Government Communications Security Bureau
Te Tira Tiaki

ANNUAL REPORT
2017

GCSB.GOVT.NZ

GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

Preface

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

CONTENTS

CHAPTER

01

OVERVIEW OF THE YEAR

MINISTER'S FOREWORD

Andrew Little
Minister Responsible for the GCSB

New Zealanders' safety and prosperity benefit from having a strong and effective intelligence and security sector. We continually see traditional and non-traditional threat actors acting in ways that can negatively impact New Zealand and the lives of New Zealanders.

Strong, timely and robust intelligence and advice enables the Government to make informed decisions and set appropriate policy. This ensures New Zealanders are safe, here and abroad, and contributes to the economic well-being of the country.

For instance, over this past year the Government Communications Security Bureau (GCSB) has helped protect New Zealand from a range of advanced cyber threats. They led New Zealand's response to a large-scale infiltration of critical internet infrastructure, and worked closely with the newly-established Computer Emergency Response Team New Zealand (CERT NZ) to address malware attacks that were unprecedented in their scale. GCSB also completed Project CORTEX, establishing a suite of defensive cyber security capabilities to protect our nationally-significant organisations.

The wider New Zealand Intelligence Community (NZIC) has also continued to play a critical role in raising protective security standards across the New Zealand public sector. By providing expert advice on information security practices, GCSB supported 35 mandated government agencies to effectively implement the Protective Security Requirements (PSR).

Over the last few years, significant effort has gone into strengthening the core capabilities and effectiveness of New Zealand's intelligence and security agencies. This work, in conjunction with the first independent review of intelligence and security conducted by Dame Patsy Reddy and Sir Michael Cullen and the subsequent enactment of the Intelligence and Security Act 2017 (ISA), will enable the security and intelligence agencies to reduce New Zealand's exposure to national security threats.

New Zealanders should feel confident the New Zealand Security Intelligence Service (NZSIS) and GCSB are working to ensure they fully comply with and gain the full benefit of the new legislation. This will serve to increase clarity around the purpose of each agency, enhance transparency around their activities and ensure they have robust policies and processes in place to support implementation of the legislation.

It is anticipated these changes will take several years to fully develop and embed. However, I am pleased at the initial progress the agencies have made. Looking ahead, I am confident this investment, and the agencies' efforts to leverage it effectively, means NZSIS and GCSB will be ready to face an increasingly challenging security environment.

DIRECTOR-GENERAL'S OVERVIEW

Andrew Hampton –
Director-General
GCSB

New Zealand's prosperity and way of life is built on us being an open and democratic nation, with the free flow of people, trade and information across our borders. Our increased connectivity to the rest of the world through technology has and will continue to bring real benefits to New Zealand and New Zealanders.

Yet with that connectedness comes new risks and threats that we must safeguard against. In the past, New Zealand could rely on our geographic remoteness to keep our people and information safe. But the technology that now connects us to the rest of the world also means we are now exposed to modern and rapidly changing cyber threats.

Not only are the number of cyber threats increasing, the nature of the threats are becoming more complex and the sources of them more diverse. For instance, this year we saw the 'Wannacry' and 'NotPetya' ransomware attacks target computer users around the world on an unprecedented scale. We also witnessed efforts to infiltrate and control key parts of the internet's architecture by hostile cyber actors. The last few years have also seen state actors, violent extremist organisations and individuals of security concern increasingly turn to the internet, and in particular social media, to carry out their agendas.

In this context, the focus of the NZIC over the last year has been on ensuring that we are fit-for-purpose to keep New Zealand and New Zealanders safe from existing and emerging threats to our national security and that the Government has access to accurate, timely and relevant foreign intelligence. Budget 2016 included a significant funding increase for the NZIC to ensure that agencies, including GCSB, have the people and tools necessary to carry out their functions in an increasingly challenging global and domestic environment.

Looking back over the last year, I have been pleased with how GCSB has responded to these challenges. We have taken some important initial steps to build our future capability in the areas of cyber defence, intelligence collection and information technology. Over the next two years, we will build on this foundation and continue to improve GCSB's performance and develop capabilities that are critical to our mission of protecting and enhancing New Zealand's security and wellbeing.

I am particularly proud of the completion of Project CORTEX. This work established a suite of defensive cyber security capabilities to protect nationally-significant government and private sector organisations from malicious software. In 2016, CORTEX capabilities prevented an estimated $39.47 million in potential harm caused by advanced cyber threats.

The last year has also seen the NZIC work hard to implement the ISA. This legislation supports better collaboration between GCSB and NZSIS and provides clarity about the roles and responsibilities of each agency. Greater alignment and collaboration between these agencies as well as the National Assessments Bureau (NAB) in the Department of the Prime Minister and Cabinet (DPMC) is fundamental to the success of the NZIC's ability to protect New Zealand and New Zealanders.

In order to keep New Zealanders and their information safe, GCSB exercises some intrusive powers, often in secret, on behalf of the Government. It is important that we are as transparent as possible about the nature of the threat New Zealand faces, our role in countering them and how we are held accountable. During my directorship, I have committed to improving the transparency of GCSB and better informing the public and our stakeholders about our work.

I am pleased with how this work is progressing. Over the last year, we have worked to make more information available to the public, including through speeches and the material we publish such as this annual report. We have also improved our practices for responding to Official Information Act and Privacy Act requests and we work closely with the Office of the Ombudsman and the Office of the Privacy Commissioner to quickly resolve the complaints and to explain the reasons behind our decisions.

Everything GCSB does needs to be carried out in New Zealand's interests and in accordance with the law, including New Zealand's human rights obligations. This is an absolute bottom-line that applies to all of our work, whether we undertake it ourselves or through others. With this in mind, I am pleased to note the Inspector-General of Intelligence and Security has found that over the past three years GCSB has had sound compliance procedures in place.

In 2016, CORTEX capabilities prevented an estimated $39.47 million in potential harm caused by advanced cyber threats.

GCSB'S MISSION IS

PROTECTING AND ENHANCING

NEW ZEALAND'S SECURITY AND WELLBEING

STRATEGIC PLAN 2016-2020

The GCSB strategic plan is based on delivering two primary outcomes to New Zealand and New Zealanders – Impenetrable Infrastructure and Indispensable Intelligence. These outcomes guide GCSB's internal planning, prioritisation and resource allocation.

