GOVERNMENT COMMUNICATIONS SECURITY BUREAU

TE TIRA TIAKI

G56

Annual Report

For the year ended 30 June 2014

www.gcsb.govt.nz

New Zealand Government

Presented to the House of Representatives pursuant to Section 12 of the Government Communications Security Bureau Act 2003

ISN 1176-4686 (Print)

ISN 1178-0789 (Online)

Preface

This is the unclassified version of the Annual Report of the Government Security Communications Bureau (GCSB) for the year ended 30 June 2014. It differs from the classified version of the report which was delivered to the Minister Responsible for the GCSB, and submitted to members of the Intelligence and Security Committee.

In accordance with section 12(4) of the Government Communications Security Bureau Act 2003, material has been omitted from this version of the report for reasons of security.

Table of Contents

Message from the Director

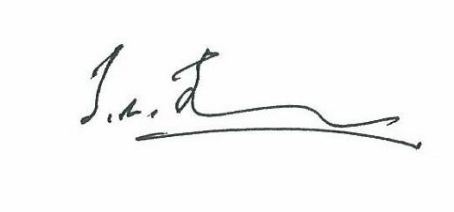
The year to the end of June 2014 has been dominated by the task of implementing the legislative amendments which Parliament enacted at the end of September 2013.

These amendments provided a good deal of clarity about GCSB's functions, associated powers, and authorising framework. The Department also benefited from the stronger provisions for oversight by the Inspector General of Intelligence and Security, which came into force at the same time.

By the end of the year in review, the Compliance Review implementation process was nearly complete (and has subsequently been completed), and a great deal of work on associated policies, training, and compliance systems has been undertaken.

As the annual report shows, work has also gone on to improve a lot of the Department's systems, and to look at its structure, functions and capabilities. A lot of this is still work in progress, with the Ministers considering the way ahead for GCSB and the wider New Zealand Intelligence Community into 2015.

Taken together, this has been the year of consolidation of changes already underway, and preparation for a future focus on capabilities, deeper and better cooperation across the intelligence community and its customers, and an enduring focus on compliance.



Ian Fletcher
Director

About GCSB

The Government Communications Security Bureau (GCSB) is a public service department and reports directly to the Minister Responsible for GCSB.

Our history

The New Zealand government has had access to a signals intelligence (SIGINT) capability since the Second World War. There was a long recognised need to ensure that the government was protected from "bugging" (technical security, or TECSEC) and that its sensitive messages could not be read by third parties (communications security, or COMSEC). Until the establishment of GCSB, these services were provided by bodies such as the New Zealand Defence Force (NZDF) and the New Zealand Security Intelligence Service (NZSIS). In 1977, Prime Minister Robert Muldoon approved the formation of GCSB, but is functions and activities were kept secret.

In 1980, it was decided that the existence of GCSB could be disclosed on a limited basis, leading to the first briefings of the Cabinet and the Leader of the Opposition. These briefings acknowledged GCSB's TECSEC and COMSEC functions, but not its SIGINT function. Prime Minister Muldoon publicly acknowledged the existence of GCSB and its SIGINT function in 1984.

In early 2000, a legislative process to place GCSB on a statutory footing similar to that of the NZSIS began. In 2003, the Government Communications Security Bureau Act 2003 (GCSB Act) took effect. In June 2003, Cabinet formalised the role of GCSB as the national authority for signals intelligence and information systems security.

Functions and objectives

The GCSB Act, as amended in 2013, sets out the functions of GCSB and makes provision for its administration and the conduct of its operational activities.

The three functions of GCSB, as set out in the Act, are:

Information assurance and cyber security

- providing advice and assistance to government and other entities regarding the protection and security of communications and information infrastructures;
- identifying and responding to threats or potential threats relating to the communications and information infrastructures of government and other entities; and
- analysing and reporting on matters relating to the security and protection of government and other entities' communications and information infrastructures.

Intelligence gathering and analysis

- gathering and analysing intelligence in accordance with the government's requirements;
- gathering and analysing intelligence about information infrastructures; and
- providing intelligence and analysis to the Responsible Minister and any other person or office holder authorised by the Responsible Minister.

Co-operation with other entities to facilitate their functions

- subject to controls and limitations, cooperating and providing advice and assistance to the New Zealand Police, the New Zealand Defence Force and the New Zealand Security Intelligence Service for the purpose of facilitating the performance of those entities' lawful functions.

The Act specifies that the objective of GCSB, in performing its functions, is to contribute to the:

- national security of New Zealand; and
- international relations and well-being of New Zealand; and
- economic well-being of New Zealand.

Location

GCSB's head office is located on Pipitea Street in Wellington. GCSB also has two communications collection and interception stations: a high frequency radio interception and direction-finding station at Tangimoana, near Palmerston North, and a satellite communications interception station at Waihopai, near Blenheim.

