Government Communications Security Bureau

Annual Report 2016

Contents

Preface

This is the unclassified version of the annual report of the Government Communications Security Bureau (GCSB) for the year ended 30 June 2016. 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.

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

01

CHAPTER

OVERVIEW OF THE YEAR

Minister's foreword

In the past year we have had frequent and very stark reminders of the impact on the world of extremist ideologies, geopolitical instability and cyber-crime. We are not immune to these impacts.

It is in this context that the Government decided this year to make a further investment in the intelligence agencies. This investment will ensure that the agencies have the capabilities and resources to support government decision making and protect New Zealanders and New Zealand's wider interests in the years ahead.

This new investment was only possible because of the significant work the agencies have already undertaken in the past two years to strengthen their core capabilities and improve their effectiveness in meeting government priorities.

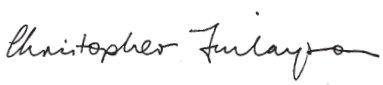
While there is more work to be done, progress to date has been very good.

It is also important to ensure that the NZSIS and GCSB's future work is underpinned by fit-for-purpose legislation and that public confidence is maintained through appropriate independent and democratic oversight. The Independent Review of Intelligence and Security (2015 Review) conducted by Sir Michael Cullen and Dame Patsy Reddy has provided useful insights into how the enabling legislation and oversight needs to develop to support the future work of the agencies. The Government subsequently introduced legislation into the House that gives effect to most of the reviewers' recommendations.

I am pleased with the efforts the New Zealand Intelligence Community (NZIC) have taken over the last year to explain the work of their agencies, the importance of what they do and how they are held accountable to the people of New Zealand. This is consistent with the Government's desire to be more open with the public about the work that the security agencies do on their behalf.

I continue to be impressed by the dedication of staff and their commitment to protecting the security and wellbeing of New Zealanders under the rule of law. Most of their work is unseen, and their achievements often unheralded, but despite that they continue to work tirelessly in the national interest.

The 2016/17 year will be another busy year for the security and intelligence agencies as they continue to build on recent progress, deliver improved value to government and adapt to the legislative changes arising from the 2015 Review. I am confident they will rise to this challenge.



Hon Christopher Finlayson
Minister Responsible for the Government Communications Security Bureau

Director's overview

Significant work has been undertaken during the past year to improve GCSB's performance and to develop many of the capabilities that are critical to our future success.

The Government's investments in the NZIC in both the financial year 2014/15 and financial year 2015/16 are underpinned by a sophisticated understanding of the connection between the outcomes government is seeking from the security agencies and the capabilities required to deliver them.

The delivery of these capabilities is captured in the NZIC Four Year Plan, which includes important changes to the way the NZIC delivers its services to government and provides value to the people of New Zealand. In alignment with the NZIC Four Year Plan, the GCSB has a new strategic plan, a document that captures our ambitions and our key deliverables through to 2020.

Our position reflects three years of hard work to strengthen GCSB and ensure it is investment-ready. We have already taken some important initial steps to build our future capability in the areas of cyber defence, intelligence collection and information technology. Over the next three years we will be leveraging this foundational work to deliver improved results for government and all New Zealanders in partnership with our NZIC colleagues.

The size and geographic location of New Zealand, coupled with the increasingly global and complex nature of the threats we face, means that collaboration is crucial to GCSB fulfilling its mission. We are working more closely with the NZSIS, New Zealand Defence Force (NZDF) and other government agencies on matters of national security – a trend that is mirrored in like-minded democracies around the world. In cyber-defence we are working with and through the private sector to detect and disrupt advanced cyber threats.

Everything GCSB does needs to be in New Zealand's interests and in accordance with the law, including human rights obligations. This is an absolute bottom-line that applies to all of our work, whether we undertake it ourselves or through others.

Our global partnerships are critical to our success. New Zealand's membership of the Five Eyes alliance generates significant benefits for New Zealand – for both intelligence sharing and capability building. Without these global partnerships, New Zealand's ability to understand and respond to events and threats offshore would be significantly constrained.

We are conscious of the need to continue to better explain the work we do in support of government and all New Zealanders. During the year we have taken a number of steps to better inform the public and our stakeholders about our work and this will continue and expand under my directorship.

Andrew Hampton
Director

Our mission

Protecting and enhancing

NEW ZEALAND'S SECURITY AND WELLBEING

Our values

RESPECT

We respect the role that each individual plays in the organisation

We value diversity in thought and approach

We treat each other with dignity

INTEGRITY

We act lawfully and ethically

We are accountable for our actions – both personally and organisationally

We act professionally and with respect

COMMITMENT

We are committed to our purpose

We are committed to excellence – recognising the contribution of our tradecraft to national security

We are committed to our customers – recognising that our success is measured in their terms

We are committed to our stakeholders – the government and people of New Zealand

COURAGE

We face facts, tell it how it is and are prepared to test our assumptions

We have the courage to make the right decisions at the right time even in the face of adversity

We are prepared to try new things, while managing the risk of failure

We perform at pace, are flexible and responsive to change

Notable achievements in 2015/16

Impenetrable infrastructure

The GCSB's National Cyber Security Centre (NCSC) provides cyber security services, including an incident response function and advice to the public and private sector. 338 cyber security incidents were logged with the NCSC during the year – an average of 28 incidents per month.

Under section 48 of the Telecommunications (Interception Capability and Security) Act 2013 (TICSA), GCSB received 69 notifications of network operator changes within areas of specified security interest. The average time for resolution was 12 working days.

There has been significant progress on the project to deliver a replacement for Cryptographic Products Management Infrastructure (CPMI), which is currently in the detailed design phase. CPMI helps ensure the security of sensitive government communications.

GCSB developed and published an Information and Communications Technology (ICT) strategic plan, which outlined the future technical direction for our system growth. This plan reflects an intelligence community enterprise view of the future that promotes collaboration and a single sector approach. This plan formed the technical basis for the New Zealand Top Secret Network (NZ TSN), an integrated set of capabilities for the secure storage and distribution of national security information for the whole New Zealand Intelligence Community.