Impenetrable Infrastructure

New Zealand's most important information infrastructures are impenetrable to technology-borne compromise.

Indispensable Intelligence

Our intelligence consistently generates unique policy and operational impacts for New Zealand.

Strategic Objectives

GCSB has eight underlying strategic objectives that underpin GCSB's efforts to deliver Impenetrable Infrastructure and Indispensable Intelligence. These activities, once complete, will represent a fundamental change to the way GCSB operates and the products and services it delivers.

1. Recruit and retain the best people.
2. Renew and extend our core IT infrastructure.
3. Continue to modernise our accesses and tradecraft.
4. Replace New Zealand's high-grade cryptographic infrastructure.
5. Implement the new legislative regime.
6. Radically improve the utility of our intelligence.
7. Embed and scale our cyber defensive capabilities.
8. Overhaul how highly classified communications are delivered.

NOTABLE ACHIEVEMENTS IN 2016/17

Impenetrable Infrastructure

Project CORTEX
Project CORTEX established a suite of defensive cyber security capabilities to protect nationally-significant government and private sector organisations from malicious software. This project was largely completed during 2016/17. In 2016 prior to full deployment, CORTEX capabilities prevented an estimated $39.47 million in potential harm caused by advanced cyber threats.

Global Cyber Attacks
GCSB's National Cyber Security Centre (NCSC) worked with CERT NZ to provide an integrated response to the 'Wannacry' and 'NotPetya' ransomware attacks. GCSB also led New Zealand's response against the infiltration of Managed Service Providers – a key part of the internet's architecture.

Cryptographic Products Management Infrastructure (CPMI) Project
The CPMI project will replace the infrastructure currently used by GCSB to protect classified New Zealand Government information. During 2016/17, the project team completed the necessary design and costing work. The project is tracking within budget and will continue to be delivered through 2017/18.

The Telecommunications Interception Capability and Security Act 2013 (TICSA)
GCSB has responsibility for administering the network security provisions set out in TICSA. Network operators are required to notify the Director-General of proposed changes made by the network operator within areas of specified security interest. In 2016/17, GCSB received 122 such notifications that were assessed, on average, within 10.2 working days. Where required, GCSB worked with the network operator to mitigate or eliminate any national security risks.

Outer Space and High-altitude Activities
GCSB, working in conjunction with the broader NZIC, progressed the development of the Space Activity Risk Assessment Group to establish the systems and processes necessary to conduct national security risk assessments for New Zealand's developing space industry.

Indispensable Intelligence

Provision of Intelligence
GCSB continued to supply foreign intelligence to 19 government agencies, as well as to appropriate Ministers and decision makers. These intelligence products – generated through our own collection operations and partner reporting – contributed to New Zealand's national advantage and ensuring the safety of New Zealand and New Zealanders.

Other Activity

ISA
The new legislation supports better collaboration between GCSB and NZSIS and provides clarity about the roles and responsibilities of each agency. GCSB and NZSIS successfully implemented the initial provisions of the ISA, which came into force on 1 April 2017, and implemented the further provisions that came into effect on 28 September 2017.

WARRANTS AND AUTHORISATIONS

The Government Communications Security Bureau Act 2003 (GCSB Act) enabled GCSB to obtain warrants or authorisations to intercept communications or access information infrastructures in pursuit of two of its three functions; information assurance and cyber security (section 8A) and foreign intelligence (section 8B). The Act also required 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.

Interception warrant data shows:

- A total of 33 interception warrants were in force during the 2016/17 year.
- A total of 26 interception warrants were issued during the 2016/17 year.

During the 2016/17 year, there were 14 instances where the Director GCSB approved the provision of advice and assistance in accordance with section 8C of the GCSB Act.

For example:

- New Zealand Defence Force (NZDF) – 1 instance.
- NZSIS – 13 instances.
- New Zealand Police (Police) – 0.

In each case, the advice and assistance was approved for a period of time associated with operational needs.

A total of 48 access authorisations were in force during the 2016/17 year. A total of 27 access authorisations were issued during the 2016/17 year.

With the enactment of ISA, GCSB will come under a shared warranty regime with NZSIS. Accordingly, progressively from 28 September 2017, GCSB's warranted activity will be covered by 'Type 1' and 'Type 2' warrants rather than 'interception warrants' and 'access authorisations'. As a result, from 2017/18, GCSB's annual report will report on the number of 'Type 1' and 'Type 2' warrants in force and issued during the reporting period, as well as GCSB Act interception warrants and access authorisations in force and issued during the reporting period.

Interception warrant data shows:

33

A total of 33 interception warrants were in force during the 2016/17 year.

26

A total of 26 interception warrants were issued during the 2016/17 year.

CHAPTER

02

OUR WORK IN DETAIL

THE NEW ZEALAND INTELLIGENCE COMMUNITY JOINT STRATEGIC FRAMEWORK

An agile, coordinated and customer focused community that can sustainably meet the Government's security and intelligence priorities.

Purpose

The purpose of the NZIC is to protect New Zealand as a free, open and democratic society. The NZIC does this by providing unique insights and capabilities that contribute to the following policy outcomes.

- Keeping New Zealand and New Zealanders safe by giving the New Zealand Government the ability to identify, investigate (including through covert collection) and respond to significant national security threats and risks.
- Protecting and growing the economy by helping the New Zealand Government and key economic entities to protect their information, assets and people.
- Advancing New Zealand's interests internationally through the collection and assessment of foreign intelligence pursuant to New Zealand's foreign policy goals.

Agencies

The NZIC is made up of:

New Zealand Security Intelligence Service
Te Pā Whakamarumaru

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

DEPARTMENT OF THE PRIME MINISTER AND CABINET
TE TARI O TE PIRIMIA ME TE KOMITI MATUA

A Community Approach

The NZIC takes a community approach to ensure the agencies are meeting the Government's intelligence and security objectives. This recognises that the threats the NZIC is managing and the opportunities it is seeking to capitalise on are often complex and multifaceted. Successful national security outcomes in the current operating environment require a team approach – no one agency can do it all.

