GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

G56

Annual Report

For the year ended 30 June 2015

www.gcsb.govt.nz

New Zealand Government

Preface

This is the unclassified version of the Annual Report of the Government Security Communications Bureau (GCSB) for the year ended 30 June 2015. 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

ISN 1176-4686 (Print)

ISN 1178-0789 (Online)

Table of Contents

Preface 2

Foreword from the Minister 4

Message from the Director 5

About GCSB 7

A year of consolidation 12

- Completing the Compliance Review recommendations 12
- Working with the strengthened Office of the Inspector-General of Intelligence and Security 12
- The first full year of the Telecommunications (Interception Capability and Security) Act 2013 13
- Completing the rebalance of the Intelligence Directorate 14

Strategic initiatives 15

- Countering advanced cyber threats 15
- New Zealand's high-grade cryptographic infrastructure 15
- Strengthening management of our information and communication technology 16
- Capability Review 16

Operational performance 17

- Identifying and reducing New Zealand's vulnerabilities 17
- Increasing the security of New Zealand deployments 19
- Informing New Zealand's policy-makers and decision-makers on foreign political and economic issues 19
- Safeguarding New Zealand against threats of violent extremism and espionage 20
- Security and stability in the South Pacific 20

Organisational health and capability 22

- Performance Improvement Framework review 22
- Working together – Intelligence Community Shared Services 23
- Workforce planning 23
- Equal employment opportunities 24
- Climate survey 25

Financial statements 27

- Independent Auditor's report 27
- Statement of Responsibility 30
- Statement of expenses and capital expenditure against appropriation for the year ended 30 June 2015 31

Foreword from the Minister

I was appointed as Minister in Charge of the New Zealand Security Intelligence Service (NZSIS) and Minister Responsible for the Government Communications Security Bureau (GCSB) in October 2014. My appointment marked the first time that these portfolios have been held by someone other than the Prime Minister. This change was made after examining overseas models and what was adopted is very similar to our closest partners. The Prime Minister, in his role as Minister for National Security and Intelligence, is responsible for leading the national security system including policy settings and the legislative framework. I set and exercise Ministerial oversight of NZSIS and GCSB.

One of my first observations after taking up my new responsibilities was the dedication of NZSIS and GCSB staff, and their commitment to protecting the security of New Zealanders. For the most part, the work NZSIS and GCSB undertake goes unseen, but I support and encourage both agencies' efforts to increasing the transparency and openness of their activities where possible.

Both portfolios have shown to me the value of belonging to the Five Eyes intelligence community. In February 2015 I attended the Five Eyes countries' Ministerial Meeting in London. It was clear that, although we differ greatly in scale, we are all facing similar security threats and concerns. It was also clear that because of our strong relationships and our ability to leverage off each other's unique strengths and capabilities, we are in a much stronger position to address the challenges before us.

GCSB achieved some significant milestones during the 2014/15 year. In particular, I note the completion of the Kitteridge Review recommendations to strengthen legal and procedural compliance, and the roll out of the CORTEX programme to provide advanced cyber protection to selected consenting New Zealand organisations against those who wish to do them harm. It has also undertaken significant work to position itself to respond to the strengthened Office of the Inspector-General of Intelligence and Security which conducts inquiries and regular audits of GCSB's activities and processes.

The 2015/16 year looks to be another busy year for GCSB and other agencies of the New Zealand intelligence community, particularly in responding to the first independent review of New Zealand's intelligence and security legislation. GCSB will also be inducting a permanent Director and progressing key strategic projects to enhance and maintain their contribution to New Zealand's national security. I am confident they possess the capability and determination to meet the challenges and opportunities that lie ahead.

Hon Christopher Finlayson
Minister Responsible for the Government Communications Security Bureau

Message from the Director

During the 2014/15 year, GCSB has been focused on consolidating the changes made to its operating environment, and bedding down its amended governing legislation and associated policies and processes. The final implementation of recommendations from the 2013 Kitteridge Review of Compliance saw that report being fully implemented in GCSB. All of the implementation reports are on GCSB's public website. We have continued to drive organisational improvement through implementing the Performance Improvement Framework review insights into the organisation and through increased cooperation within the New Zealand Intelligence Community (NZIC) to deliver better, coordinated outcomes for Government.