Indispensable intelligence

In 2015/16, GCSB continued to provide regular delivery of intelligence to 19 government agencies, and to appropriate Ministers, their offices and the Leader of the Opposition. The intelligence provided includes intelligence generated by GCSB, as well as intelligence provided to New Zealand by the Five Eyes alliance.

GCSB continued to support domestic and international efforts to counter terrorist activity.

GCSB is represented on the New Zealand Major Events Security Committee (MESC), chaired by the Department of the Prime Minister and Cabinet (DPMC). This has involved the provision of advice and assistance, including intelligence and technical support, to the security arrangements surrounding a range of major New Zealand events both domestically and overseas.

GCSB's New Zealand Security Operations Centre (NZSOC) has continued to provide a Watch and Warn service on a 24/7 basis in support of major events, NZDF operations and travelling VIPs.

In the 2015/16 performance year, GCSB continued to provide support to NZDF in relation to their operations overseas.

Other activity

Contributing to the Independent Review of Intelligence and Security

GCSB provided information and advice to the Independent Review of Intelligence and Security (2015 Review) led by Sir Michael Cullen and Dame Patsy Reddy and advice to government on the operational implications of the reviewers' recommendations. A Bill is now before Parliament and the implementation of any legislative change that may result is a top priority for 2016/17.

Outer Space and High Altitude Activities Bill

Subject to parliamentary processes, legislation for the licensing and permitting of space and high altitude activities is anticipated to be in force mid-2017. This legislation will seek to protect New Zealand's national security and national interests.

GCSB's experience in providing communications security assurance and undertaking our regulatory role under TICSA positions us well to contribute to this role for New Zealand.

Organisational health and capability

Intelligence Community Shared Services (ICSS) implemented improvements and enhancements to facilities to improve safety and security and provide additional accommodation for an increased number of staff.

Core corporate systems were significantly improved, including:

- a financial management system, processes and business intelligence tools
- a Human Resources Information Management System (HRIMS) enhancement, including a performance review system with online functionality and improved reporting
- revised NZIC Health and Safety and Human Resources (HR) delegations and a harmonised suite of financial policies

We also improved organisational factors such as remuneration, employment terms and conditions, and staff management and leadership capabilities across agencies.

Warrants and authorisations

The GCSB Act enables GCSB to secure formal authorisation to intercept communications or access information infrastructures in pursuit of two of its three functions, which are information assurance and cyber security (section 8A) and foreign intelligence (section 8B). The GCSB Act also requires GCSB to have authorisation from its Minister to cooperate with, provide assistance to, or share information with certain entities in relation to section 8A or 8B activity.

There is no provision in the Act for GCSB to seek its own authorisation to intercept communications, or for any other activity, to assist NZSIS, NZDF or the New Zealand Police with their functions (section 8C). This is because any activity carried out by GCSB with respect to section 8C of the GCSB Act must rely on the lawful authority held by the requesting agency. GCSB policy provides an internal approval procedure for requests for assistance under section 8C.

1

Statements on interception warrants

A total of 22 interception warrants were in force during the 2015/16 year.

A total of 15 interception warrants were issued during the 2015/16 year.

2

Statements on access authorisations

A total of 46 access authorisations were in force during the 2015/16 year.

A total of 30 access authorisations were issued during the 2015/16 year.

3

Advice and assistance provided to other entities

During the 2015/16 year, there were nine 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:

- NZDF – 2 instances
- NZSIS – 7 instances

02

CHAPTER

OUR WORK IN DETAIL

About GCSB

GCSB is a public service department and reports directly to the Minister Responsible for the GCSB.

Our history

The New Zealand Government has had access to a Signals Intelligence (SIGINT) capability since World War Two. There was a long-recognised need to ensure that 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 NZDF and NZSIS.
In 1977, Prime Minister Robert Muldoon approved the formation of GCSB, but its 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 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 began. In 2003, the Government Communications Security Bureau Act 2003 (the GCSB Act) took effect. The GCSB Act was amended in 2013.

In June 2003, Cabinet formalised the role of GCSB as the national authority for signals intelligence and information systems security.

In May 2014, the Telecommunications (Interception Capability and Security) Act 2013 (TICSA) came into effect. Under TICSA, GCSB acquired responsibility for administering the network security provisions set out in Part 3 of the Act.

Functions and objectives

The GCSB Act sets out the functions of GCSB and makes provision for its administration and the conduct of its operational activities.

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

- national security of New Zealand
- international relations and wellbeing of New Zealand
- economic wellbeing of New Zealand

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

1. 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
- analysing and reporting on matters relating to the security and protection of government and other entities' communications and information infrastructures

2. INTELLIGENCE GATHERING AND ANALYSIS

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

3. COOPERATION WITH OTHER ENTITIES TO FACILITATE THEIR FUNCTIONS

- cooperating and providing advice and assistance to the New Zealand Police, the NZDF and the NZSIS for the purpose of facilitating the performance of those entities' lawful functions

Locations

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

In early 2016 GCSB opened an office in Auckland.

Staff

GCSB employs approximately 353 staff in a wide range of disciplines including foreign language experts, communications and cryptography specialists, engineers, technicians and corporate staff. We are set to progressively grow over the next four years as a result of the recent budget announced increase.

The Director GCSB

The 2015/16 year saw two changes to the role of Director GCSB. The then Chief Legal Adviser, Lisa Fong, became acting Director in February 2016 after Una Jagose, who had been acting since February 2015. Lisa was acting Director until April 2016 when the current Director, Andrew Hampton, began his tenure.

Beyond the specific responsibilities under the GCSB Act, the principal responsibilities of the Director GCSB are set out in section 32(1) of the State Sector Act 1988, which ensures 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 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
- the efficient and economical delivery of the services provided by GCSB and how effectively those services contribute to the intended outcomes
- a shared leadership role within New Zealand, alongside the Director of Security and Deputy Chief Executive, Security and Intelligence Group, DPMC

The Senior Leadership Team

The Director is supported by an internal Senior Leadership Team (SLT).