Staff

GCSB employs approximately 300 staff in a wide range of disciplines including foreign language experts, communications and cryptography specialists, engineers, technicians and corporate staff.

The Director GCSB

Ian Fletcher started as Director GCSB at the end of January 2012.

The principal responsibilities of the Director GCSB are those set out in section 32(1) of the State Sector Act 1988, which ensure that the Director is accountable to the Responsible Minister for:

- GCSB carrying out the purpose of the State Sector Act;
- GCSB's responsiveness on matters relating to the collective interests of government;
- the stewardship of GCSB, including of its medium and long-term sustainability, organisational health, capability, and capacity to offer free and frank advice to successive governments;
- the stewardship of–
  - assets and liabilities on behalf of the Crown that are used by or relate to GCSB;

    - the legislation administered by GCSB;
- the performance of the functions and duties and the exercise of the powers of the Director or of GCSB (whether imposed by any enactment or by the policies of the government);
- the tendering of free and frank advice to Ministers;
- the integrity and conduct of the employees for whom the Director is responsible; and
- the efficient and economical delivery of the services provided by GCSB and how effectively those services contribute to the intended outcomes.

The GCSB Board

The Director is supported in his role by an internal GCSB Board.

The Board meets regularly to focus on GCSB's: strategic direction; risk; opportunities; overall work programme; significant organisation-wide policies; major projects; departmental budget; and workforce capability and capacity.

In addition to the Director, the Board is comprised of the:

- Associate Director;
- Chief Financial Officer;
- Chief Information Officer;
- Chief Legal Advisor;
- Chief of Staff;
- Deputy Director Information Assurance and Cyber Security;
- Deputy Director Intelligence;
- Director National Security Communications;[1] and
- General Manager Intelligence Community Shared Services.

Risk and Audit Committee

The Risk and Audit Committee is an independent committee reporting directly to the Director. The role of the Committee is to assist the Director in fulfilling his governance responsibilities, through the provision of independent advice on the:

- risk management framework;
- assurance system and framework, including legal, policy and procedural compliance; and
- audit system (internal and external).

The Risk and Audit Committee has two members.

---

[1]The Director National Security Communications is an employee of the Security and Intelligence Group (SIG) within the Department of the Prime Minister and Cabinet. The National Security Communications team (within SIG) provides services to all agencies of the New Zealand Intelligence Community.

Oversight

The Intelligence and Security Committee (ISC) is the parliamentary oversight mechanism for intelligence agencies, and examines issues of efficacy and efficiency, budgetary matters and policy settings. The ISC is made up of the Prime Minister, two members of Parliament nominated by the Prime Minister, the Leader of the Opposition, and one Member of Parliament nominated by the Leader of the Opposition.

GCSB is subject to further oversight by the Inspector-General of Intelligence and Security (IGIS). The principal role of the IGIS is to assist the Responsible Minister in the oversight and review of GCSB and NZSIS and in particular:

- to assist the Minister in ensuring that the activities of GCSB and NZSIS comply with the law;
- to inquire into any complaint by a New Zealand person, or an employee or former employee of GCSB or NZSIS;
- to inquire into any matter where it appears that a New Zealand person has or may have been adversely affected by GCSB or NZSIS; and
- to inquire into the propriety of particular activities of GCSB or NZSIS.

GCSB is part of a wider intelligence community

GCSB, along with the NZSIS and the Security and Intelligence Group within the Department of the Prime Minister and Cabinet (DPMC), form the core New Zealand Intelligence Community (NZIC).

There are other intelligence capabilities too. The New Zealand Defence Force, New Zealand Police, New Zealand Customs Service and Immigration New Zealand all have intelligence units. The core NZIC works with these other intelligence units, and the wider New Zealand government sector, to ensure the security of New Zealand and promote New Zealand's interests.

A year of transformation

Amendments to GCSB's governing legislation

On 26 August 2013, Parliament enacted amendments to the GCSB Act that took effect from 27 September 2013.

The amendments made changes to the objective, functions, and limitation provisions to improve clarity about the legal basis for GCSB's activities, and to accommodate changes in the prevailing security environment, particularly in relation to cyber security and information security.

The amendments ensured that GCSB's cyber-defence work would be subject to Ministerial authorisation, and for the first time also required GCSB to engage with the Commissioner of Security Warrants. The Commissioner now issues cyber security warrants and authorisations jointly with the Minister Responsible for GCSB. The amendments also refreshed the statutory criteria to be met with respect to all other Ministerial authorities, to ensure that statutory functions are strictly adhered to and that outcomes are properly evaluated to confirm they cannot be achieved by any other means.

