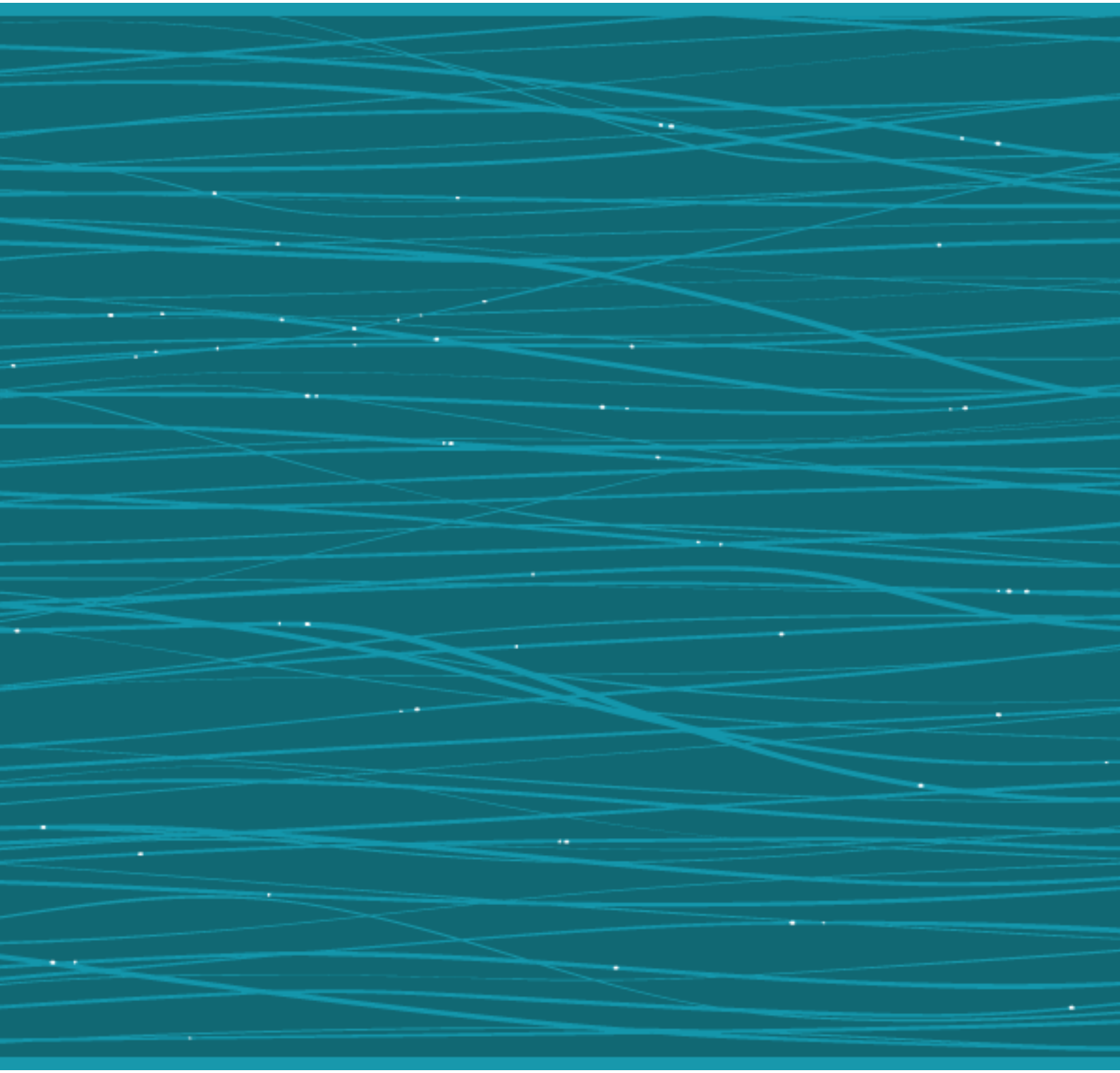
G56

ANNUAL REPORT 2013

FOR THE YEAR ENDED 30 JUNE



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)

This work is licensed under the Creative Commons Attribution 3.0 New Zealand licence. In essence, you are free to copy, distribute and adapt the work, as long as you attribute the work to the Crown and abide by the other licence terms. To view a copy of this licence, visit http://creativecommoncs.org/licences/by/3.0/nz/. Please note that no departmental or governmental emblem, logo or Coat of Arms may be used in any way that infringes any provision of the Flags, Emblems, and Names Protection Act 1981. Attribution to the Crown should be in written form and not by reproduction of any such emblem, logo or Coat of Arms.

Cover and banner illustration © istockphoto.com/friztin

LETTER OF TRANSMITTAL

Prime Minister,

I have the honour to present to you the Annual Report of the Government Communications Security Bureau for the year ended 30 June 2013.