SLT 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 SLT, during the reporting year, is comprised of:

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

Risk and Assurance Committee

The Risk and Assurance Committee is an independent committee reporting to the Director. The Committee met twice during 2015/16, in December and June.

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
- audit system (internal and external)

The Risk and Assurance Committee has two members.

1 The Director, National Security Communications is an employee of the Security and Intelligence Group (SIG) within DPMC. 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 also subject to scrutiny by the Inspector-General of Intelligence and Security (IGIS), a statutory office appointed to provide independent oversight of the activities of GCSB and NZSIS. The IGIS's role is to assist the Minister Responsible for the GCSB and the Minister in Charge of the NZSIS to ensure the agencies act lawfully and with propriety and to provide an independent determination of complaints about their conduct. The IGIS conducts inquiries into matters of concern and also reviews the agencies' compliance procedures and systems.

Along with every other public service agency, GSCB is subject to the State Sector Act, Public Finance Act, Employment Relations Act, the Privacy Act and the Official Information Act and is subject to the scrutiny of central agencies, as well as the Auditor-General, Privacy Commissioner and the Ombudsman.

Strategy, Capability and Resource Review

The NZIC Strategy, Capability and Resource Review (SCRR) was initiated to identify and present options to the Government that address the relationship between the New Zealand Government's security and intelligence requirements, the capability that the NZIC needs to meet those requirements and the consequential resource needs. SCRR was fundamentally about ensuring the NZIC can continue to respond to government's key national security risks in a world that is getting more dangerous.

In Budget 2016, the Government announced an increased funding package for the NZIC of $178.7m over four years. As at 30 June 2016, SCRR has been completed and the focus now shifts to implementing the NZIC Four Year Plan, which was developed on the basis of SCRR funding being made available to ensure the NZIC can meet the government and public's expectations.

GCSB is part of a wider domestic intelligence community

GCSB, NZSIS, and the Security and Intelligence Group within DPMC form the core of the New Zealand Intelligence Community (NZIC).

The agencies meet regularly to ensure close alignment on intelligence matters. The recent establishment of a joint leadership team will ensure strong oversight for shared work programmes and priorities. A shared workforce strategy will ensure the agencies achieve the benefits from the recent investment made by government and implement any legislative change that results from the 2015 Review.

There are other intelligence capabilities within government. NZDF, Ministry for Primary Industries (MPI), New Zealand Police, New Zealand Customs Service and Immigration New Zealand all have intelligence units. The core members of the NZIC work with these other intelligence units, and the wider New Zealand government sector, to ensure the security of New Zealand and to promote New Zealand's interests.

New Zealand is part of an international intelligence community

New Zealand is a member of an international intelligence alliance formalised by the UKUSA Agreement (a multilateral agreement for SIGINT cooperation).

The following four agencies are also members:

- Australian Signals Directorate, Australia
- Communications Security Establishment, Canada
- Government Communications Headquarters, United Kingdom
- National Security Agency, United States

This international alliance is also referred to as the Five Eyes.

It is not possible for an organisation the size of GCSB to collect foreign intelligence on all matters relevant to New Zealand's interests. However, through long-standing relationships with our Five Eyes partners, we can draw on greater support, technology and information than would otherwise be available to us.

GCSB may only receive intelligence or assistance from our international partners in accordance with New Zealand law. Any such support must also be provided in accordance with the law of the country that provides that support.

GCSB values collaboration both domestically between agencies and with our Five Eyes partners. The significant intelligence breakthroughs in recent years have involved people working across disciplines, across agencies and often across countries. Co-location, leadership commitment and a strong focus on customers are key enablers of successful collaboration.

NZIC Joint Strategic Framework

To meet the challenges of a broad and complex national security agenda, the NZIC is working hard to coordinate the efforts of constituent agencies, including GCSB. To ensure we can work together as an integrated sector, New Zealand's intelligence agencies are collectively guided by two documents. They are the New Zealand Intelligence Community Statement of Intent and the New Zealand Intelligence Community Four Year Plan.

These documents set out how the NZIC will deliver on its vision of 'building a safer and more prosperous New Zealand'.

The Statement of Intent outlines how, over the next four years, the NZIC will deliver on government's requirements and how this aligns with other agencies such as New Zealand Police, New Zealand Customs Services and NZDF.

The NZIC Four Year Plan outlines the planned growth and development of the NZIC. Importantly, it puts the NZIC in a strong position to ensure that our collective resources are used efficiently and that the planned growth activities across agencies are complementary.

The NZIC Four Year Plan was the basis for the development of GCSB's Strategic Plan 2016-2020, finalised this year.

GCSB Strategic Plan 2016-2020

GCSB's Strategic Plan 2016-2020 (the Strategic Plan) was finalised this year. This was developed by the Senior Leadership Team by drawing on the NZIC Four Year Plan and the Performance Improvement Framework Review, which highlighted the areas we can improve our performance for our customers, our corporate enablers and our collaborative activities as a sector.

The Strategic Plan gives a shared sense of the GCSB's aims and informs our planning and decisions about resource allocation.

SLT's intent is that directorates and units use the Strategic Plan to guide their own annual planning, that conversations at the senior leadership table are focused according to strategic priority and that GCSB input to NZIC planning and operational activities are meaningful.

The Strategic Plan has the following two key outcomes for the next four years.

IMPENETRABLE INFRASTRUCTURE

INDISPENSABLE INTELLIGENCE

It has eight identified strategic objectives, which are:

1 recruit and retain the best people

2 implement the new legislative regime

3 renew and extend GCSB's core IT infrastructure

4 replace New Zealand's high-grade cryptographic infrastructure

5 embed and scale GCSB's cyber defensive capabilities

6 radically improve the utility of our intelligence product

7 continue to modernise GCSB's accesses and tradecraft

8 overhaul how highly classified communications are delivered

In order to deliver on these outcomes and objectives, GCSB recognises the need to make important changes, including customer orientation, collaborative use of resources and corporate enablement.

In this annual report, the outcomes and objectives from the Strategic Plan provide a framework for reporting on GCSB's activities and achievements in 2015/16.