To meet the security and intelligence challenges facing New Zealand, the NZIC is working hard to coordinate the efforts of NZIC agencies. To ensure the agencies can work together as a more integrated sector, the NZIC agencies are guided by three documents. The documents are the *New Zealand Intelligence Community Statement of Strategic Intentions, the New Zealand Intelligence Community Four Year Plan* and *the New Zealand National Intelligence Priorities*. These documents set out how the NZIC will deliver on its vision of building a safer and more prosperous New Zealand.

NZIC Statement of Strategic Intentions

The strategic intentions statement outlines how, over the next four years, the NZIC as a whole will deliver on the Government's requirements and how this aligns with the work of other agencies such as the Police, the New Zealand Customs Service (Customs) and the NZDF. In contrast, the NZIC Four Year Plan provides a detailed growth and development plan for the NZIC.

The National Security Committee of Cabinet, using a DPMC-led process, reviews and agrees to a set of National Intelligence Priorities every 12 to 24 months. The National Intelligence Priorities drive the collection and assessment activities of the wider New Zealand system, not just the core NZIC agencies. Other agencies such as the New Zealand Customs Service, Maritime New Zealand, New Zealand Police, the Ministry of Business, Innovation and Employment and the NZDF all actively participate in the delivery of these priorities. The purpose of the priorities is to ensure relevant government sectors and agencies focus intelligence collection, reporting and assessment activities on what matters most to the Government.

New Zealand – Part of An International Intelligence Community

International intelligence sharing arrangements are fundamental to how GCSB and NZSIS progress New Zealand's national interest. New Zealand could not hope to deliver the current level of security and intelligence activity alone.

Alongside Australia, Canada, the United Kingdom and the United States of America, New Zealand is a member of an international intelligence partnership known as the Five Eyes. This partnership allows us to draw on greater support, technology and information than would otherwise be available to us.

The Five Eyes partnership has been central to New Zealand's approach to intelligence and security since World War Two. The partnership started out as a narrow cryptologic venture to share effort and results in code breaking (and code making) in wartime. From that experience, a much wider framework for cooperation has evolved, involving all aspects of security and intelligence, the armed forces, police, law enforcement, customs services and Attorneys-General.

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.

STRATEGIC OPERATING ENVIRONMENT

Cyber Security

Safe and secure access to and use of the internet is critically important to New Zealand. Government agencies, private business and New Zealanders increasing use and rely on the internet in their day-to-day lives.

New Zealand's cyber threat environment is increasingly complex and far from benign. GCSB continues to see a range of international actors targeting New Zealand systems, infrastructure and businesses for financial gain. The number of cyber threats in New Zealand continues to grow in line with international trends – threatening the economy and potentially undermining New Zealand's strategic advantage. The threats seen are both direct (deliberate attacks on New Zealand's cyber security) and indirect (indiscriminate phishing attempts by state-sponsored actors that may not be deliberately targeted at New Zealand but can harm us nonetheless).

In 2016/17, some examples of incidents responded to included 'Wannacry' and 'NotPetya' ransomware attacks and a global infiltration of Managed Service Providers – a key part of the internet's architecture.

As New Zealand's lead cyber-security agency, GCSB plays a critical role in protecting New Zealand's national security and economic well-being from threats arising from cyberspace. Accordingly, much of GCSB's time and resources are devoted to detecting and responding to cyber threats to New Zealand.

Foreign Interference

New Zealand is not immune to the threat of espionage by foreign states or to foreign efforts to interfere with the normal functioning of government or the rights of New Zealanders. Such activities in New Zealand over the past year have included attempts to access sensitive government and private sector information and attempts to unduly influence expatriate communities.

Espionage will almost certainly remain a key aspect of statecraft for many countries – particularly around international flashpoint issues. The methods, technologies and defences used will likely change with countries evolving intelligence priorities. Hostile cyber activities are increasingly becoming a key tool for foreign states to undertake espionage and interference activities.

Violent Extremism

The global terrorism environment continues to be dominated by the influence of the Islamic State of Iraq and the Levant (ISIL). Coalition military operations in Iraq and Syria have considerably degraded ISIL's capability and territorial possession in the past 12 months. Despite battlefield losses, ISIL continues to attract and inspire followers around the world and this is likely to continue well beyond their almost certain military defeat.

As ISIL cedes territory, terrorist attacks have continued – especially in Europe. These have been both sophisticated and rudimentary, often targeting places of mass gathering and busy city streets, using weapons that are easily acquired.

Internationally, the number of individuals travelling to support ISIL in the Middle East conflict zone is believed to have decreased significantly. It is possible that foreign terrorist fighters in Iraq and Syria may seek to leave, either returning to their country of origin or possibly to other countries.

New Zealand is not set apart from these events. Violent extremist ideology and messaging, primarily accessed through online content and social media platforms, continues to resonate with a small number of individuals in New Zealand. Offshore a very small number of New Zealanders are thought to remain alongside ISIL in Syria or Iraq.

ABOUT THE GOVERNMENT COMMUNICATIONS SECURITY BUREAU

GCSB is a Public Service department that reports directly to the Minister Responsible for the GCSB.

The New Zealand Government has had access to a signals intelligence capability since World War Two. There was a long recognised need to ensure that government was protected from 'bugging' and that its sensitive messages could not be read by third parties. Until the establishment of GCSB, these services were provided by bodies such as 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. Prime Minister Muldoon publicly acknowledged the existence of GCSB and its signals intelligence function in 1984.

In early 2000, a legislative process to place GCSB on a statutory footing began. In 2003, the GCSB Act took effect. In June 2003, Cabinet formalised the role of GCSB as the national authority for signals intelligence and information systems security. Through this legislation, the GCSB also became a Public Service department.

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. The Outer Space and High-altitude Activities Act 2017 came into force on 21 December 2017. Under this legislation, GCSB along with the broader NZIC, will support national security risk assessments to be done on outer space launches, launch facilities, payloads and high altitude vehicles.

Following the first independent review of the intelligence and security legislation in 2015, the ISA was enacted in 2017. This was an important milestone for NZSIS, GCSB and the wider intelligence community. This legislation supports better collaboration between NZSIS and GCSB by bringing the agencies under a single warranting regime and providing clarity about the role of each agency.