Ian Fletcher
Director

PREFACE

This is the unclassified version of the Annual Report of the Government Communications Security Bureau for the year ended 30 June 2013. It differs from the classified version of the report which was delivered to the Prime Minister, 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.

CONTENTS

Letter of Transmittal I

Preface II

Director's Overview V

Part One – Overview

Our Operating Environment 2
The Government Communications Security Bureau (GCSB) 3
The Wider New Zealand Intelligence Community 5
Leveraging Partnerships 6

PART TWO – 2012/2013 PRIORITIES

Foundational Changes 9
Organisational Health & Capability 11
Activities Over the Reporting Period 13

Part Three – Review of Operational Performance

Impacts 18
Statements on interception warrants 22
Statements on access authorisations 22
Co-operation with other entities to facilitate their functions 23

Part Four – Financial Statements

Independent Auditor's Report 25
Statement of Responsibility 29
Statement of expenses and capital expenditure 30
Statement of unappropriated expenditure 30

DIRECTOR'S OVERVIEW

2012/13 has been dominated by the Department's disclosure of unlawful surveillance, and the subsequent events that have played out in public, through the courts, and a Police investigation.

Within the Department, Rebecca Kitteridge's review has led to a significant internal change programme to strengthen legal and procedural compliance.

Externally, the same events led Government to conclude, as the Kitteridge review did, that the Government Communications Security Bureau Act 2003 as it then stood was fundamentally not fit for purpose. Government amendments to the legislation took effect on 27 September 2013.

The Department's management team and structure has been strengthened. Our top and middle management layers are now substantially stronger and more diverse in talent and experience than was previously the case. This investment is already beginning to pay dividends as the legislative and review implementation processes unfold; the Department is also now beginning to turn its mind to its operational strategies and priorities for the coming period.

It's clear that, having put strengthened compliance, oversight and policy processes in place, the Department needs to look afresh at its delivery of both information assurance/cyber and intelligence products to government. This reflects the changing environment within New Zealand and externally, and the resource pressures faced by all departments.

Our thinking about this is being informed by the first Performance Improvement Framework (PIF) review for the core New Zealand Intelligence Community. We have also undertaken a survey of our customers, as we identify ways to improve our service delivery. Looking forward, we are working on a series of product and service improvements which will reflect the feedback that this survey and the PIF review will provide for us.

The combination of the customer survey and the PIF review is a valuable foundation for improvements. Taken together with the compliance, policy and legislative reform, the result is an opportunity for the Department's products and services to reflect the security and intelligence environment which New Zealand faces now and into the future.

DIRECTOR'S OVERVIEW

That environment continues to present a number of real, but not necessarily obvious, challenges. These include:-

The rapid take up of advanced digital services using Internet protocol-based networks has led to an explosion in economically valuable services offered and delivered over the Internet. It has also led to an explosion of opportunity for cyber borne espionage, crime and (increasingly) aggression.

* New Zealand's open economy, and growing economic engagement with emerging markets in the Asia-Pacific region mean that New Zealand's security interests and its economic interests are not automatically the same; this puts a premium on providing government with strong information assurance and cyber defence, and on the development and deployment of effective security and intelligence capabilities to enable New Zealand to identify, advance and defend its interests in a more complex and less stable global, political and economic environment.
* These challenges extend increasingly across New Zealand's economy and society, as these issues apply almost as significantly to major economic actors as they do to the mechanisms and information requirements of government itself.

Against these challenges, the Department needs to continue to work hard to develop a combination of compliance, customer focus and delivery, and constant adaptation to a rapidly evolving operating environment. The Department now has a good understanding of these issues, a strong team in place, and a growing sense of how to tackle these challenges in the years ahead.

Ian Fletcher
Director
Government Communications Security Bureau

Part One
Overview

1

PART ONE – OVERVIEW

Our Operating Environment

For New Zealand to be a safe and prosperous country, its national interests must be protected from harm. Increasingly, threats to our interests do not respect national boundaries, and individuals and groups can carry out events that cause New Zealand harm without ever needing to set foot on our shores.

Cyber capabilities are spreading rapidly. In many respects this is a positive development as the rise of internet technologies, and the global interconnectivity which this brings, are of immense social and economic value to New Zealanders. But cyber capabilities also enable hostile actors to use information systems or computer technology to gain unauthorised access to, or direct malicious activity against, our computers, networks, and communications.

New Zealand's government, as well as many economic and intellectual property generators, are subject to systematic cyber intrusion, and these intrusions are increasing in scale and sophistication. Government departments hold vast amounts of personal information about New Zealanders, and the public expect service delivery from government that is increasingly digital, responsive and personalised. New Zealanders need to have confidence that the information that they share with government is transmitted securely, and that there are appropriate safeguards to protect it from loss or misuse.