Strategic outcomes

As a government department, GCSB must deliver demonstrable value for New Zealand. GCSB's mission is to protect and enhance New Zealand's security and wellbeing. Over the 2016-2020 period, this mission will be fulfilled through activity focused around two strategic outcomes: *impenetrable infrastructure and indispensable intelligence.*

Impenetrable infrastructure

By 2020, New Zealand's most important information infrastructures are impenetrable to technology-borne compromise

GCSB will be more active across a wider span of the cyber threatscape, and will work closely with the recently announced Computer Emergency Response Team (CERT) and other government agencies to ensure the provision of 'best fit' for incident response.

The key objectives will be to embed and substantially scale GCSB's cyber defence capabilities and to replace New Zealand's obsolescing high-grade cryptographic infrastructure.

GCSB will increase the value of the advice given to enable both public and private entities to improve the security of their networks.

Information Assurance and Cyber Security

Information assurance and cyber security is one of GCSB's core functions. GCSB works with the public and private sectors to provide supervision, standards and services, which strengthen the protection of New Zealand information and information infrastructure.

For government, GCSB provides keys and devices to encrypt highly classified information and accredits sites and systems holding highly classified information in accordance with the New Zealand Information Security Manual (NZISM), the policy standard issued and updated by the GCSB as part of the Protective Security Requirements (PSR). GCSB also conducts inspections to ensure the integrity of secure locations. With respect to public telecommunication networks, the Director exercises regulatory responsibilities under the Telecommunications (Interception Capability and Security) Act 2013 (TICSA).

Meanwhile, through the National Cyber Security Centre (NCSC), GCSB provides cyber security services (including an incident response function) and advice to the public and private sector. These activities are intended to enhance rather than supplant the functions performed by other public agencies and commercial suppliers.

National Cyber Security Centre highlights 2015/16

338 cyber security incidents were logged by the NCSC during the 2015/16 year – an average of 28 incidents per month.

38 government agencies and 44 private firms approached the NCSC for advice or assistance in handling cyber incidents. This included banks or financial institutions, network operators or internet service providers and tertiary institutions. Some of these entities received assistance from the NCSC on multiple occasions.

The NCSC has provided hands-on, intensive incident response assistance on 28 occasions to 18 different organisations, including 9 private sector companies.

National Cyber Security Centre operational summary

The focus of the National Cyber Security Centre (NCSC) is on countering cyber-borne threats to organisations of national significance, e.g. government departments, key economic generators, niche exporters, research institutions and operators of critical national infrastructure. NCSC assists others to protect their networks from the types of advanced, persistent and sophisticated threats that are typically beyond the capability of commercially available tools.

With customer consent NCSC analysts monitor a range of customer data feeds to detect threats and cyber security incidents impacting New Zealand entities. Upon detection of a cyber threat, through CORTEX capabilities, the NCSC will engage directly with the affected entity (usually at an unclassified level) and offer mitigation advice and reporting. If the situation warrants it, the NCSC may escalate the incident to a full forensic investigation.

Equally, the NCSC has developed capabilities to disrupt malicious communication and prevent it from reaching its intended target. This capability is being provided as part of project CORTEX and the NCSC engages with the affected entity in order to report the incident accurately and to consider potentially relevant contextual information first hand.

The NCSC currently produces Computer Network Defence (CND) advice and reporting for domestic customers.

The NCSC's Incident Coordination and Response team is on call to victims of cyber incidents and ready to deploy 24/7. The NCSC triages, refers and/or responds to these public-derived incidents. These public-derived services will require realignment following Cabinet's decision to establish the NZ CERT (Computer Emergency Response Team).

What is CORTEX?

- CORTEX is a project to counter cyber threats to organisations of national significance – e.g. to operators of critical national infrastructure
- COREX involves GCSB implementing capabilities to protect these organisations against advanced malicious software (malware). The capabilities will allow advanced malware to be detected and disrupted
- CORTEX operates with the explicit agreement of the organisations that are protected from cyber threats
- CORTEX operates under the GCSB Act. The detection and disruption of malware by GCSB is governed by warrants and access authorisations approved by the Minister Responsible for GCSB and the Commissioner of Security Warrants
- Background to the project is seen in redacted Cabinet papers available on the beehive.govt.nz website

Other activities of the National Cyber Security Centre

Cyber security is a major function for GCSB. The NCSC has a wide range of responsibilities, including deploying and operating the CORTEX cyber-defence capabilities and responding to cyber incidents. In addition to these operational activities, the NCSC engages in a number of other activities aimed at strengthening the cyber security ecosystem in New Zealand.

GCSB has provided input into the business case for the burgeoning NZ CERT. Staff from across the directorate participated in working groups throughout the year, supporting the establishment of a CERT, its role and functions and how the new agency could work alongside the NCSC.

Information assurance

GCSB acts as the New Zealand national authority for COMSEC – the technology, processes and key material used to encrypt our most sensitive data at-rest and in-transit.

GCSB also provides technical inspection services, ensuring that areas that contain classified material are free from interception devices or vulnerabilities.

In addition, GCSB provides a significant level of assurance for government agencies by fulfilling the Director's role as the operating authority for highly classified information systems and sites.

Telecommunications (Interception Capability and Security) Act 2013

May 2016 marked the two year anniversary of Part 3 of TICSA coming into force. The purpose of this part of the Act is to prevent, mitigate or remove security risks arising from:

- the design, build or operation of public telecommunications networks
- interconnections to or between public telecommunications networks in New Zealand or with networks overseas

To achieve this, Part 3 of TICSA gives the Director GCSB, responsibility for decisions and actions in relation to network security.

These actions arise under two sections of the Act:

- Section 46(1) of TICSA, which requires a network operator to engage with the Director after becoming aware of any network security risk that may arise if a proposed decision, course of action or change is implemented
- Section 48 of TICSA, which requires a network operator to notify the Director GCSB of proposed changes made by the network operator within areas of specified security interest

All of the TICSA notifications received during 2015/16 were made under section 48 of the Act. During the reporting year, there were no instances where a network operator engaged with the GCSB after self-identifying a possible network security risk under section 46(1) of the Act.