IMPENETRABLE INFRASTRUCTURE

GCSB works to achieve its goal of providing impenetrable infrastructure through its cyber security and information assurance services. It responds to and mitigates cyber threats through the National Cyber Security Centre (NCSC) and provides defensive cyber threat services to public and private sector organisations of national significance. It also delivers cyber threat intelligence reporting to customers and partners. A strong outreach and engagement function supports this work.

GCSB's information assurance activities include providing high-grade encryption services to protect classified information and assessing proposed near space activity and changes to telecommunications networks for risks to national security. It also publishes the New Zealand Information Security Manual (NZISM) containing minimum protection standards and guidance for agencies.

Cyber Security

GCSB focuses on countering cyber-borne threats to organisations of national significance including government departments, key economic generators, niche exporters, research institutions and operators of critical national infrastructure. Through its CORTEX cyber defensive capabilities, GCSB supports these organisations to protect their networks from malicious, advanced, persistent and sophisticated threats with tools and expertise that are not typically available. GCSB's NCSC also produces classified cyber threat intelligence reporting for international and domestic partners and shares threat information with CORTEX customers.

GCSB leads the New Zealand Government's response to significant cyber events – particularly those that may affect national security and nationally-significant systems and information. The NCSC Incident Coordination and Response team is on call 24/7. GCSB also works closely with the newly-formed CERT,[1] which deals with day-to-day online security advice and coordinates response to incidents that are outside GCSB's mandate.

In 2016/17, GCSB began reviewing the security arrangements of a number of nationally-significant organisations. This included undertaking an initial assessment of the capabilities of customers, so the agency could better tailor its products and services to the needs of customers. The GCSB also created exercises to test customer preparedness for cyber security incidents. The agency is now also developing an online portal for NCSC reports, advisories and guidance to make it easier to disseminate this material to customers.

NCSC's outreach team is working to encourage greater awareness of cyber security risks in New Zealand, particularly amongst nationally-significant organisations. This work includes promoting understanding of how GCSB and other agencies such as CERT may be able to provide assistance. The focus of this outreach is on helping key stakeholders develop their own understanding of cyber security best practice.

1 CERT NZ helps businesses, organisations and individuals wanting prevention and mitigation advice on day-to-day online security issues and has primary responsibility for cyber threat reporting and a coordination role in threat response

Project CORTEX

CORTEX, a three year project, was largely completed during 2016/17. CORTEX is a suite of capabilities developed by GCSB that helps mitigate cyber threats to 66 nationally-significant organisations. It provides a network defence capability to identify malicious, advanced, persistent and sophisticated threats. Successfully implementing this complex and ambitious project represents a significant achievement for GCSB. The implementation of CORTEX has already achieved a sizable uplift in New Zealand's cyber defence capabilities.

In 2015/16, GCSB commissioned an independent evaluation of the potential impact of advanced cyber harm on New Zealand's nationally-significant organisations. The resulting analysis indicated the potential 'harm cost' to New Zealand and New Zealanders could be around $640 million annually. Using the same methodology, it is estimated that the initial implementation of CORTEX in 2016/17 has resulted in a "gross reduced harm benefit" of $39.47 million to New Zealand.

Now that deployment of CORTEX cyber defence capabilities is largely complete, GCSB's focus is turning to broadening its engagement with nationally-significant organisations with the aim of increasing overall network resilience. This includes sharing cyber threat information and working with organisations to identify risks, consider mitigations and improve their overall security posture. GCSB is also considering options for making its malware detection and disruption capabilities available to a wider range of nationally-significant organisations.

As part of future CORTEX initiatives, GCSB is piloting a Malware-Free Networks capability, where it shares cyber threat information and technology with an Internet Service Provider, so they can actively mitigate advanced threats from malicious software for a small subset of its consenting commercial customers.

Incident Detection

During 2016/17, NCSC recorded 396 incidents, an increase of 56 on the previous year. This increase is in part a reflection of NCSC's increasing insight into the activity occurring on networks of national significance.

Information Assurance

GCSB acts as the New Zealand national authority for communications security (COMSEC) – the technology, processes and key material used to encrypt the country's most sensitive data at-rest and in-transit.

GCSB provides key material and equipment to support New Zealand's high-grade cryptographic infrastructure. This allows communications classified higher than RESTRICTED to be protected through advanced encryption. The infrastructure ensures the integrity of New Zealand's highly classified communications is maintained.

GCSB also provides technical inspection services, ensuring 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-General's role as the operating authority for highly-classified information systems and sites.

To protect government agencies from information security risk, the GCSB publishes the NZISM. The manual contains minimum standards; along with guidance for agencies to protect information from threats to confidentiality, integrity or availability. The NZISM is part of the Protective Security Requirements (PSR) delivered by NZSIS and GCSB.

TICSA

In May 2014, the TICSA came into effect. Under TICSA, GCSB acquired responsibility for administering New Zealand's telecommunications network security. GCSB is having a positive impact on New Zealand's protective security standards in the telecommunication sector through TICSA.

During 2016/17, GCSB received 122 notifications of possible activities of security interest that were assessed, on average, within 10.2 working days.

CPMI

The CPMI project will replace the infrastructure (equipment, hardware, software, networks, facilities and support arrangements) currently used by GCSB to protect classified New Zealand Government information. The new infrastructure will affect several other government agencies in the sector, most notably the NZIC, NZDF, the Ministry of Foreign Affairs and Trade and Police.

In the past year, the CPMI project has progressed through detailed design and contract negotiation stages. The project has now moved on to implementing approved organisation and technology designs and developing accompanying policy and procedures.

Outer Space and High-altitude Activities

The Outer Space and High-altitude Activities Act 2017 came into force on 21 December 2017. The purpose of this legislation is to facilitate the development of a safe and secure space industry in New Zealand and to ensure that space activities are consistent with New Zealand's international obligations and national interests, including national security.

GCSB, working in conjunction with the broader NZIC, progressed the development of the Space Activity Risk Assessment Group to establish the systems and processes necessary to conduct national security risk assessments on outer space launches, launch facilities, payloads and high-altitude vehicles. GCSB's contributions have been coordinated by the Regulatory Unit of the Information Assurance and Cyber Directorate, given its experience in providing communications security assurance under the regulatory regime established by TICSA.

Top Secret Network (TSN)

GCSB is working to develop a New Zealand TSN, an integrated set of capabilities for the secure storage and distribution of national security information for the wider NZIC.