Furthermore, New Zealand firms have achieved success in a number of industries through their creation of innovative and leading-edge technology and processes. This makes them highly attractive targets for economic espionage. From the attacker's perspective it is cheaper, and often less difficult, to steal intellectual property than to develop it. While economic losses from cyber intrusion are currently unquantified, based on the experience of our overseas partners we believe they are likely to be significant and affect New Zealand not just in the short-term, but over the long-term with potential loss of competitiveness and markets.

The Government is pursuing an independent foreign policy programme that contributes to global and regional stability. To achieve this, our decision-makers need to be well-informed on foreign, political, economic and defence-related issues from here and overseas. They require access to information that helps clarify their understanding of events and issues, in order to develop and support decisions that protect and advance New Zealand's interests.

PART ONE – OVERVIEW

The Government Communications Security Bureau (GCSB)

GCSB's Mission

To inform and enhance the decision-making processes of the New Zealand Government in the areas of information assurance, national security, foreign policy, and support to law enforcement by:

* Ensuring the integrity, availability and confidentiality of official information through the provision of information assurance services to government.
* Improving the protection of the national critical infrastructure from cyber threats.
* Providing foreign intelligence to support and inform government decision-making.
* Providing an all-hours intelligence watch-and-warn service to government.

Outcomes

In the Joint Statement of Intent 2012-2016, the agencies that comprise the New Zealand Intelligence Community (NZIC) specified that they would assist Ministers and other departments in achieving the Government's priority of building a safer and more prosperous New Zealand by contributing to three outcomes:

1. New Zealand is protected from harm.
2. New Zealand's decision-makers have an advantage.
3. New Zealand's international reputation and interests are enhanced.

Impacts

GCSB's contribution to the outcomes is provided through these NZIC impacts:

* New Zealand's vulnerabilities are identified and reduced.
* Increased security for New Zealand deployments.
* New Zealand policy-makers are well-informed on foreign political and economic issues.
* New Zealand is safe-guarded against threats of espionage and violent extremism.

GCSB Outputs

As outlined in the GCSB's Output Plan and Agreement 2012/13, GCSB's contribution is provided through five outputs:

1. Foreign intelligence reports;
2. Intelligence alerts and warnings;
3. Policy and support;
4. Advice and services; and
5. Cyber security operations.

The Organisation

The GCSB's head office is located at Pipitea House on Pipitea Street in Wellington. The 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.

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

Director and Board

The Director of the GCSB since January 2012 is Ian Fletcher. The Director is supported by an internal Board comprising the:

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

The Board's principal duties are to focus on:

- setting and monitoring the GCSB's strategic direction;
- identifying and responding to strategic risks;
- considering where resources should be applied to achieve the GCSB's and the wider NZIC's objectives;
- workforce capability;
- monitoring major projects; and
- monitoring the departmental budget and ensuring adequate financial controls are in place.

Risk and Audit Committee

The Risk and Audit Committee is an independent committee reporting directly to the Director. The Committee re-formed early in 2013 after a three-year hiatus (since June 2010), and met twice in the 2012/13 financial year.

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;

1 The Strategic Communications Manager is an employee of the Department of the Prime Minister and Cabinet.

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

Responsible Minister

The Prime Minister is the Responsible Minister for the GCSB.

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.

The 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 the GCSB and the New Zealand Security Intelligence Service (NZSIS), and in particular:

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

The Wider New Zealand Intelligence Community

The GCSB, along with the National Assessments Bureau (NAB) within the Department of the Prime Minister and Cabinet (DPMC), and the NZSIS, form the core New Zealand Intelligence Community (NZIC). The Intelligence Coordination Group (ICG), also within DPMC, assists the intelligence agencies in the coordination of their work.

There are other intelligence capabilities too. The New Zealand Defence Force also has intelligence capabilities in the Directorate of Defence Intelligence, and in GEOINT New Zealand as well as in the individual services.

There are intelligence units in the New Zealand Police, the New Zealand Customs Service, and Immigration New Zealand. 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.

Some of the other threats that the wider NZIC seeks to mitigate include:

Transnational organised crime

Transnational organised crime is a serious and growing security threat to New Zealand and its interests. Transnational organised criminals exploit a wide range of vulnerable markets: illicit drugs, money laundering, technology-enabled fraud, and identity crime pose the biggest threats.

Threats to natural resources and the environment

Activities such as illegal, unreported and unregulated (IUU) fishing result in widespread environmental, social and economic consequences. IUU fishing distorts competition, and jeopardises the economic survival of those who fish legitimately. This is a significant concern for New Zealand where the fishing industry is a large employer, and seafood exports consistently rank as New Zealand's fourth or fifth largest export earner.