As of February 2016, the TICSA team reached its full complement of five staff members, including two security consultants, two security engineers and one regulatory and compliance advisor.

The team endeavours to complete assessments within 20 working days of receipt of a notification, counting from the date on which complete information regarding the proposed decision, course of action or change from the network operator is received.

During 2015/16, the GCSB received 69 notifications that were resolved, on average, within 12 working days. In some cases, the team worked directly with the Network Operator to mitigate or eliminate any risk identified.

The Regulatory Unit has taken a number of steps to proactively engage with network operators on network security concerns. This reflects the commitment to involve them in the ongoing review of both the implementation and application of the Act.

In late 2015, the Regulatory Unit consulted with network operators on a review and update of the guidance originally published before TICSA came into effect, which is expected to be completed in the 2016/17 year. Team members regularly meet with network operators in order to discuss and address network security issues and risks.

Indispensable intelligence

By 2020, GCSB-sourced intelligence consistently generates unique policy and operational impacts for New Zealand

Intelligence has value only if it is used. GCSB will transition to an engagement model that focuses on the outcomes achieved for the customer and measures success through the eyes of customers.

This will involve re-positioning GCSB as an agency that delivers tangible impacts by providing intelligence service that can be practically applied to customers' policy and operational imperatives.

In 2015/16, GCSB provided regular delivery of foreign intelligence and operational support for:

- domestic and international counter-terrorism operations
- serious incidents involving the safety of New Zealanders overseas
- NZDF operations overseas
- policy and decision makers across government
- security arrangements supporting New Zealand Gallipoli commemorations

This service included regular delivery of intelligence to 19 government agencies and to appropriate Ministers, their officers and the Leader of the Opposition.

Counter-terrorism

GCSB supports domestic and international efforts to counter terrorist activity.

Major event support

GCSB is represented on the New Zealand Major Events Security Committee (MESC), chaired by DPMC. This has involved the provision of advice and assistance, including intelligence and technical support, to the security arrangements surrounding a range of major New Zealand events both domestically and overseas.

The GCSB's New Zealand Security Operations Centre (NZSOC) has continued to provide a Watch and Warn service on a 24/7 basis in support of major events, NZDF operations and to travelling VIPs. This involves the active monitoring of classified and unclassified sources of intelligence for potential threats, with timely notification to relevant New Zealand government agencies as required.

Support to NZDF operations

In the 2015/16 performance year, GCSB continued to provide support to NZDF in relation to their operations overseas. Support of various kinds was provided with the aim of improving the capability of NZDF to detect and counter threats to New Zealand military personnel deployed in various locations overseas.

Strategic objectives

During the 2015/16 year, GCSB has set eight objectives that work toward delivering indispensable intelligence and impenetrable infrastructure. The objectives align with the Strategic Plan and are the priorities for GCSB, not a complete workload. These activities, once complete, represent fundamental changes to the way GCSB works and the services delivered.

Here is an overview of each objective and the key activities that have occurred over the past year.

Recruit and retain the **best people**

Renew and extend our core **IT infrastructure**

Implement the new **Legislative regime**

Continue to modernise our **accesses and tradecraft**

Replace New Zealand's high-grade **cryptographic infrastructure**

Radically improve the **utility of our intellgence**

Overhaul how highly **classified communications are delivered**

Embed and scale our **cyber defensive capabilities**

Recruit and retain the best people

GCSB is an organisation of experts drawn from an increasingly competitive market. Over the long term it is staff, more than our technology, that generate the unique value GCSB's customers are seeking.

It is therefore critical that GCSB is able to attract and provide fulfilling career options for New Zealand's top talent.

Workforce strategy

NZSIS and GCSB leaders approved a 2016-2020 Workforce Strategy, which outlines the programme of work supporting further development of a growing astute, skilled and resilient intelligence workforce.

The focus for development will be centred on the following five key areas.

1. Brand & Culture: ensuring an employment brand that attracts the high calibre and specialist skills required and a culture that matches the employment experience with the brand
2. Recruit & Vet: selection decisions and vetting of potential employees are conducted in a manner that is both robust and efficient
3. Induct & Equip: supporting the ability of new starters to quickly function productively through exceptional induction and core skill development
4. Perform & Develop: ensuring systems and processes are platforms for developing and delivering technical and leadership excellence
5. Progress & Retain: effectively retaining our talent and proactively manage career development

A number of key strategic initiatives from the strategy were delivered in the reporting year, including:

- implementation of a new remuneration system to support business strategy, provide flexibility to attract and retain staff and give consistency for reward and recognition strategies
- implementation of an online human resources toolkit that provides managers and staff access to online advice, policy, resources and templates
- successful delivery of the inaugural career development boards for technical roles providing pathways for progression to attract and retain talent
- development and delivery of a single human resources policy framework and delegations policy
- development and delivery of a framework for human resources reporting and metrics linked to organisation strategic outcomes that informs progress and decision making
- lifting health and safety capability through development and implementation of a health and safety training and education programme, new policy and governance guidelines

Attracting new talent

There was a significant increase in the volume and quality of people recruited into the NZIC during the reporting year.

In November 2016, a new employment brand, 'Beyond Ordinary', will be launched. It is expected that this will further strengthen the ability to attract top talent into the intelligence community.

Growing our leaders

NZIC senior leaders participate in the State Services Commission (SSC) Leadership Insights programme and this is being progressively rolled out throughout the leadership cohort. All managers undergo structured leadership development training.

Additionally, an NZIC leadership competency job family that is modelled on the SSC Leadership Success Profile and looks at competencies and assessment from potential leaders to senior leaders has been developed. This initiative, focusing on further development of NZIC leaders, will be fully implemented in the 2016/17 year.

At the more senior level, the NZIC Leadership Career Board merges with the Public Sector Intelligence and Security Career Board. This allows talented NZIC leaders to gain experience across the wider public sector and develop the leadership skills required of a senior public servant irrespective of the agency they work in.