The New Zealand TSN will provide a similar set of services at the TOP SECRET level to those provided by the Government Chief Information Officer for the RESTRICTED community. The initial stages of this project are now complete. GCSB is now working to identify the network's core requirements and undertaking detailed design work.

INDISPENSABLE INTELLIGENCE

GCSB provides the New Zealand Government with intelligence that allows decision makers to generate policy and operational impacts.

GCSB is New Zealand's primary source of signals intelligence (SIGINT) generated foreign intelligence. Through the use of SIGINT capabilities and by leveraging relationships with New Zealand and international partners, GCSB is well placed to provide key intelligence insights to government decision-makers and other New Zealand Government agencies. This enables enhanced policy development and informed geo-political decision making.

GCSB aims to ensure New Zealand's security, advance the country's national interest, support regional security in the Pacific and support New Zealand agencies to carry out their functions.

In the 2016/17 year, GCSB supplied intelligence products to 19 government agencies. These intelligence products were generated through GCSB's collection operations and partner reporting – contributed to New Zealand's national advantage and ensuring the safety of New Zealand and New Zealanders.

Violent Extremism

GCSB supports domestic and international efforts to counter terrorist activity. The agency's focus in this area is predominately on supporting NZSIS and other New Zealand agencies to counter threats of terrorist activity in New Zealand.

Support for Major Events

GCSB is represented on the New Zealand Major Events Security Committee, 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.

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 dignitaries. 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.

CO-OPERATION WITH OTHER AGENCIES

Under section 8C of the GCSB Act, GCSB cooperates and provides advice and assistance to NZDF, NZSIS and the Police. This function is for the purpose of facilitating the performance of those entities' lawful functions and is carried out within the bounds of New Zealand's laws. In 2016/17 GCSB provided cooperation and advice to NZSIS and NZDF in support of national security investigations and to assist with the security of NZDF operations overseas.

Support to New Zealand Defence Force Operations

In 2016/17, 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.

Support to Law Enforcement

GCSB supports domestic efforts to counter criminal activity targeting New Zealand.

New Zealand DEFENCE FORCE
Te Ope Kātua O Aotearoa
NAVY NZ ARMY AIR FORCE

New Zealand Security Intelligence Service
Te Pā Whakamarumaru

New Zealand POLICE
Nga Pirihimana O Aotearoa

IMPROVE GCSB'S INTELLIGENCE PRODUCT

GCSB is working with NZSIS and DPMC's NAB to ensure there is alignment between reporting customer requirements and delivering in accordance with the customer's expectation for timeliness and format.

In February 2017, GCSB, NZSIS and DPMC's NAB launched a new collaborative customer engagement initiative. This is the intelligence community's most ambitious programme to date to better understand customers and increase the value intelligence provides them. The three agencies – with support from State Services Commission (SSC) 'Better Every Day' continuous improvement business coaches – are working to identify where the intelligence system works well for customers and where there are obstacles.

The engagement initiative has identified opportunities for improving the way intelligence is currently tailored, delivered and used by customers, including government agencies, appropriate Ministers and decision makers. The next stage of the process is to trial improvements in all of these areas. The lessons learned will then be evaluated and, as appropriate, applied more broadly and made sustainable across GCSB, NZSIS and NAB.

The 'Better Every Day' methods will be used in the months and years to come to ensure that NZSIS and the other agencies are continuously improving the way they work with customers and ensure customers are getting as much value as possible from the intelligence community.

CHAPTER

03

ORGANISATIONAL HEALTH AND CAPABILITY

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

LEADERSHIP

Director-General of GCSB

Andrew Hampton began his term as Director of the GCSB in April 2016.

Beyond the specific responsibilities set out in the GCSB Act 2003, the Director had the following responsibilities (also set out in section 32(1) of the State Sector Act 1988).

- Stewardship of GCSB, including its medium and long-term sustainability, organisational health and capability and capacity to offer free and frank advice to successive governments.
- Ensuring the performance of the functions and duties and the exercise of the powers of the GCSB director.
- The tendering of free and frank advice to Ministers, as well as the integrity and conduct of the employees for whom the Director is responsible.
- The efficient and economical delivery of GCSB services and the effective provision of those services, ensuring they contribute to intended outcomes.

The Director GCSB is accountable to the Minister Responsible for the GCSB.

Due to the enactment of the ISA, on 28 September 2017 the title of the Director GCSB changed to Director-General GCSB. The titles of other senior staff also changed from Deputy Director to Director.

Senior Leadership Team

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

SLT met 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-General, SLT includes the following roles.

- Director, Strategy, Governance and Performance.
- Director, Intelligence.
- Director, Capability.
- Director, Information Assurance and Cyber Security.
- Chief Legal Adviser.
- Chief Financial Officer, Intelligence Community Shared Services.
- Chief People Officer, Intelligence Community Shared Services.

Growing Leaders

NZIC senior leaders participate in the State Services Commission (SSC) Leadership Insight programme, which is being progressively rolled out throughout the leadership cohort.

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. During 2016/17, a framework was developed for this initiative to ensure leaders at different levels receive training tailored to their specific roles.

A New Way of Doing Business

In 2016/17, GCSB and NZSIS commenced a review of how to promote greater alignment, cooperation and more efficient use of corporate support for the organisations. The organisational changes resulting from this review will ensure that the NZIC is well placed to grow and effectively serve all its stakeholders.

Intelligence Community Shared Services

GCSB hosts the Intelligence Community Shared Services (ICSS), which provides human resource and finance services to GCSB and NZSIS. Over the reporting period, the ICSS has completed a number of projects that contribute to recruitment, retention and development of GCSB's workforce. These activities are listed in the following sections.

Risk and Assurance Committee

The Risk and Assurance Committee is an independent committee reporting to the Director-General. The role of the Committee is to assist the Director-General 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.
- Internal and external audit system.

RECRUIT AND RETAIN THE BEST PEOPLE

GCSB is a Public Service department, which employs approximately 392[2] staff from a wide range of disciplines, including foreign language experts, communications and cryptography specialists, engineers, technicians and corporate staff.

Recruiting, developing and retaining outstanding people is a critical aspect of the NZIC's workforce development. Having high quality people is critical to any organisation's success. This is particularly the case for GCSB which, due to the nature of the agency's work, relies on the technical expertise of staff.