During 2013/14, GCSB put a considerable amount of effort into developing and implementing a revised suite of operational policies to give effect to the legislative amendments. In particular, attention was given to strengthening the nationality assessments process to ensure compliance with obligations under section 14 of the GCSB Act. Work was also undertaken to improve the management of requests for advice and assistance submitted to GCSB under section 8C of the GCSB Act.

Amendments to the Inspector-General of Intelligence and Security Act 1996

Since 1996, both GCSB and NZSIS have been subject to oversight by the Inspector-General of Intelligence and Security (IGIS). This statutorily-established role exists within a wider framework of oversight that was set up to provide a balance between the secrecy required for effective intelligence operations and legitimate public expectations of government agency transparency.

The statute governing the position and functions of the IGIS was amended in 2013 alongside the GCSB Act. A number of changes were made to strengthen the Office of the IGIS, increase the resources of the Office to enable a greater range of activities to be carried out, expand the IGIS's statutory work programme and enhance the corresponding reporting requirements. GCSB and NZSIS have assisted with the implementation of these changes by making sure the Office of the IGIS has sufficient resources and is properly secure. Both agencies also established mechanisms to give the IGIS appropriate and flexible access to systems, staff and information as required and to proactively provide the IGIS and others within the Office with all necessary and desirable information to ensure operations were understood, informed decisions could be made and work programmes could be appropriately focussed.

Regular contact with the IGIS and her staff at senior levels ensures that the GCSB and NZSIS continue to be responsive to the needs of that Office. Both agencies are committed to rebuilding public trust in the wider intelligence community and to that end it is critical that the IGIS be well-informed and able to exercise her statutory oversight role to the full extent anticipated by Parliament.

Introduction of the Telecommunications (Interception Capability and Security) Act 2013

On 11 November 2013, Parliament enacted the Telecommunications (Interception Capability and Security) Act 2013 (TICSA). Part 3 of TICSA, which took effect on 11 May 2014, relates to network security and establishes a framework under which New Zealand's telecommunications network operators are required to engage with government on proposals for procurement or changes to areas of specified security interest in their networks. TICSA continues the GCSB's role, alongside other interception agencies, in relation to interception capability.

GCSB applied a substantial amount of resource to support the implementation of TICSA, including network security and telecommunications engineering expertise, policy, analysis, regulatory expertise and legal advice. One of the first activities was the preparation of a guidance paper to assist network operators and GCSB to work co-operatively and collaboratively with each other to apply the principles set out in section 8 of TICSA relating to network security risks. The draft guidance was issued to all network operators in March 2014 for consultation, supported by face to face meetings to walk through the proposal.

The feedback received from network operators during the consultation process was very valuable and resulted in a number of amendments to improve the clarity of the final guidance paper, which was issued on 6 May 2014. GCSB intends to review the guidance paper in 2015 to gain network operators' feedback about how the process is working in practice and to make any required refinements.

Continuing implementation of the Compliance Review recommendations

In September 2012, the Director and the DPMC Chief Executive initiated a review of compliance at GCSB. The review, which was conducted by Rebecca Kitteridge, took into account GCSB's activities, systems and processes since 1 April 2003 (the date the GCSB Act came into force).

Ms Kitteridge's report, which was released by the Government in April 2013, highlighted a longstanding lack of good systems and processes in relation to compliance, as well as underlying organisational problems for GCSB. The Director accepted all of the report's recommendations and committed to publicly reporting each quarter on the progress that had been made in implementing them.

Prior to the period this report covers, 25 of the 76[2] recommendations had been fully-implemented. These recommendations included the things that needed to be put in place immediately before further change could be effected – e.g. making appointments to key roles such as Chief Legal Advisor and the Compliance and Policy Manager.

During the 2013/14 year, GCSB fully-implemented a further 48 recommendations in the seven broad areas of:

- compliance;
- oversight;
- information management;
- legal capability and capacity;
- measuring and reporting;
- organisation structure and culture; and
- outreach capability and capacity.

One of the most significant achievements was the development of a comprehensive framework of processes, tools and structures to support the effective management of compliance obligations. The day to day monitoring of the framework is the responsibility of a newly created compliance and policy team. In addition to revising procedures and developing compliance training for operational staff across GCSB (including SIGINT and Information Assurance and Cyber Security), the team implemented an internal audit regime, the results of which are provided to the IGIS through a regular reporting programme.

Another significant response to the Compliance Review recommendations was the strengthening of the internal legal capability, and the extent to which it is ingrained into the day to day activities of GCSB.