Graduate recruitment

GCSB has run a graduate recruitment programme since 2014 in order to bring exceptional new talent into the organisation. It is an innovative programme, encouraging graduates to get a wide range of experience in the business before settling into a permanent role.

The graduate recruits for each year start at the same time and begin their GCSB career spending two years rotating through a variety of roles in the directorates. This broadens their experience and gives them a real opportunity to learn about the various areas of GCSB. At the end of their rotation schedules, they settle into a permanent role.

Implement the new legislative regime

GCSB provided information and advice to the Independent Review of Intelligence and Security (2015 Review) led by Sir Michael Cullen and Dame Patsy Reddy. Advice was also provided to government on the operational implications of the reviewers' recommendations.

Changes of the scale and scope envisaged by the 2015 Review will require substantial revision of GCSB's warrants, policies, process, operational practices and training.

Given the magnitude of potential change, NZSIS and GCSB have established a joint project to prepare for and implement any legislative changes arising.

Renew and extend GCSB's IT infrastructure

It is no surprise that a rapidly changing technology landscape is having a disproportionate effect on a technology organisation like GCSB.

The growth in GCSB's technology-based service delivery, e.g. the cyber defence programme, the rising expectations of intelligence customers and the importance of maintaining the security of GCSB systems, place a heavy demand on our IT infrastructure development programme.

Over the past 12 months, the Capability Directorate has been actively recruiting a diverse range of skills and building teams to ensure the organisation can cope with the growing demands of the NZIC.

New Zealand Top Secret Network (NZ TSN)

GCSB's response to growing technology challenges is the development of the NZ TSN, an integrated set of capabilities for the secure storage and distribution of national security information for the whole New Zealand Intelligence Community.

The NZ TSN will provide a similar set of services at the TOP SECRET level to those provided by the Government Chief Information Officer (GCIO) for the RESTRICTED community.

In the reporting year, GCSB redirected its project effort to focus on delivery of the NZ TSN and has made significant progress in both the planning of the overall programme and the delivery of foundational projects.

Replace New Zealand's high-grade cryptographic infrastructure

New Zealand's high-grade cryptographic infrastructure allows communications classified higher than RESTRICTED to be protected through advanced encryption.

The infrastructure is the primary means by which the integrity of highly classified New Zealand information – including that received from and shared with Five Eyes partners – is maintained.

Cryptographic Products Management Infrastructure (CPMI) project

The project to deliver the replacement cryptographic infrastructure was initiated in August 2013.

CPMI will impact a number of other government agencies in the sector, most notably the intelligence community, NZDF, Ministry of Foreign Affairs and Trade (MFAT) and the New Zealand Police. GCSB will work closely with these agencies to ensure that continuity of service is maintained and that benefits of the new infrastructure are realised in full. GCSB has undertaken this work with a strong focus on stakeholder engagement because the replacement infrastructure will enable an all-of-government service. The project governance board includes independent representatives from the Ministry of Business, Innovation and Employment (MBIE), MFAT and the NZDF.

In October 2015, Cabinet approved the detailed business case for the CPMI project. Following approval, GCSB negotiated with the preferred supplier for the acquisition and through-life support of the replacement infrastructure. Ministers approved the implementation business case in March 2016.

The CPMI project is currently in the detailed design phase. The project team is designing the organisational, policy and technical change associated with implementing the replacement infrastructure.

Embed and scale GCSB's cyber defensive capabilities

To provide cyber security services to the most significant national information infrastructures in New Zealand, under its CORTEX project, GCSB has developed and deployed capabilities to protect selected entities against foreign-sourced cyber threats.

GCSB works with an increasingly large number of public and private sector customers on a wide range of information security topics, adding particular value through its focus on the threats that are advanced in terms of technical sophistication and/or persistence.

In addition to providing cyber defence services to its CORTEX customers, GCSB distributes cyber threat alerts and advisories to all government departments and a large number of private sector organisations, including key economic generators, niche exporters, research institutions and operators of critical national infrastructure.

Radically improve the utility of our intelligence product

GCSB has started a significant stream of work to ensure that we are aligning our reporting to customer requirements and delivering in accordance with the customer's expectation for timeliness and form. Part of this is enabling customers to co-create intelligence requirements.

Continue to modernise GCSB's accesses and tradecraft

GCSB's enduring mission is to collect and make sense of communications intelligence in a lawful manner consistent with the national interest. The ability to interpret and make best use of that intelligence depends on the skills, experience and unique capabilities applied to it.

Increasingly important is GCSB's ability to blend different intelligence sources, a process that may include using non-secret intelligence and tools to enrich secret interception and capabilities.

Overhaul how highly classified communications are delivered

NZIC's customers want fundamental change to how intelligence reporting is made available to them. They expect delivery to be electronic whenever possible, easily accessible, timely and highly targeted. NZIC's customers also want a better platform for secure mobile communications.

This is a challenging area of work but is extremely important to the continuing effectiveness of the NZIC.

A number of projects have been initiated to improve and extend the electronic delivery of intelligence reporting to GCSB's customers.

This includes the following two foundational projects that will underpin future service delivery, a new intelligence portal and new secure mobile capabilities.

Intelligence portal

GCSB operates an electronic intelligence portal on behalf of the NZIC in order to facilitate the distribution of intelligence to its customers.

The existing intelligence portal is no longer fit-for-purpose and will be replaced by a modern solution to facilitate better access to intelligence.

Requirements for a new portal, to be hosted on the NZ TSN are currently being gathered.

Better secure mobile communications

A project to deliver new secure mobile capabilities for the New Zealand Government was initiated in 2016.

The project concludes a Request for Proposal process and is presently evaluating bids from commercial suppliers.

03

CHAPTER

ORGANISATIONAL HEALTH AND CAPABILITY

GCSB Auckland office

Recognising the frequent and ongoing contact with a growing external customer base, the GCSB opened an Auckland office in early 2016.

This new facility is now fully functioning with five staff and capacity for future growth across the NZIC.