The technical expertise required is in high demand and is 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 the organisation can attract, and provide fulfilling career options for, New Zealand's top talent.

As a result, GCSB has put in place a number of initiatives to meet this challenge, including a graduate recruitment programme, a recruitment campaign called 'Beyond Ordinary', a single remuneration framework for GCSB and NZSIS and a joint NZIC Career Pathways Framework.

The importance of GCSB's ability to recruit and retain staff extends beyond maintaining the organisation's current capabilities. As a result of funding received by the NZIC in Budget 2016, GCSB is set to progressively grow over the next four years.

Workforce Planning

The NZIC has completed a comprehensive review of its workforce needs and has developed workforce plans out to 2019/20 to ensure it has the requisite people capability to deliver the security and intelligence outcomes expected by government. The workforce plan is based on the funding received by the NZIC in Budget 2016 and the community's growth and development pathway detailed in the NZIC 2017 Four Year Plan.

Beyond Ordinary Careers

During 2016/17, a new employment brand, 'Beyond Ordinary', was launched to strengthen GCSB and NZSIS's ability to attract top talent. As a result of this work, there was a significant increase in the volume and quality of people recruited into the NZIC during the reporting year.

Work is underway to refocus the 'Beyond Ordinary' brand towards advertising the career pathway opportunities that the NZIC provides, rather than just focusing on advertising vacancies.

2 Full Time Equivalent (FTE) – this number is derived from the total of all staff members' employment, proportional to amount of a full time role they are employed to For example, a staff member who only does half a full time role is counted a 0 5 FTE Fixed Term, permanent employees, parental leave and those on leave without pay are included in this metric Metrics taken as at 30 June 2017

Graduate Recruitment

GCSB has run a graduate recruitment programme since 2014 to bring exceptional new talent into the organisation. It encourages graduates to get a wide range of experiences within GCSB before they are appointed into a permanent role.

The graduates begin their GCSB career spending two years rotating through a variety of roles in the directorates. This broadens their experience and gives them the opportunity to learn about the areas of GCSB. At the end of their rotation schedules, they settle into a permanent role.

Tertiary Scholarship for Women Studying STEM

In late 2016/17, GCSB launched a tertiary scholarship for women studying science, technology, engineering or mathematics (STEM). The scholarship, which is worth $10,000, targets students in their second year and above who are studying any of those subjects at a New Zealand tertiary institution. GCSB will further promote the scholarship through engagement with universities and polytechnics and the 'Beyond Ordinary' website.

Career Pathways

The Career Pathways and Career Board system were introduced in GCSB and NZSIS in 2015/2016. This is a joint framework that illustrates the different careers available within the NZIC and their progression requirements. It provides a robust and consistent competency-based framework against which staff can be assessed and promoted. It is a core part of the agency's workforce strategy to build more capability internally to help address market supply issues. Since its introduction last year, 59 GCSB staff have applied for progression through the Career Boards system with 33 successful applications.

Staff Retention

Staff retention is critical for GCSB, particularly given the unique and demanding environment staff operate in and the time involved in recruiting, vetting and training suitable personnel. The ICSS continues to monitor attrition figures and exit interview information to identify reasons why staff exit.

2016/17 Climate Survey Results

In 2017, GCSB conducted a Climate and Engagement Survey to give the SLT insights into staff engagement levels. GCSB was in the top 25 per cent of public sector agencies in terms of staff engagement.

SLT was particularly pleased the survey showed that staff:

- Felt highly connected to GCSB's mission of protecting and enhancing New Zealand's security and wellbeing.
- Felt they were actively contributing to this outcome.
- Believed that as an organisation, GCSB was making the right changes for future success.

Following on from the Climate and Engagement Survey, GCSB's SLT has agreed to an action plan to address the areas that staff identified as needing improvement and to further build on the organisation's strong results.

GCSB Core Unplanned Staff Turnover (2012 to 2017)

GCSB staff	2012/13	2013/14	2014/15	2015/16	2016/17
Turnover	6.8%	10.1%	9.8%	9.5%	7.1%

Core Unplanned Turnover is derived from the number of permanent staff who left the agency due to resignation, retirement, dismissal or unknown reason, divided by average total permanent headcount of the current and preceding financial year. Metrics are taken as at 30 June of relevant year.

DIVERSITY IN THE WORKFORCE

GCSB and the wider NZIC seek to ensure that their workforce reflects the diverse population the organisations serve. Diversity can improve innovation and decision making among employees, help attract and retain talented people and build the reputation of an organisation. This is particularly important for intelligence communities. The NZIC can serve its communities better with a workforce that is representative and reflective of the people it serves.

Ethnic Diversity

GCSB (and the wider NZIC) workforce is generally less ethnically diverse than the wider Public Service in part 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 (a requirement of the vetting process). The NZIC recognises this as an issue and is actively seeking ways to address this issue.

Gender Diversity

Women are well represented in GCSB at senior level (60% of senior managers are women – compared with a public sector average of 47.9%). However, overall only 36.4% of the workforce is female (much lower than the public sector average of 60.5%).

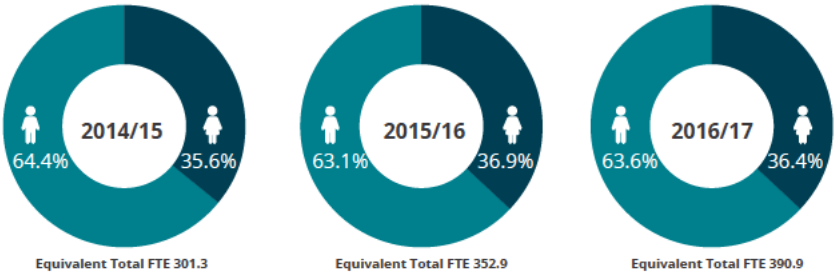
GCSB Staff Ethnicity

Ethnicity	2014/15	2015/16	2016/17
New Zealand European & European	66.0%	69.0%	68.7%
New Zealand Māori	7.5%	6.5%	7.2%
Asian	6.75%	5.8%	5.4%
Pacific Peoples	3.17%	1.6%	1.8%

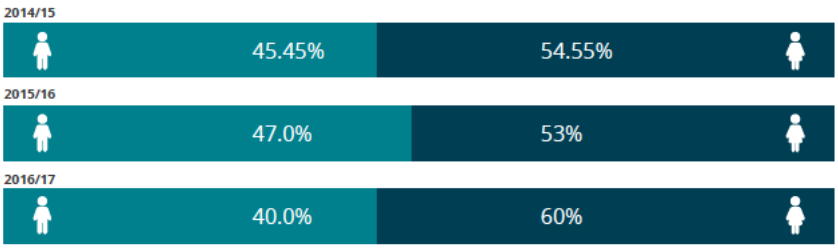
These metrics cover the number of employees who identify themselves as having a certain ethnicity. They are calculated by taking the number of people who identify themselves as being a certain ethnic group, divided by the number who have provided an ethnic group. Metrics are taken as at 30 June of the relevant year.