During 2012/13, a new Chief Legal Advisor role was created, and in 2013/14 a further three legal advisors were appointed. One of the first tasks for the legal team was to complete an analysis of the domestic legislative instruments relevant to GCSB and implement the tool *ComplyWith* to audit compliance. The team adapted ComplyWith to reflect the particular obligations and responsibilities of GCSB as an intelligence agency. The first audit using ComplyWith was undertaken in early 2014/15, the results of which were notified to Audit New Zealand and the IGIS.

Key international obligations were also assessed through warranting and legal advice, including Crown Law as appropriate.

GCSB's Legal Team is connected to other public sector lawyers through a variety of fora including the Government Legal Network's (GLN) Defence, Security and Intelligence Legal Practice Group, and the Chief Legal Advisors' forum. In addition, the GCSB Chief Legal Advisor has been classified as a key legal position within government which means the role receives particular oversight and attention from GLN.

[2] The report contained 80 recommendations in total; GCSB was directly responsible for implementing 76.

Two of the recommendations completed were not implemented in the way described in the Compliance Review. Recommendations 17 and 50 addressed reconfiguration, centralising functions, and standardising processes for all aspects of GCSB's activities, including both its foreign intelligence gathering and information assurance activities. GCSB believed it could better achieve the objectives of the Compliance Review and provide greater internal oversight by keeping requests for assistance for foreign intelligence and for information assurance activities separate, in keeping with the way these functions are treated in our newly amended legislation.

The three recommendations not fully-implemented by the end of 2013/14 related to some aspects of staff training and the examination to test the effectiveness of that training. These recommendations were completed in the first quarter of 2014/15.

Strategic initiatives undertaken in 2013/14

Capability Review

In 2014, following completion of the NZIC four-year planning process, the NZIC committed to undertake a capability review. This review will identify options for Government that address the relationship between the New Zealand government's security and intelligence requirements, the capability that the NZIC needs to meet these requirements and the resourcing of the NZIC.

In the 2013/14 year, the review team undertook initial scoping and preparation. The outcomes of the review will be presented to Ministers in 2015.

Functional Review

In late 2013, GCSB initiated a Functional Review (the Review) of some operational arrangements. In part, the Review resulted from observations in the Review of Compliance at GCSB, as well as from the Performance Improvement Framework self-review team, that the structure of GCSB might not be ideal.

The Review resulted in a series of recommendations to rebalance GCSB's Intelligence Directorate in order to ensure GCSB remained capable of meeting the New Zealand government's intelligence needs.

The Review also recommended the creation of a Capability Directorate to strengthen GCSB's information and communications technology (ICT). This new directorate would be responsible for GCSB's corporate ICT requirements and issues of ICT governance (such as software licensing). GCSB's technical ICT needs would be retained by the Intelligence and Information Assurance and Cyber directorates to maintain mission focus and enable flexibility and agility.

In March 2014, GCSB's Board approved the proposals in the Review for consultation with affected staff. The feedback received from staff during the consultation period was valuable and led to a number of refinements and changes to the original proposal.

The implementation of the final proposal document will be completed during the 2014/15 year.

Countering advanced cyber threats

GCSB is acquiring capabilities to protect selected entities against foreign-sourced cyber threats that are particularly advanced in terms of technical sophistication and/or persistence (Project CORTEX). GCSB's acquisition of these capabilities is consistent with, and will contribute to, the objectives of the New Zealand Cyber Security Strategy.

The harms at issue – e.g. theft of intellectual property, or damage to IT systems – are caused by malicious software ('malware') that cannot always be countered by commercial tools. Advanced malware is being directed against networks or systems

owned by: key economic generators; niche exporters including in knowledge-intensive industries; major IT service providers; and government agencies.

During 2013/14, GCSB developed a detailed business case for Project CORTEX to present the Government with a range of options to protect organisations under particular threat from advanced cyber threats. All options contained in the business case, which was presented to Cabinet in July 2014, were consistent with the amended GCSB Act and necessary warranting procedures, and involve obtaining the express consent of the participating entities.

Reviewing New Zealand's high grade cryptographic infrastructure

One of GCSB's core roles, under its information assurance function, is to operate New Zealand's high-grade cryptographic infrastructure (HGCI) which ensures that all New Zealand information and communications classified at a level higher than RESTRICTED are protected through advanced encryption. During 2013/14, GCSB continued a project reviewing the operability of the HGCI.

Operational performance

The agencies that comprise the NZIC undertake activities and produce outputs in order to contribute towards the five joint impacts as stated in the outcome framework (2013/17 Statement of Intent refers). The extent to which an individual agency contributes to each of the joint impacts is dependent upon the objectives and functions set out in its enabling legislation and any direction given to it by its Responsible Minister.

Identifying and reducing New Zealand's vulnerabilities

Through the provision of cyber and intelligence reporting, threat alerts, information assurance and technical services, GCSB enables government to identify and mitigate against threats to national security.