Weapons of mass destruction (WMD)

A wide range of seemingly benign industrial goods, technology and expertise can assist would-be proliferators of weapons of mass destruction. Ongoing attempts to acquire controlled and dual-use technology from New Zealand presents our greatest single proliferation-related threat.

Fragile and failing states

Fragile states impact on New Zealand's security and economic prosperity with instability potentially undermining the health of New Zealand's trade-driven economy. New Zealand's reaction to the problem of fragile and failing states could involve humanitarian, law enforcement and other forms of development assistance, through to the deployment of troops for peacekeeping purposes.

Leveraging Partnerships

It is not possible for the GCSB, as currently resourced, to collect foreign intelligence on all threats to New Zealand's national security interests. However, the GCSB is able to have far greater visibility of risks because of our access to global sources of high-quality intelligence through long-standing and close intelligence partnerships.

New Zealand is a member of an arrangement for sharing intelligence along with Australia, Canada, the United Kingdom and the United States of America (referred to as the 'Five-Eyes'). This helps compensate for our small size and lack of global reach, and enables New Zealand to be a better informed player on the world stage than would otherwise be the case. Given the costs of intelligence collection, being a member of the

PART ONE – OVERVIEW

Five-Eyes provides a very substantial net economic benefit to New Zealand.

2 Part Two
2012/2013 PRIORITIES

PART TWO – 2012/2013 PRIORITIES

Foundational Changes

Review of compliance

Following the September 2012 discovery of unlawful intercept, the Director and the DPMC Chief Executive initiated a review of compliance at the GCSB. Rebecca Kitteridge was seconded to the GCSB as Associate Director to undertake the review, which took into account the GCSB's activities, systems and processes since 1 April 2003 (the date the Government Communications Security Bureau Act 2003 came into force).

Ms Kitteridge's report was released by the Government on 9 April 2013. It highlighted a longstanding lack of good systems and processes in relation to compliance, as well as underlying organisational problems for the GCSB. The report made 80 recommendations - 76 of which the GCSB were directly responsible for implementing. The recommendations fell into seven broad areas:

* compliance (29 recommendations);
* oversight (3 recommendations);
* information management (9 recommendations);
* legal capability and capacity (9 recommendations);
* measurement and reporting (4 recommendations);
* organisation structure and culture (20 recommendations); and
* outreach capability and capacity (2 recommendations).

The Director accepted all recommendations, and committed to publicly reporting each quarter on the progress that had been made in implementing them.

At the end of June 2013 the Director issued a report saying that 25 of the recommendations had been fully-implemented. These recommendations focused on the things that needed to be put in place immediately in order for the GCSB 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, Chief of Staff, Chief Legal Advisor and the Compliance and Policy Manager.

Since the end of this reporting period the Director has issued a second quarterly update stating that an additional 9 recommendations have been fully-implemented, bringing the total to 34. A further 8 recommendations have been partially implemented, and work is underway on more than 15 others.

Some of the recommendations will take well into the 2013/14 year to implement, as they involve longer-term programmes including staff rotation, external secondments and performance management practices.

Inquiry by the Inspector-General of Intelligence and Security (IGIS)

Following the September 2012 discovery of unlawful intercept, the Director wanted to ensure that no other similar breaches had occurred. This led to instances where the GCSB had provided assistance to domestic agencies between 1 April 2003 and 26 September 2012 being referred to the IGIS for review.

The cases referred to the IGIS involved a total of 88 New Zealanders, and were based on issues including potential WMD development, people smuggling, foreign espionage in New Zealand, and drug smuggling.

The IGIS formed the view that there were arguably no breaches by the GCSB in the cases involving the 88 individuals, although the law was unclear and the IGIS recommended amending it. The IGIS also made a further recommendation regarding the need for some improvement in the precision of the GCSB's paperwork.

Legislation amendments

The GCSB function is governed by the Government Communications Security Bureau Act 2003. Oversight of the GCSB is governed by the Inspector-General of Intelligence and Security Act 1996 and the Intelligence and Security Committee Act 1996.

During 2012/13, the Government proposed an omnibus bill significantly amending all three statutes. This amending legislation was enacted on 26 August 2013, to take effect on 27 September 2013.

In relation to the GCSB Act, the amendments made changes to the objective, functions, and limitation provisions to improve clarity about the legal basis for the GCSB's activities and to accommodate changes in the prevailing security environment, particularly in relation to cyber security and information security. For the first time the GCSB is required to formulate a policy on personal information and the Privacy Commissioner has a new oversight role, both in the development and review of that policy and also subsequent audits of compliance.