GCSB Gender Representation (2014 to 2017)

All staff



Senior Management (Tier 2 and 3)



Senior Management figures include Tier 2 and 3 managers only. Metrics are taken as at 30 June of the relevant year.

Diversity and Inclusion Strategy

Training and education, review of recruitment processes and the influence of the NZIC Women's Network have helped with diversity and inclusion in the NZIC.

GCSB is currently finalising a diversity and inclusion strategy, which will set out diversity targets and the specific actions the organisation will take to achieve them.

In the interim, 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.

Also, in the latter half of 2016/17, GCSB announced the tertiary scholarship for women students taking a STEM qualification to attract more women into computer technology, computer science and engineering roles.

LOCATIONS

GCSB has an office located on Pipitea Street in Wellington and opened an office in Auckland in early 2016. 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 communication interception station at Waihopai, near Blenheim.

The ICSS Property Group is currently undertaking a review of the NZIC's property portfolio to ensure our facilities are optimised, fit-for-purpose and compliant with the PSR. A review is also underway into the future utilisation of the Tangimoana site.

INVESTMENT IN CAPABILITY DEVELOPMENT

GCSB continues to develop its strategic planning and investment around its 2016-2020 Strategic Plan and the additional funding made available to GCSB through Budget 2016. During the last financial year, the organisation focused on embedding the eight strategic priority objectives into business planning, achieving the four *Strategy Capability Resourcing Review (SCRR)* capability outcomes set for completion during 2016/17 and establishing strong foundations for future growth.

Overall, GCSB is pleased with progress to date and expects to see accelerated progress in achieving SCRR deliverables as it aligns and develops GCSB, NZSIS and NZIC systems.

IMPLEMENT THE NEW LEGISLATIVE REGIME

Following the *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand* review conducted by Sir Michael Cullen and Dame Patsy Reddy, the ISA was enacted on 28 March 2017. This was an important milestone for GCSB and NZSIS.

GCSB and NZSIS established a joint dedicated project team to implement the ISA. This work included running education and training sessions for managers and staff about the impact of the changes to law will have on their work.

The initial provisions of the ISA, which came into force on the 1 April 2017, have been successfully implemented. In the latter part of the 2016/17 financial year, GCSB and NZSIS have focused on preparing implementation of the remaining provision, which came into effect on the 28 September 2017.

HEALTH AND SAFETY

A number of additional changes and improvements have been implemented this year to further strengthen GCSB's health and safety awareness.

These include:

- Ongoing training and education for the Health and Safety Governance Group, managers and staff on health and safety obligations, responsibilities and accountabilities;
- The launch of a Health and Safety Toolkit for all staff. This is a one-stop-shop for all things related to health and safety providing online advice, policy, processes, tool and resources;
- The development and implementation of a range of education and awareness resources, including NZIC-specifically designed posters and an induction brochure; and
- The establishment of a full time dedicated Senior Health and Safety Advisor position to support NZSIS and GCSB was also approved as part of the NZIC Workforce Plan.

GOVERNANCE AND OVERSIGHT

By necessity most of GCSB's activities are classified, meaning the organisation is not able to talk publicly about much of the work it does. Accordingly, effective oversight of its activities is essential to provide confidence to New Zealanders and the government of the day that the agency acts in a lawful manner and adheres to the democratic principles of the society it seeks to serve.

Office of the Inspector-General of Intelligence and Security (IGIS)

The IGIS and their office is the key oversight body of the NZIC. They provide a way for the public to have confidence GCSB complies with the law. The IGIS also acts as a mechanism to investigate complaints against the activities of GCSB by the public. GCSB regularly engages with the Office of the IGIS to discuss issues and provides information and resources to support of IGIS investigations and queries. Over the last three years, the IGIS has found GCSB to have sound compliance procedures in place.

This year, the IGIS released a public report of her inquiry into GCSB's process for determining its foreign intelligence collection activities. This inquiry was initiated as a result of issues raised by the public about the New Zealand Government's campaign to advance a candidate for Director-General of the World Trade Organisation. The IGIS's investigation found that the GCSB had acted consistently with its legal and policy framework and had acted lawfully and appropriately in providing its assistance to the campaign.

The Intelligence and Security Committee (ISC)

ISC is the parliamentary oversight mechanism for intelligence agencies. It examines issues of efficacy and efficiency, budgetary matters and policy settings. The ISC was 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. This composition of the ISC changed when the ISA came fully into force on 28 September 2017.

Transparency

Like other Public Service agencies, GCSB is subject to the Official Information Act 1982 (OIA) and the Privacy Act 1993. In responding to requests for information under these Acts, the organisation aims to be as open as possible.

Due to the sensitive nature of its work, however, revealing what it does or does not know can prejudice New Zealand's interests. GCSB could be the target of orchestrated information requests from people who want to know if they are under investigation and who may share responses with each other to draw conclusions about what GCSB is or is not aware of or the nature of the agency's capabilities.

GCSB will make a decision on a case-by-case basis about what, if any, information is provided in response to a request. It must protect its activities, sources of information, methods, partners and GCSB staff identities. Not doing so would potentially impact people's safety and may limit the agency's ability to achieve lawful objectives.

Official Information and Privacy Act Requests

For the period from 30 June 2016 to 1 July 2017, GCSB:

- Completed 57 OIA requests, with eight requests not completed within the legislated timeframe.
- Completed 27 Privacy Act requests, with seven requests not completed within the legislated timeframe.