During 2013/14, GCSB provided specialist services to some government agencies to protect them against sophisticated or persistent malware that cannot always be countered by commercial tools. It is likely that GCSB will extend those services to other government agencies during the 2014/15 year.

The National Cyber Security Centre (NCSC), which sits within GCSB, provides enhanced cyber security services to New Zealand government and private sector organisations to assist them in defending themselves from cyber-borne threats.

The NCSC delivered a number of cyber threat advisories during the reporting period. These covered issues such as vulnerabilities in commonly used software and operating platforms, through to risk and mitigation information relating to the use of mobile electronic devices.

On an annual basis, NCSC compiles Incident Summary Reports to raise awareness and general understanding of the nature of the cyber-threat landscape facing New Zealand organisations and individuals. In May 2014, NCSC published the report for the 2013 calendar year which showed a continued increase in the number of cyber incidents reported and recorded, from a total of 134 recorded incidents in 2012 to a total of 219 in 2013. GCSB believes this increase can be attributed, in part, to greater awareness of the importance of reporting incidents among New Zealand government agencies and critical infrastructure providers, as well as a growing awareness of the role and function of NCSC.

NCSC Case Study - Spoofed Email Addresses

Private sector organisations reported receiving emails purporting to be from employees. These 'spoofed' emails were actually sent by scammers who were able to identify employees from the organisations' open source information.

The scammers used these names, or similar variations, to establish free email accounts. These web-based addresses were then used to send emails to colleagues of the legitimate employees, requesting that funds be paid on behalf of the organisation to bank accounts operated by the scammers. Some organisations suffered financial losses as a consequence.

During 2013/14 staff from NCSC, in partnership with the New Zealand Control Systems Security Information Exchange (CSSIE) group developed the *NCSC Voluntary Cyber Security Standards for Industrial Control Systems*. This guidance assists organisations to recognise and address cyber security risks associated with the operation of industrial control systems (ICS) technologies.

As much of New Zealand's critical infrastructure makes heavy use of ICS technologies, and the infrastructure of New Zealand is highly interconnected and interdependent, cyber-threats could have major economic ramifications or result in environmental damage or loss of life. The development of these voluntary standards provides an important baseline of cyber security protection by establishing common security countermeasures that can be applied to ensure reliable operation across and between critical infrastructure operations.

Under its information assurance function, GCSB continued to assist government entities regarding the protection and security of their communications and information infrastructure.

Increasing the security of New Zealand deployments

In 2013/14, GCSB continued to provide critical support to New Zealand Defence Force (NZDF) personnel who were deployed overseas.

GCSB provided information assurance advice and services to help protect NZDF and its equipment from compromise, as well as intelligence information to support NZDF's operations.

GCSB also supported naval training and provided advice and assistance to NZDF's Capability Branch on a number of different projects.

Informing New Zealand's policy-makers and decision-makers on foreign political and economic issues

GCSB informs policy-makers and decision-makers on foreign political and economic issues by producing and disseminating foreign intelligence reports that meet the intelligence requirements of government.

In 2013/14, GCSB collected, processed and analysed foreign intelligence to produce reports covering topics of national interest.

In addition to the provision of foreign intelligence, the availability of information assurance and cyber security advice and services also continued to inform decision-makers of the economic implications of malicious cyber intrusions in New Zealand.

Customer Outreach

The main interface between GCSB and its intelligence customers is the Customer Outreach Team that interacts daily, weekly, or as required, with multiple individuals from over twenty government departments.

Through building relationships with customers and understanding their needs, the team feeds back requirements into the intelligence cycle to ensure that GCSB is working on the issues and topics of greatest importance to government.

In addition to sourcing customers' requirements, the Customer Relations Officers (CROs) are responsible for scanning GCSB and partner intelligence reports and assessments, and then selecting the material that meets each individual customer's needs. In the Partner and Customer Survey undertaken in 2013, customers said that they particularly valued the relationship they had developed with their CRO from face-to-face contact, as well as the ongoing ability to refine their intelligence requirements through direct feedback.

Safeguarding New Zealand against threats of violent extremism and espionage

GCSB contributes to this impact across all of its operational areas.

During 2013/14, the New Zealand SIGINT Operations Centre (NZSOC) continued its provision of a 24 hour 7 day a week watch and warn service, which alerted customers when it obtained information that could have affected the safety and/or security of New Zealanders and New Zealand entities both at home and abroad.

Through the NCSC, GSCB also monitored reports of suspicious cyber-activity experienced by New Zealand. As a result, advisories on threats and security risks were provided to organisations through security information exchanges and direct engagement.

Security and stability in the South Pacific

In 2013/14, GCSB maintained reporting lines focusing on regional trends and resource issues.