Importantly, the restriction that has always prevented the GCSB from targeting New Zealanders remains in place in respect of foreign intelligence gathering.

In relation to the Inspector-General of Intelligence and Security Act, the amendments strengthened the office of the IGIS, increasing the resources of the office to enable a greater range of activities to be carried out, expanding the IGIS's statutory work programme and enhancing the corresponding reporting requirements.

In relation to the Intelligence and Security Committee Act, the amendments improved the Committee's ability to provide effective oversight

and accountability of the intelligence agencies. As part of this, the Committee will now conduct a financial review of the intelligence agencies in public. The amendments to this Act also require periodic reviews of New Zealand's intelligence and security agencies, the legislation governing them and their oversight legislation, with the first review due to commence in 2015.

Organisational Health & Capability

Increasing staff capability

The GCSB remains a fundamentally technical agency, and an on-going priority is to ensure that staff have the capability to provide security and advice services, and derive intelligence in a rapidly evolving telecommunications environment. Because of the nature of the work undertaken by the GCSB, there is a limited ability to access training opportunities from external providers.

In 2012/13, the GCSB delivered a four week full-time technical training programme to approximately 40 staff. This internally developed training programme remains the most comprehensive staff education scheme undertaken by the GCSB in recent years.

Knowledge management

The compliance review made a number of recommendations relating to the GCSB's management of information. The GCSB committed to implementing all recommendations, and as its first step migrated all file stores into an electronic document records management system. This is ensures that all information is located in one central repository that is secure and discoverable, and that there is appropriate oversight of files and records.

Performance Improvement Framework self-review

Towards the end of the 2012/13 year, the GCSB commenced a self-review process to assess how well it had identified and responded to current government priorities; how effectively and efficiently it had delivered on core business; and to review its capability in key operational management areas: leadership, direction and delivery; external relationships; people development; and financial and resource management. This self-review was the pre-cursor to the Performance Improvement Framework review of the NZIC that will be undertaken in the 2013/14 year.

Equal employment opportunities

The GCSB recognises that understanding and knowledge of different perspectives enhances the performance of its employees and hence the organisation as a whole. The GCSB endeavours to ensure that all employees have equal access to employment opportunities, and fosters non-discriminatory practices in its recruitment procedures.

The GCSB 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 40 percent female and 60 percent male employees, compared with the public sector average of 59 percent female and 41 percent male employees. Women hold 35 percent of management positions.

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

GCSB Staff	2011	2012	2013
Staff Turnover	6.9%	6.5%	7.7%
EEO Information			
Female	30%	32%	40%
Male	70%	68%	60%
NZ European	48%	53%	48%
Maori	7%	6%	6%
Pacific Island	2%	3%	5%
UK	9%	10%	10%
Asian	2%	3%	3%
Indian	1%	1%	1%
Undeclared	31%	24%	27%
Equivalent full-time staff at 30 June	286	294	304.6

and depending on their circumstances some employees are entitled to a childcare subsidy.

Climate survey

The GCSB intended to carry out a staff climate survey in mid 2012/13. This was deferred until March 2014 when the GCSB and the NZSIS will undertake a joint staff survey.

Activities Over the Reporting Period

Co-location project

In March 2013, the relocation of the NZSIS into Pipitea House on Pipitea Street was completed. Pipitea House now hosts the GCSB and NZSIS, as well as elements of the DPMC.

Co-location was a significant project for the NZIC, and involved input from all business areas. For example, a significant amount of ICT resource went into ensuring common printing, resources, classified and unclassified telephony and video teleconferencing, and networking for all Pipitea House occupants.

Although undertaken partly out of necessity in order to align the support functions of the NZSIS and the GCSB, co-location also signalled the commitment of both agencies to work towards integration, to the maximum extent consistent with our different roles and legislation, in order to achieve more efficient and effective outcomes.

As a result of co-location Pipitea House is being fully utilised, and this has identified the need to develop a long-term accommodation strategy for the wider NZIC. This will be progressed as part of the next stage of our joint planning.

Intelligence Community Shared Services

In April 2013, the NZIC implemented Intelligence Community Shared Services (ICSS) as a response to the Government's challenge to deliver better public services. This model for corporate support services combined the GCSB's and the NZSIS's human resources, learning and development, finance, facilities, procurement and physical security functions.

The objective of ICSS was to improve efficiency, effectiveness and service levels, as well as greater resiliency to cope with the NZIC's current and future challenges. Essentially, ICSS enables the NZIC to make each corporate support area greater than the sum of the parts.

The GCSB is the employer of all employees in the ICSS group. A single employer provided an opportunity to standardise terms and conditions of employment for a large proportion of staff, and it also reduced the likelihood of increased administrative and management costs.