GCSB is looking at its current OIA processes to address timeliness and to improve the way the agency responds to requests for information.

Complaints

For the same period of 30 June 2016 to 1 July 2017:

- 13 OIA complaints were completed by the Office of the Ombudsman during the period and 9 complaints were received. Eight of the completed complaints were resolved with a final opinion (in favour of the GCSB), 2 investigations were discontinued, 1 complaint was resolved without investigation, there was no investigation undertaken in relation to one complaint and one complaint was outside the Ombudsman's jurisdiction
- Five complaints were completed by the Office of the Privacy Commissioner during the period, with all completed complaints closed with a finding in favour of the GCSB.

In all cases, the GCSB worked proactively with the Office of the Ombudsman and the Office of the Privacy Commissioner to quickly resolve the complaints and to explain the reasons behind its decisions.

CHAPTER

04

FINANCIAL STATEMENTS

AUDIT NEW ZEALAND
Mana Arotake Aotearoa

INDEPENDENT AUDITOR'S REPORT

To the readers of the Government Communications Security Bureau's financial statements for the year ended 30 June 2017.

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, on his behalf, the audit of the financial statements of the Bureau for the year ended 30 June 2017, which is made up of the statement of expenses and capital expenditure against appropriation on page 39.

Opinion

In our opinion the statement of expenses and capital expenditure against appropriation of the Bureau on page 39 is presented fairly, in all material respects, in accordance with the requirements of section 45A of the Public Finance Act 1989.

Our audit was completed on 29 September 2017. This is the date at which our opinion is expressed.

The basis for our opinion is explained below. In addition, we outline the responsibilities of the Director-General and our responsibilities relating to the information to be audited, we comment on other information, and we explain our independence.

Basis for our opinion

We carried out our audit in accordance with the Auditor-General's Auditing Standards, which incorporate the Professional and Ethical Standards and the International Standards on Auditing (New Zealand) issued by the New Zealand Auditing and Assurance Standards Board. Our responsibilities under those standards are further described in the Responsibilities of the auditor section of our report.

We have fulfilled our responsibilities in accordance with the Auditor-General's Auditing Standards.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Responsibilities of the Director-General for the financial statements

The Director-General is responsible on behalf of the Bureau for preparing the financial statements, which are made up of 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 and the Intelligence and Security Act 2017.

The Director-General is responsible for such internal control as is determined is necessary to enable the preparation of the financial statements that are free from material misstatement, whether due to fraud or error.

In preparing the financial statements, the Director-General is responsible on behalf of the Bureau for assessing the Bureau's ability to continue as a going concern. The Director-General is also responsible for disclosing, as applicable, matters related to going concern and using the going concern basis of accounting, unless there is an intention to merge or to terminate the activities of the Bureau, or there is no realistic alternative but to do so.

The Director-General's responsibilities arise from the Public Finance Act 1989 and the Intelligence and Security Act 2017.

Responsibilities of the auditor for the audit of the financial statements

Our objectives are to obtain reasonable assurance about whether the financial statements as a whole, which are made up of the statement of expenses and capital expenditure against appropriation, are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion.

Reasonable assurance is a high level of assurance, but is not a guarantee that an audit carried out in accordance with the Auditor-General's Auditing Standards will always detect a material misstatement when it exists. Misstatements are differences or omissions of amounts or disclosures, and can arise from fraud or error. Misstatements are considered material if, individually or in the aggregate, they could reasonably be expected to influence the decisions of readers, taken on the basis of the financial statements.

For the budget information reported in the financial statements, our procedures were limited to checking that the information agreed to the Bureau's Estimates and Supplementary Estimates of Appropriations 2016/17 for Vote Communications Security and Intelligence.

We did not evaluate the security and controls over the electronic publication of the financial statements.

As part of an audit in accordance with the Auditor-General's Auditing Standards, we exercise professional judgement and maintain professional scepticism throughout the audit.

Also:

- We identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for our opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.
- We obtain an understanding of internal control relevant to the audit 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.
- We evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by the Director-General.

- We conclude on the appropriateness of the use of the going concern basis of accounting by the Director-General and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the Bureau's ability to continue as a going concern. If we conclude that a material uncertainty exists, we are required to draw attention in our auditor's report to the related disclosures in the financial statements or, if such disclosures are inadequate, to modify our opinion. Our conclusions are based on the audit evidence obtained up to the date of our auditor's report. However, future events or conditions may cause the Bureau to cease to continue as a going concern.
- We evaluate the overall presentation, structure and content of the financial statements, including the disclosures, and whether the financial statements represent the underlying transactions and events in a manner that achieves fair presentation.

We communicate with the Director-General regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal control that we identify during our audit.

Our responsibilities arise from the Public Audit Act 2001.

Other information

The Director-General is responsible for the other information. The other information comprises the information included on pages 4-34 and page 38, but does not include the financial statements, and our auditor's report thereon.

Our opinion on the financial statements does not cover the other information and we do not express any form of audit opinion or assurance conclusion thereon.

Our responsibility is to read the other information. In doing so, we consider whether the other information is materially inconsistent with the financial statements or our knowledge obtained in the audit, or otherwise appears to be materially misstated. If, based on our work, we conclude that there is a material misstatement of this other information, we are required to report that fact. We have nothing to report in this regard.

Independence

We are independent of the Bureau in accordance with the independence requirements of the AuditorGeneral's Auditing Standards, which incorporate the independence requirements of Professional and Ethical Standard 1 (Revised): Code of Ethics for Assurance Practitioners issued by the New Zealand Auditing and Assurance Standards Board.

Other than in our capacity as auditor, 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-General of the GCSB for the following.

- 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 is 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 statements fairly reflect the financial position of the GCSB as at 30 June 2017 and its operations for the year ended on that date.

Andrew Hampton

Director-General of the GCSB
29 September 2017

STATEMENT OF EXPENSES AND CAPITAL EXPENDITURE AGAINST APPROPRIATION

FOR THE YEAR ENDED 30 JUNE 2017

In accordance with section 45E of the Public Finance Act 1989 (PFA), I report as follows:

The 'total appropriation' below 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.

Total appropriation and actual expenditure for 2016/17 ($000)

	$000
Total Appropriation	$145,043
Actual Expenditure	$114,434

GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

New Zealand Government