Statements on Interception Warrants

A total of 19 interception warrants were in force during the 2013/14 year.

A total of 14 interception warrants were issued during the 2013/14 year.

Statements on Access Authorisations

A total of 59 access authorisations were in force during the 2013/14 year.

A total of 48 access authorisations were issued during the 2013/14 year.

Errors contained in the 2012/13 annual report

On 20 February 2014, an erratum was tabled in Parliament advising that GCSB's annual report for the 2012/13 financial year contained errors relating to the number of interception warrants and access authorisations issued and in force during the period.

The errors occurred due to a misunderstanding of the information required, and a miscount resulting from all the relevant material not being stored in a single repository.

The Inspector-General of Intelligence and Security inquired into the errors contained in the annual report, concluding that adequate safeguards had or were being put in place to avoid recurrence and that the risk of recurrence was negligible. The report into the inquiry can be viewed on the Inspector-General's website (www.igis.govt.nz).

Advice and assistance provided to other entities

During the 2013/14 year, there were 17 instances where the Director GCSB approved the provision of advice and assistance in accordance with section 8C of the GCSB Act. In each case, the advice and assistance was approved for a period of time associated with operational needs.

Organisational health and capability

Performance Improvement Framework review

GCSB, along with the other core NZIC agencies, had their first Performance Improvement Framework (PIF) review in 2013/14. The findings of the PIF review confirmed GCSB's own assessment and that of other recent external assessments (e.g. the Compliance Review). GCSB and the wider NZIC agree with the performance challenges identified by the PIF reviewers and will continue to work together as a community to prioritise and implement the PIF recommendations.

Expansion of Intelligence Community Shared Services

In April 2013, GCSB and NZSIS collaborated on the establishment of a business unit called Intelligence Community Shared Services (ICSS) to provide financial, procurement, human resources, learning and development, facilities and physical security services, as well as a Programme Management Office, to GCSB and NZSIS. The objective of ICSS was to improve efficiency, effectiveness and service levels, as well as develop greater resilience to cope with the NZIC's current and future challenges. GCSB is the employer of all staff in the ICSS team.

During 2013/14, ICSS expanded the provision of its services outside of the NZIC. In March 2014, ICSS commenced providing a mix of human resource advice and specialised services such as organisational development to the Ministry of Defence.

Improving our financial management systems

One of the goals of ICSS, when originally established, was to provide a fully integrated system for accounting and financial management. During 2013/14, ICSS developed the requirements to inform a tender process for a financial management information system (FMIS) to support both GCSB and NZSIS, and as a result of that tender process selected the services of an implementation provider.

The new FMIS will enable manually intensive supplementary systems currently in use to be disestablished, give budget managers improved tools for financial management and allow for the exploitation of organisational information by gathering data from where it is held and efficiently delivering it to managers and decision-makers. The new FMIS is scheduled to go live in March 2015.

During 2013/14, ICSS made good progress on integrating the capital and asset management intentions of GCSB and NZSIS. A single capital asset policy was implemented, ensuring consistent accounting treatment and identical capital practice (e.g. for acquisition and disposal) across the community. In addition, both agencies are committed to working towards a Joint Asset Management Committee over the longer term. One of the purposes of the Committee will be to approve further areas where the community can leverage off its combined capability – i.e. the community will

maintain independent operational capability where it makes sense to do so, but will seek to combine common technology to gain efficiencies and potential cost savings.

During 2013/14, ICSS also developed a single procurement policy for GCSB and NZSIS, bringing the community in line with the Government Rules of Sourcing to show accountability for the use of public funds and to ensure successful outcomes from procurement processes. As is consistent with Rule 13 of the Government Rules of Sourcing, the procurement policy allows for some appropriate opt-out exceptions in order for the agencies to maintain operational security.

Workforce planning

One of the key collaborative initiatives being pursued by the NZIC is a goal of 'One Intelligence Workforce'. This goal will be achieved when staff movement across the agencies for career development is normal, facilitated and expected and extends past the core NZIC agencies into the wider national security sector.

In October 2013, GCSB and NZSIS approved the *One Workforce Strategy* which contains a number of initiatives, to be implemented over a two year period. These will not only facilitate lateral movement across agencies, but also develop careers more broadly in the NZIC.

One of the key enablers for these initiatives is an ICSS-led project to deliver a single remuneration model for GCSB and NZSIS. This will ensure that jobs are equitably sized, and that the pay ranges applied to job sizes will be the same for both agencies. Throughout the course of the 2013/14 year there was an ongoing project to evaluate every role in both agencies using a single evaluation methodology.