Establishing and implementing ICSS was a very ambitious project, and it was undertaken during a period of considerable change for the GCSB. Despite this, most key deliverables of the project were achieved on time, and ICSS has made some significant progress to support the NZIC's strategic capability, as well as efficiencies and service improvements.

The ICSS introduced a new joint orientation programme which provides new members to the GCSB and the NZSIS with a detailed strategic and operational view of both organisations, and serves to promote a culture of cooperation and shared purpose between the two organisations.

The ICSS also developed a NZIC community orientation programme to provide new NZIC staff with a greater understanding of the NZIC as an integrated community, while also providing a greater depth of knowledge on the specific roles and functions of the individual agencies.

A number of ICSS initiatives that were intended to be delivered in the 2012/13 year were delayed, primarily due to the capability not being in place to progress them. For example, although some work was undertaken to progress the NZIC Workforce Strategy, it will not be finalised until the new Manager Organisational Development and Performance joins ICSS in the next financial year.

In 2013/14, the NZIC will explore incorporating the GCSB's and NZSIS's separate security functions in to a single capability. Mutual confidence and assurance about our security standards and behaviour of our staff, together with security integrity of our information are critical areas that could significantly benefit from greater collaboration.

In its first 3 months of operation, ICSS:

- *delivered 26 training courses to 328 participants, totalling 6,838 hours of learning*
- *advertised 38 positions; processed 413 job applications; finalised the recruitment for 22 staff*
- *drafted 8 joint policies*
- *received 2,010 visitors to Pipitea House, including 108 international visitors*
- *facilitated 337 meetings and 57 conferences.*

National Cyber Security Centre

As directed in the National Cyber Security Strategy of June 2011, the GCSB established the National Cyber Security Centre (NCSC) in September 2011 to protect government systems and information, plan for and respond to cyber incidents, and to work with providers of critical national infrastructure to improve the protection and

computer security of such infrastructure against cyber-borne threats.

In 2012/13, the GCSB undertook work to develop the capability of the NCSC in accordance with Cabinet direction.

Customer and partner survey

2012/13 was the first year that the GCSB undertook a comprehensive customer and partner survey. The survey was designed to provide insight into customer and partner perspectives of the GCSB, and the products and services it had produced over the previous 12 month period.

The survey responses fell broadly into three themes. Respondents:

- expressed a desire for the GCSB to provide greater education about the extent of our authority and responsibility; the types of products and services we can provide; and, how they can access assistance from us.
- want the GCSB to improve our level of engagement with them. In particular, customers want the opportunity to have regular and sustained contact to ensure that we understand their priorities and requirements, and how our product and services are incorporated into their business activities.
- told us that they would like the GCSB to improve its responsiveness to requests for advice and assistance.

The survey included a question where respondents were asked to rate their agreement with five statements about the GCSB's products/services and performance. This question allowed the GCSB to benchmark its current levels of performance, and the ability to analyse trends over time as the survey is repeated. Table One shows the average results for each statement – where 5 equalled strongly agreed and 1 equalled strongly disagreed.

Table One – Average results for product/service performance statements:

	GCSB's products and services are:			GCSB:	
	Unique	Timely	High quality	is flexible and responsive	Engages effectively with my organisation
Average	4.65	3.28	4.14	3.35	3.47

The results of the customer and partner survey are informing our strategic change programme, and the GCSB intends to repeat the survey periodically to check how we are progressing.

Increasing the connectivity of NZIC's customers

The GCSB provides secure communications network connectivity and services for the NZIC. During 2012/13 the GCSB enhanced the network connectivity to address customer needs. Further future enhancements will take into account feedback received in the customer and partner survey.

Part Three – Review of **Operational Performance**

3

PART THREE – REVIEW OF OPERATIONAL PERFORMANCE

Impacts

The agencies that comprise the NZIC undertake activities and produce outputs in order to achieve the five joint impacts as stated in the Outcome Framework (***2012/16 NZIC Statement of Intent*** refers). The extent that 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.

During 2012/13, resourcing and implementing the compliance review recommendations and amended legislation required many of the GCSB's analytical staff to be redirected to these activities. (Recruitment would have taken too long, and business knowledge was essential.) This did have an effect on output, and some lower-priority activities were reduced or stopped.

The following section reports how the activities undertaken and outputs produced by the GCSB in 2012/13 contributed to the five joint NZIC impacts.

New Zealand's vulnerabilities are identified and reduced

Through the provision of cyber and intelligence reporting, threat alerts, and cooperation with New Zealand Government partners, the GCSB's products and services enabled the Government to identify and mitigate vulnerabilities in the nation's security, including protection of critical infrastructure.

