommendations, including recommendations about changes to external oversight and legislation, which the GCSB is not responsible for, but to which it can contribute.

The recommendations fell into seven broad areas, which are described below:

1. **Compliance (29 recommendations)**
   The GCSB will develop and implement a comprehensive and externally peer reviewed compliance framework. The framework will include regularly convening GCSB's Risk and Audit Committee; regularly reviewing compliance advice regarding operational activity; forming a compliance team; instituting more vigorous compliance training and testing for staff; and formalising procedures for dealing with non-compliance.

2. **Oversight (3 recommendations)**
   While this is an area "owned" principally outside of the GCSB, the GCSB will be prepared for more engagement with the Inspector General of Intelligence and Security (IGIS), and will provide access to all necessary information, team reviews and spot audits. There will be greater clarity about the relationship between the GCSB, IGIS and Crown Law in relation to legal advice.

3. **Information Management (9 recommendations)**
   A new Information Manager will review and rationalise systems and implement a robust information management strategy and guidelines. A centralised system for legal information including precedents will be established, alongside (but separate to) a centralised searchable repository for operational precedents, examples and other authoritative information, which will be frequently updated.

4. **Legal Capability and Capacity (9 recommendations)**
   In-house legal capacity will be increased and consideration given to greater sharing of legal resources among the New Zealand Intelligence Community. In-house legal staff will provide training for staff. Legal developments and all relevant laws will be scanned systematically to ensure that current GCSB practice is consistent with the law.

5. **Measurement and Reporting (4 recommendations)**

Legal compliance will be reported regularly to the GCSB Risk and Audit Committee. Internal auditing will be reported quarterly to the IGIS, and the IGIS's and GCSB's annual reports will include compliance reporting information. The GCSB will develop specific compliance objectives and will monitor performance against these.

6. **Organisation Structure and Culture (20 recommendations)**
   A standard process will be established for the coordination of all Requests for Information or Assistance (RFI/RFA). Audit responsibilities will be reflected in individual position descriptions and performance documents. Monitoring and risk assessment will be used to prioritise improvement activity and on-going work programmes.

   The Compliance Review considered that GCSB's organisational structure is somewhat fragmented. The organisation will contemplate how to reconfigure and centralise roles that should have a more GCSB-wide focus. The role of the National Cyber Security Centre will be clarified. A Board charter will be developed with a strategic focus, and a secretariat will help the Board (i.e. senior management team) to achieve that focus. Staff performance management will be improved, role rotation will be increased, and an internal and external secondment programme will be established.

7. **Outreach Capability and Capacity (2 recommendations).**
   The GCSB will establish a centralised point of contact for day-to-day engagement with external agencies, and will be part of a more strategic stakeholder relations function.

Commentary by Ian Fletcher, Director GCSB

We have made good progress implementing the recommendations from the Compliance Review of the Government Communications Security Bureau (GCSB) in the two and a half months since the Review was delivered.

Of the 80 recommendations, there are 76 that the GCSB is directly responsible for implementing, and there are others, such as legislation, for which others are responsible.

One of our greatest challenges has been finding staff with expertise in the areas we need with appropriate security clearances. Nonetheless, we have made real progress, which means we will have even greater resource to implement the recommendations.

The first tranche of recommendations that we have implemented focuses on the things that we need to have in place immediately to function more effectively: getting new processes and systems bedded in to be business as usual, and making appointments to key roles including the Associate Director, a Chief of Staff, a Chief Legal Adviser, and a Compliance and Policy Manager.

A total of 25 recommendations have been completed. We are on track to have another 11 recommendations implemented in the next quarter.

Some of the recommendations will take well into 2014 to implement, as they involve longer term programmes including staff rotation, external secondments and performance management practices.

The Bureau is also in the first stages of working through the State Service Commission's public service Performance Improvement Framework (PIF). This looks at organisational capability now and in the future. It will both complement and underpin the immediate business improvement activities recommended in the Compliance Review. The results of the external PIF Review will be published late this year or early next year.

The next quarterly progress report on the GCSB's implementation of the Compliance Review's recommendations will be published at the end of September 2013.

Ian Fletcher
Director GCSB
30 June 2013

Completed GCSB Compliance Review Recommendations – June 2013

#	RECOMMENDATION
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.
7	GCSB's in-house counsel to be better connected with other public sector lawyers, including the Crown Law Office.
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.
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.
16	Thought be given to the costs and benefits of a consolidated database, as discussed in classified Appendix 6.
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.
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.
29	Thought be given to whether there should be a policy against auditors auditing their own teams.
43	The compliance team be allocated the responsibility to support and monitor this process and report to the Senior Leadership Board.
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.
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.
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.
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 position (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.

#	RECOMMENDATION
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.
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.
78	The Compliance Manager, in consultation with the legal team, provide close supervision of the Compliance Advisors' advice.
80	Some consideration be given as to how some compliance aspects of the Outreach Manager's role, such as sensi-checking and reviewing of product, connect with the compliance team.