In addition, ICSS has run a separate but related project to design the philosophy, principles and framework under which GCSB and NZSIS people will be paid. It has been a deeply consultative project and at the end of the reporting period engagement was still continuing and will do so well into the 2014/15 year. Implementation is anticipated to commence in the last quarter of 2014/15.

The move to a single remuneration model has been supported by the installation of the same software solutions for both GCSB and NZSIS. In the 2014/15 financial year, the two payroll systems will be integrated onto a new single human resources management information system which will improve internal and external management reporting, increase automation of business processes and reduce administrative and support system costs.

To facilitate movement of staff across the community a career pathways project commenced in May 2014. When fully implemented, in the course of 2015/16, this will result in all NZSIS and GCSB job families having defined career progression opportunities that are transparent and provide staff with the opportunity to identify and drive their career within NZIC.

The *One Workforce Strategy* is also very much future focused and concerned with ensuring workforce capability over the longer term. During 2013/14 ICSS delivered a combined GCSB and NZSIS succession planning capability and commenced work to create individualised development plans for all tier three managers in order to prepare

them for future leadership positions. This will be extended to all tier four managers during the next reporting period.

Equal employment opportunities

The NZIC is a committed equal opportunity employer. It endeavours to ensure that all employees have equal access to employment opportunities and fosters non-discriminatory practices in its recruitment processes.

The NZIC employs on merit and the ability to meet the required security clearance, which involves extensive vetting. As a result of the latter, the NZIC workforce is less diverse than the rest of the public sector in respect of ethnicity and nationality. This is because it is more difficult to confirm the personal information of people who have not been resident in New Zealand for a long period of time.

The GCSB has 36 percent female and 64 percent male employees, compared with the public sector average of 59 percent female and 41 percent male employees. Women hold 36 percent of senior management positions.

GCSB has employment policies to ensure that the varied needs of its employees are met. For example, a number of staff have flexible working hours and arrangements so they are able to balance work with other commitments, and depending on their circumstances some employees are entitled to a childcare subsidy.

GCSB STAFF	2012	2013	2014
Staff turnover	6.5%	7.7%	12.1%
EEO information			
Female	32%	40%	36%
Male	68%	60%	64%
NZ European	53%	48%	52%
Maori	6%	6%	6%
Pacific Island	3%	5%	2%
Other/undeclared	38%	41%	40%
Equivalent full-time staff at 30 June	294	304.6	315.7

During 2013/14, ICSS examined the representation of Pacific Island and Maori people, as well as women in leadership roles, in GCSB and NZSIS. Learnings from this exercise will be reviewed, and incorporated where appropriate, into the *One Workforce Strategy*.

Climate survey

The *One Workforce Strategy* outlined that a joint approach would be undertaken to delivering the Climate and Engagement Survey for both GCSB and NZSIS. The delivery of the survey was initially scheduled to take place in the first quarter of the 2014 calendar year. However, due to the intense level of change occurring within the NZIC,

a decision was made by the leadership teams of both agencies to defer the launch of the survey until September 2014. In addition to GCSB and NZSIS staff, the survey will now be expanded to include staff from the Security Intelligence Group of DPMC.

Financial Statements

Independent Auditor's Report

AUDIT NEW ZEALAND
Mana Arotake Aotearoa

Independent Auditor's Report

To the readers of the Government Communications Security Bureau's financial statements for the year ended 30 June 2014

The Auditor-General is the auditor of the Government Communications Security Bureau (the Bureau). The Auditor-General has appointed me, Kelly Rushton, using the staff and resources of Audit New Zealand, to carry out the audit of the financial statements of the Bureau on her behalf.

We have audited:

- the financial statements of the Bureau on page 28, that comprise the statement of departmental expenses and capital expenditure against appropriation for the year ended 30 June 2014.

Opinion

In our opinion:

- the statement of expenditure and appropriation of the Bureau on page 28 fairly reflects the Bureau's expenses and capital expenditure incurred for the financial year ended 30 June 2014 against the Bureau's appropriation for that financial year.

Our audit was completed on 30 September 2014. This is the date at which our opinion is expressed.

The basis of our opinion is explained below. In addition, we outline the responsibilities of the Director and our responsibilities, and we explain our independence.

Basis of opinion

We carried out our audit in accordance with the Auditor-General's Auditing Standards, which incorporate the International Standards on Auditing (New Zealand). Those standards require that we comply with ethical requirements and plan and carry out our

audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

Material misstatements are differences or omissions of amounts and disclosures that, in our judgement, are likely to influence readers' overall understanding of the financial statements. If we had found material misstatements that were not corrected, we would have referred to them in our opinion.

An audit involves carrying out procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on our judgement, including our assessment of risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, we consider internal control relevant to the Bureau's preparation of the financial statements that fairly reflect the matters to which they relate. We consider internal control in order to design audit procedures that are appropriate in the circumstances but not for the purpose of expressing an opinion on the effectiveness of the Bureau's internal control.