The NCSC delivered a range of education initiatives to help increase New Zealand organisations' preparedness to respond to cyber incidents. Working with trainers from the United States based Computer Security Incident Response Team (CSIRT) Program of Carnegie Mellon University's Software Engineering Institute, staff from the NCSC provided cyber incident response training to staff from 38 national critical infrastructure organisations and other private sector operators. The lessons learned in the training will help increase the resilience of our information networks and critical infrastructures and also helps set up trusted communication channels and collaboration across New Zealand.

An agreement was reached with the Wellington Institute of Technology (WelTec) to periodically deliver a one-week Fundamentals of Information Assurance and Security programme. This is an NZQA registered programme delivered at a second-year university level. Although designed for government agencies and information security practitioners, this is a public programme and, over time, is expected to improve information assurance and cyber security capabilities nationally.

Staff from the NCSC also worked with a group of New Zealand critical infrastructure organisations

to establish the New Zealand Cyber Security Voluntary Standards for Industrial Control Systems. These critical infrastructure organisations operate industrial control systems, which allow centralised supervision or control of remote assets. The standards are a compilation of best practice and guidance for establishing secure control systems and will assist to minimise the threat from unauthorised or inappropriate access, and also to maintain access and control during adverse conditions. The voluntary standards are applicable to a range of New Zealand industries including electricity, oil and gas, water, transport, chemical, pharmaceutical, food and beverage, and manufacturing industries.

There have also been presentations at public conferences, including keynote addresses at the ISACA (previously known as the Information Systems Audit and Control Association) Computer Audit, Control and Security international conference in September 2012 and the Gallagher Industries international security conference in February 2013.

Cyber threat advisories were issued covering threat activity ranging from new vulnerabilities in commonly used software and operating platforms, through to information on new forms of online scams and phishing schemes. The NCSC interprets information from a wide range of sources to provide value added input in its advisory notifications.

The GCSB provided IT security advice for the New Zealand Government Cloud Programme, as well as the inquiry led by the Department of Internal Affairs into public-facing internet systems. The GCSB also participated in two cyber-security response exercises which developed government's ability to respond effectively to cyber incidents of national significance.

Through the customer and partner survey, we know that the impacts of these activities, as well as of other GCSB products and services:

* helped protect critical information;
* informed the protection of New Zealand assets; and
* helped to inform responses to security incidents.

The number of reports on suspicious cyber activity made to the NCSC continued to increase. In the first six months of 2013, 161 incidents were recorded compared with 134 incidents for the full 2012 calendar year and 90 for the 2011 calendar year.

PART THREE – REVIEW OF OPERATIONAL PERFORMANCE

Spear phishing compromise

Spear phishing emails are targeted emails which try to pass themselves off as legitimate emails with attachments containing malware, and are designed to trick the recipients into opening them. Upon doing so, malware is automatically installed on the user's computer and can then be used by the attacker for further compromises.

In one case in 2012/13, a targeted spear phishing email containing a malicious pdf file was sent to a number of email addresses. Several recipients at an organisation opened the attachment which then exploited a known vulnerability to install malware on the user's accounts.

Once the malware was installed, the "phishers" were able to access the network and get greater privileges to increase their access across the network, and then collect and extract data.

The NCSC's subsequent investigation identified instances of compromise on the organisation's network and corrective measures were applied to mitigate the risk of re-infection.

Ransomware attack on company

The NCSC received a number of "ransomware" reports in the 2012/13 year. In one case a small business reported they had received emails from outside of New Zealand threatening to disable their business unless funds were paid.

When no funds were paid, the email senders – we call them "threat actors" – compromised the business's servers, installed malware which encrypted their files, causing the owners to lose access to their systems.

Eventually the organisation was able to restore its networks using historic back-ups, however they lost many recent records and were unable to conduct business for several days resulting in financial losses.

Increased security for New Zealand deployments

The GCSB continued to provide critical support to New Zealand Defence Force (NZDF) personnel deployed overseas.

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

PART THREE – REVIEW OF OPERATIONAL PERFORMANCE

"The role of GCSB has been critical in providing force protection intelligence to our personnel. The work carried out by GCSB saved lives of NZDF personnel on a number of occasions."

Letter to Director GCSB from Chief of Defence Force Lieutenant General R.R. Jones, 22 May 2013.

New Zealand policy-makers and decision-makers are well-informed on foreign political and economic issues

The GCSB delivered against this impact through the dissemination of foreign intelligence reports which met government requirements on foreign political and economic topics, and contributed to policy formulation.

Feedback from the customer and partner survey indicated that the GCSB's foreign intelligence reports informed foreign relations and defence policy.