Remuneration framework

During 2014, development of a single remuneration framework for both NZSIS and GCSB began. This framework supports the alignment of both intelligence agencies' remuneration with the external market. It established mechanisms to address anomalies, provided a consistent system and established mechanisms to raise the remuneration of staff to more closely reflect sustained and effective performance. In September 2015, the new remuneration framework was rolled out to staff.

Career Pathways implementation

As part of the One Workforce Strategy, the 2014-15 Career Pathways project developed a shared framework for career planning and development for core NZIC agencies. In the past year, the implementation of Career Pathways began with the first series of joint NZSIS-GCSB Career Development Boards. These boards, comprising professional leaders from both organisations, are responsible for the ongoing health of their profession and for assessing applications for career progression.

The Career Pathways framework describes the skills, knowledge and abilities required within NZSIS and GCSB. It provides a common foundation to enable the delivery of common workforce management and development processes. It also provides the foundation to a systematic, sector-wide approach to developing and deploying our workforce so the core agencies can achieve its objectives, now and in the future.

By using the framework, our people can make informed decisions about whether they want to be a deep specialist in a subject area, have a multifaceted career or become a leader with the NZIC.

Stewardship of resources

Preserving the trust and confidence of partners is central to GCSB's success. GCSB is trusted with a variety of extremely sensitive classes of information, all of which are protected to the highest levels.

Working closely with the NZSIS, GCSB actively applies the protective standards laid down in the Protective Security Requirements (PSR) and has a work programme to monitor the physical, personnel and IT security systems in use to ensure they comply with all expected standards.

That work programme is subject to continuous improvement as it is assessed how to make our protective systems as effective and efficient as possible.

GCSB has, for instance, updated the annual process for oversight of the personnel security of its workforce to help staff meet the high levels of security behaviour expected of security clearance holders.

Now a task performed jointly with the NZSIS, the protective security programme ensures staff can operate securely and there is an IT security programme to ensure systems are fit-for-purpose with ongoing programmes of monitoring and logging. GCSB also supports the wider NZIC to protect the most sensitive information by providing tailored security advice to a wide range of customers.

The close collaboration enabled by the co-location of GCSB and other NZIC agencies in Pipitea House on Pipitea ensures that GCSB's key resources (people, information and systems) are protected from harm, be it from outside influences, either natural or man-made, or arising from malicious behaviour by a trusted insider.

Part of the stewardship of resources involves planning to cope with disruptive events and the GCSB, like all government agencies, is obliged to comply with the Civil Defence Emergency Management Act by ensuring delivery of critical services during and after a disruptive event.

There are ongoing programmes across the GCSB intended to identify and treat potential vulnerabilities so that, regardless of the source of disruption, those key services can be delivered and GCSB can meet its business objectives.

Improving our financial processes

GCSB has continued to enhance and improve financial and procurement systems and processes and financial performance and accountability is being incrementally improved. During the 2015/16 performance year, oversight of GCSB's asset portfolio was also improved.

GCSB staff	2012/13	2013/14	2014/15	2015/16
Staff turnover	6.8%	10.1%	9.8%	9.5%
EEO information				
Management				
Women	13%	38%	55%	53%
Men	87%	62%	45%	47%
Overall				
Women	36%	36%	36%	37%
Men	64%	64%	64%	63%
Equivalent FTE at year end	**303**	**315.7**	**301.3**	**353**

The staff turnover figures reported above differ from those in the 2015 Annual Report as they do not include planned redundancies. The figures reported above are in accordance with the turnover definition used by SSC.

Climate survey

A climate survey for the GCSB and NZSIS was conducted in 2014. This identified a series of priority actions to improve staff engagement, which have been an important focus of the leadership teams during the year with a range of initiatives and actions implemented to continue to address Climate Survey findings.

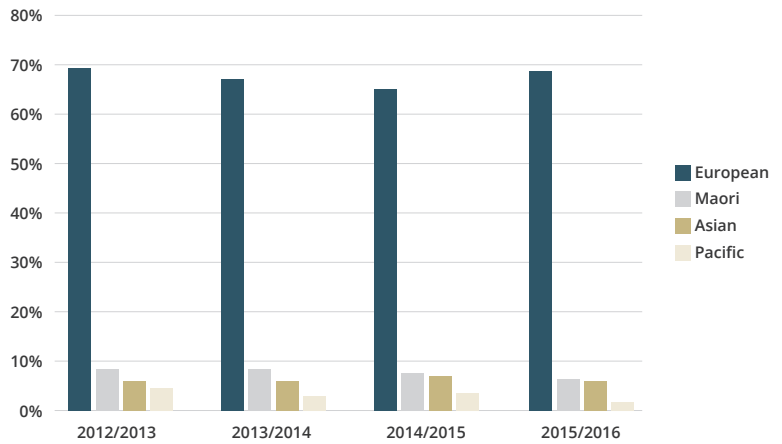
A new provider has been selected to complete a climate survey for GCSB and NZSIS in the 2016/17 year and planning is under way. This will inform progress made since 2014 and future priorities and actions.

Health and safety

A number of changes have been implemented as a result of the new Health and Safety at Work Act 2015 to lift the organisation's awareness and performance in health and safety requirements.

These include:

- a new health and safety policy implemented for the GCSB and NZSIS
- new health and safety committees established
- a new health and safety governance framework and membership developed and implemented
- training provided to assist with understanding of new, increased responsibilities
- revision of the health and safety module of the induction programme
- a specific health and safety objective will be included in performance and development documents for all staff and managers for 2016/17



The figures set out above vary from those in the 2015 Annual Report because of a change in the way diversity in the workforce is measured. The figures reported above are in accordance with SSC guidance.

During the year, NZSIS and GCSB have focussed on supporting staff who, in the course of their work, see or have access to disturbing material. A series of psychologist-run seminars for staff were put in place.

Topics covered include why material is hard to deal with, early warning signals, coping strategies, action plans and when and where to get help.

Where the need for additional support for staff was identified, a series of personally tailored sessions with a psychologist were arranged.

Managers have been coached and supported on how to have meaningful conversations about mental health and wellbeing.