An audit also involves evaluating:

- the appropriateness of accounting policies used and whether they have been consistently applied;
- the reasonableness of the significant accounting estimates and judgements made by the Director;
- the adequacy of all disclosures in the financial statements; and
- the overall presentation of the financial statements.

We did not examine every transaction, nor do we guarantee complete accuracy of the financial statements.

We have obtained all the information and explanations we have required and we believe we have obtained sufficient and appropriate audit evidence to provide a basis for our audit opinion.

Responsibilities of the Director

The Director is responsible for preparing:

- financial statements that:
    - comply with generally accepted accounting practice in New Zealand;
    - fairly reflect the Bureau's financial position, financial performance, cash flows, expenses and capital expenditure incurred against each appropriation and its unappropriated expenses and capital expenditure.

The Director is also responsible for such internal control as is determined is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error. The Director is also responsible for the publication of the financial statements, whether in printed or electronic form.

The Director's responsibilities arise from the Public Finance Act 1989.

Responsibilities of the Auditor

We are responsible for expressing an independent opinion on the financial and reporting that opinion to you based on our audit. Our responsibility arises from section 15 of the Public Audit Act 2001 and the Public Finance Act 1989.

Matters Relating to the Electronic Presentation of the Audited Financial Statements and Statement of Service Performance

This audit report relates to the financial statements and statement of service performance of the Government Communications Security Bureau (GCSB) for the year ended 30 June 2014 included on the GCSB's website. The Director is responsible for the maintenance and integrity of the GCSB's website. We have not been engaged to report on the integrity of the GCSB's website. We accept no responsibility for any changes that may have occurred to the financial statements and statement of service performance since they were initially present on the website.

The audit report refers only to the financial statements and statement of service performance named above. It does not provide an opinion on any other information which may have been hyperlinked to or from the financial statements and statement of service performance. If readers of this report are concerned with the inherent risks arising from electronic data communication they should refer to the published hard copy of the audited financial statements and statement of service performance and related audit report dated 30 September 2014 to confirm the information included in the audited financial statements and statement of service performance presented on this website.

Legislation in New Zealand governing the preparation and dissemination of financial information may differ from legislation in other jurisdictions.

Independence

When carrying out the audit, we followed the independence requirements of the Auditor-General, which incorporate the independence requirements of the External Reporting Board.

Other than the audit, we have no relationship with or interests in the Bureau.

Kelly Rushton
Audit New Zealand
On behalf of the Auditor-General
Wellington, New Zealand

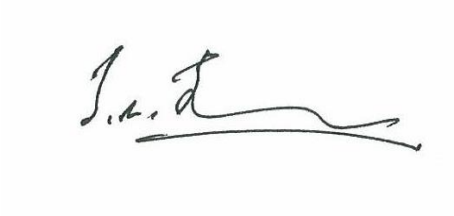
Statement of Responsibility

In terms of sections 35 and 37 of the Public Finance Act 1989, I am responsible as Director of the Government Communications Security Bureau ("GCSB"), for the preparation of GCSB's financial statements and the judgments made in the process of producing those statements.

I have the responsibility of establishing and maintaining, and I have established and maintained, a system of internal control procedures that provide reasonable assurance as to the integrity and reliability of financial reporting.

In my opinion, these financial statements fairly reflect the financial position and operations of GCSB for the year ended 30 June 2014.

The forecast financial statements of GCSB have been prepared in accordance with the requirements of the Public Finance Act 1989, which includes the requirement to comply with new NZ Public Benefit Entities standards effective 1 July 2014. These forecast financial statements fairly reflect the forecast financial position and operations of the department for the financial year to which they relate.



Ian Fletcher, Director GCSB

30 September 2014

Countersigned by:

Karen Robertson, Chief Financial Officer

30 September 2014

Statement of expenses and capital expenditure against appropriation for the year ended 30 June 2014

Section 7A of the Public Finance Act 1989 (PFA) requires a single line appropriation for the Intelligence Departments and incorporates both the operating expenses and the capital expenditure to be incurred.

In accordance with the PFA Section 45E, I report as follows:

	$000
Total appropriation	$72,692
Actual expenditure	$66,972

The "Total Appropriation" in the table above incorporates both operating expenses and the agreed capital contributions forecast for the year. The "Actual Expenditure" includes the actual operating expenses and the actual capital expenditure incurred. Under the current legislation, section 24 of the PFA also allows departments to invest their working capital into the replacement of capital assets.

Statement of unappropriated expenditure

The Operating Expenses was within appropriation, and there was no unappropriated expenditure for the year ended 30 June 2014.