The availability of information assurance and cyber advice and services also gave decision-makers a greater grasp of the economic implications of malicious cyber intrusions into New Zealand communications networks. Furthermore, the customer and partner survey showed that products and services from the GCSB informed ICT and telecommunications policy.

Intelligence in Action – foreign intelligence reporting

The GCSB produced foreign intelligence reports to support New Zealand's foreign intelligence requirements as set out by the Foreign Intelligence Requirements Committee (FIRC). FIRC is responsible to the Officials Committee for Domestic and External Security Coordination (ODESC).

In 2012/13, the GCSB's foreign intelligence reporting supported specific topics of significant national interest and concern to the Government.

New Zealand is safe-guarded against threats of espionage and violent extremism

The GCSB continued to contribute to this impact across all of its operational areas.

The New Zealand SIGINT Operations Centre (NZSOC) continued to provide a 24 hour 7 day a week watch and warn service which notified customers when information was received that could affect the safety and/or security of New Zealanders and New Zealand entities both at home and abroad.

PART THREE – REVIEW OF OPERATIONAL PERFORMANCE

Intelligence in Action— The NZSOC

The NZSOC provides a 24-hour 7-day threat warning service based on the combined efforts of the Five-Eyes watch-keeping services. These bring together and fuse information from a variety of sources in order to alert customers to threats in a sufficiently timely manner.

For example, if civil unrest breaks out in a country or region where the safety of New Zealanders or interests of New Zealand are likely to be threatened, it is the NZSOC who will source the relevant information and raise the warning so that customers can take action to avoid or reduce the threat, or to manage the aftermath response to an incident.

Feedback from the Customer Survey reported that NZSOC was generally very helpful and responsive to customer needs and queries, and that NZSOC communications were effective and useful.

The NCSC monitored reports of suspicious cyber activity experienced by New Zealand organisations, and provided advisories on threats and security risks through security information exchanges and direct engagement with government organisations.

The NCSC also prepared and delivered Information Assurance training and education to government agencies in support of the New Zealand Information Security Manual.

Security and stability in the South Pacific

The GCSB's efforts focused on providing information on regional trends and resource issues.

Statements on interception warrants

A total of 11 interception warrants were in force over the 2012/13 year.

A total of 5 interception warrants were issued during the 2012/13 year.

Statements on access authorisations[2]

A total of 26 access authorisations were in force over the 2012/13 year.

A total of 11 access authorisations were issued during the 2012/13 year.

2 Under the Government Communications Security Bureau Act 2003 as originally drafted (before the recent legislative amendments), access authorisations were referred to as computer access authorisations.

PART THREE – REVIEW OF OPERATIONAL PERFORMANCE

Co-operation with other entities to facilitate their functions

From 27 September to 26 November 2013 (the day this report went to print) there have been five instances where the Director GCSB has approved the provision of advice and assistance in accordance with section 8C of the Government Communications Security Bureau Act 2003. In each case, the advice and assistance was approved for a period of time associated with operational needs.

It is not possible to report, for the 2012/13 year, the number of instances where advice and assistance was provided by GCSB under its function in section 8C, because the provision took effect from 27 September 2013.

4 Part Four
Financial Statements

AUDIT NEW ZEALAND
Mana Arotake Aotearoa

Independent Auditor's Report

To the readers of
Government Communications Security Bureau's
financial statements
for the year ended 30 June 2013

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 30, that comprise the statement of expenses and capital expenditure against appropriation for the year ended 30 June 2013.

Opinion

In our opinion the statement of expenditure and appropriation of the Bureau on page 30 fairly reflects the Bureau's expenses and capital expenditure incurred for the financial year ended 30 June 2013 against the Bureau's appropriation for that financial year.

Our audit was completed on 30 September 2013. 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 a statement of expenses and capital expenditure against appropriation that fairly reflects the Bureau's expenses and capital expenditure incurred for the financial year ended 30 June 2013 against the Bureau's appropriation for that financial year.

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 unclassified 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 statements 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 2013 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 2013 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

PART FOUR – FINANCIAL STATEMENTS

Statement of Responsibility

In terms of sections 35 and 37 of the Public Finance Act 1989, I am responsible as Chief Executive of the Government Communications Security Bureau, for the preparation of the Bureau's financial statements and the judgements 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 2013.

Ian Fletcher
Director GCSB
30 September 2013

Countersigned by

Simon Wall, CA
Chief Financial Officer
30 September 2013

Statement of expenses and capital expenditure against appropriation for the year ended 30 June 2013

Section 7(1)(g) 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	$67,925
Actual expenditure	$73,409

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 2013.

Government Communications
Security Bureau

PO Box 12-209
Wellington
New Zealand

Telephone: (04) 472 6881
Fax: (04) 499 3701
Website: www.gcsb.govt.nz

New Zealand Government