Based on early benchmarks for stress in the workplace, against which we can assess the health of the organisation in future, additional approaches are being investigated.

A range of wellbeing support is available to staff, including resilience training, access to a clinical psychologist who is on site weekly, as well as ongoing support through the Employee Assistance Programme, access to Southern Cross health care group scheme and subsidised flu vaccinations.

Diversity in the workforce

The NZIC workforce is generally less diverse than the public service. One reason for this is the requirement for a checkable background and difficulty to confirm the personal information of potential employees who have not been resident in New Zealand for a long period of time.

Exit information provided by employees leaving the NZIC is reviewed and analysed quarterly. New staff are surveyed within three months of their start dates. This data is used to consider additional ways for staff to be provided equal access to employment opportunities and for the agencies to continually improve in this area.

During the 2015/16 performance year, seminars about unconscious bias were held for managers.

The NZIC Women's Network was established in May 2015 with a focus on networking, sharing experiences and providing the opportunity to hear the stories of inspirational leaders. Speakers have included a Minister and senior public servants at the chief executive and deputy chief executive level.

GCSB has employment policies in place to meet the varied needs of staff. This includes flexible hours and working arrangements and childcare subsidies where applicable.

Overall GCSB's workforce is made up of 37% women and 63% men, with women holding 53% of senior management positions within GCSB.

The above graph depicts the percentage of the GCSB workforce who have identified themselves by ethnicity.

04

CHAPTER

FINANCIAL STATEMENTS

AUDIT NEW ZEALAND
Mana Arotake Aotearoa

Independent Auditor's report

Independent Auditor's Report

To the readers of the Government Communications Security Bureau's annual report for the year ended 30 June 2016

The Auditor General is the auditor of 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 on her behalf of:

- the statements of expenses and capital expenditure against appropriation of the Bureau for the year ended 30 June 2016 on page 40

Opinion

In our opinion:

- the statements of expenses and capital expenditure against appropriation of the Bureau on page 40 are presented fairly, in all material respects, in accordance with the requirements of the Public Finance Act 1989

Our audit was completed on 23 September 2016. 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 information we audited is 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 information we audited. 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 information we audited. The procedures selected depend on our judgement, including our assessment of risks of material misstatement of the information we audited, whether due to fraud or error. In making those risk assessments, we consider internal control relevant to the Bureau's preparation of the information we audited 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 the disclosures in the information we audited; and
- the overall presentation of the information we audited

We did not examine every transaction, nor do we guarantee complete accuracy of the information we audited. Also, we did not evaluate the security and controls over the electronic publication of the information we audited.

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 present fairly the Bureau's financial position, financial performance, and its cash flows, and that comply with generally accepted accounting practice in New Zealand
- the statement of expenses and capital expenditure against appropriation of the Bureau, that are presented fairly, in accordance with the requirements of the Public Finance Act 1989

The Director's responsibilities arise from the Public Finance Act 1989. The Director is responsible for such internal control as is determined is necessary to ensure that the annual report is free from material misstatement, whether due to fraud or error. The Director is also responsible for the publication of the annual report, whether in printed or electronic form.

Responsibilities of the Auditor

We are responsible for expressing an independent opinion on the information we are required to audit, and reporting that opinion to you based on our audit. Our responsibility arises from the Public Audit Act 2001.

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

I am responsible as Director of the Government Communications Security Bureau (GCSB) for:

- the preparation of GCSB's financial statements and the statement of expenses and capital expenditure and for the judgements made in them
- having in place a system of internal control designed to provide reasonable assurance as to the integrity and reliability of financial reporting
- ensuring that end of year performance information on each appropriation administered by the GCSB provided in accordance with sections 19A to 19C of the Public Finance Act 1989, whether or not that information is included in this annual report
- the accuracy of any end of year performance information prepared by the GCSB, whether or not that information is included in the annual report

In my opinion:

The financial statement fairly reflect the financial position of GCSB as at 30 June 2016 and its operations for the year ended on that date; and its operations for the year ended on that date.

Andrew Hampton
Director
23 September 2016

Statement of expenses and capital expenditure against appropriation

For the year ended 30 June 2016

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

	$000
Total appropriation	143,568
Actual expenditure	135,084

The total appropriation in the table above incorporates both operating expenses and capital expenditure forecast for the year. The actual expenditure includes the actual operating expenses and the actual capital expenditure incurred.

Glossary of Terms

2015 Review	Independent Review of Intelligence and Security
CERT	Computer Emergency Response Team
CND	Computer Network Defence
COMSEC	Communications Security
CPMI	Cryptographic Products Management Infrastructure
DPMC	Department of the Prime Minister and Cabinet
Five Eyes	International intelligence alliance formalised by the UKUSA Agreement (a multinational agreement for SIGINT cooperation). The following four agencies are also members: • Australian Signals Directorate, Australia • Communications Security Establishment, Canada • Government Communications Headquarters, United Kingdom • National Security Agency, United States.
GCSB	Government Communications Security Bureau
GCSB Act	Government Communications Security Bureau Act 2003
HRIMS	Human Resources Information Management System
ICSS	Intelligence Community Shared Services
ICT	Information and Communications Technology
IGIS	Inspector-General of Intelligence and Security
ISC	Intelligence and Security Committee
MESC	New Zealand Major Events Security Committee
MFAT	Ministry of Foreign Affairs and Trade
MPI	Ministry for Primary Industries
NCSC	National Cyber Security Centre
NZDF	New Zealand Defence Force
NZIC	New Zealand Intelligence Community
NZISM	New Zealand Information Security Manual
NZSIS	New Zealand Security Intelligence Service
NZSOC	New Zealand Security Operations Centre
NZ TSN	New Zealand Top Secret Network
PSR	Protective Security Requirements
SCRR	New Zealand Intelligence Community Strategy, Capability and Resource Review
SIGINT	Signals Intelligence
TECSEC	Technical Security
TICSA	Telecommunications (Interception Capability and Security) Act 2013

gcsb.govt.nz

GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

New Zealand Government