We have heard, and are responding to, public calls for greater transparency. That remains a focus for both GCSB and the NZIC more broadly. Transparency and openness are not entirely straight forward in the security environment but we remain committed to them as concepts underpinning our work. We have to ensure that we do not inadvertently increase our vulnerabilities to people who do not have New Zealand's best interests at heart by revealing our sources, methods or targets. We don't want people we are gathering foreign intelligence on, or defending computer networks from, to know that we are looking at them or how we are doing that. We don't even want them to know what we are or are not capable of. Getting the balance between security and transparency right requires the independent oversight functions now embedded in the system. We are not a closed shop, setting our own standards, judging ourselves against them and saying "trust us". Far from it; we work under a rigorous authorising regime and we are the subject of significant, strong and independent oversight by the Inspector-General of Intelligence and Security, the Parliamentary Intelligence and Security Committee, the Ombudsman and the Privacy Commissioner.

This year has seen considerable advances in understanding the cyber threatscape and defending New Zealand infrastructure networks from attacks. These threats continue to evolve and challenge us – but the CORTEX cyber defence programme has been in the midst of implementation over the course of this year and allows a strong platform from which to support and protect organisations of significant importance to New Zealand. We are working closely with industry in sharing the information we obtain about cyber threats to enable them to assist and protect themselves and their customers. We have a role as regulator under the Telecommunications (Interception Capability and Security) Act 2013 (TICSA) network security provisions, which is now well implemented.

The changing cyber threatscape is not a problem for New Zealand alone – it is an international issue. We work closely with our Five Eyes partners to share technology, training, expertise and understanding of current threats.

The 2014/15 year has seen us working collaboratively with our NZIC colleagues in reviewing our delivery of foreign intelligence product to customers to ensure we remain customer-focused and deliver high quality foreign intelligence to the right people, at the right time, and relevant to their context. We have also provided timely and critical foreign intelligence reports to policy-makers and decision-makers, including on matters relating to security and stability in the South Pacific.

For our talented and committed staff we have continued working in a number of areas to provide them with strong performance and development processes to allow them to develop their skills and to enhance their careers.

In the year ahead, we look forward to making further progress on our key strategic initiatives, as well as in relation to the recommendations arising out of the NZIC Performance Improvement Framework report. We know that this will keep us well-positioned to continue the delivery of highly effective products and services that maintain and enhance New Zealand's national security and wellbeing.

Una Jagose
Acting Director

About GCSB

The Government Communications Security Bureau (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 the Second World War. There was a long recognised need to ensure that the Government was protected from "bugging" (technical security, or TECSEC) and that its sensitive messages could not be read by third parties (communications security, or COMSEC). Until the establishment of GCSB, these services were provided by bodies such as the New Zealand Defence Force (NZDF) and the New Zealand Security Intelligence Service (NZSIS). In 1977, Prime Minister Robert Muldoon approved the formation of GCSB, but 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 similar to that of the NZSIS began. In 2003, the Government Communications Security Bureau Act 2003 (GCSB Act) took effect. The 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; and

- international relations and wellbeing of New Zealand; and
- economic wellbeing of New Zealand.

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

Information assurance and cyber security

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

Intelligence gathering and analysis

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

Cooperation with other entities to facilitate their functions

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

Location

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

Staff

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

The Director GCSB

The 2014/15 year saw a change of Director for GCSB. Ian Fletcher, who had been Director since January 2012, left in February 2015 and was replaced by Una Jagose, to act as Director until early 2016.

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

- GCSB carrying out the purpose of the State Sector Act;
- GCSB's responsiveness on matters relating to the collective interests of government;
- the stewardship of GCSB, including of its medium and long-term sustainability, organisational health, capability, and capacity to offer free and frank advice to successive governments;
- the stewardship of–
  - assets and liabilities on behalf of the Crown that are used by or relate to GCSB;
  - the legislation administered by GCSB;
- the performance of the functions and duties and the exercise of the powers of the Director or of GCSB (whether imposed by any enactment or by the policies of the government);
- the tendering of free and frank advice to Ministers;
- the integrity and conduct of the employees for whom the Director is responsible; and
- the efficient and economical delivery of the services provided by GCSB and how effectively those services contribute to the intended outcomes.

The Senior Leadership Team

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

The 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 is comprised of the:

- Associate Director;
- Chief Financial Officer;
- Chief Legal Adviser;
- Chief of Staff;
- Deputy Director Capability;
- Deputy Director Information Assurance and Cyber Security;

- Deputy Director Intelligence;
- Director National Security Communications;[1] and
- General Manager Intelligence Community Shared Services.

Risk and Audit Committee

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

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

The Risk and Audit Committee has a chair and one independent member.

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 oversight of the activities of the 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.

GCSB is part of a wider domestic intelligence community

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

---

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

There are other intelligence capabilities within Government too. The New Zealand Defence Force, Ministry for Primary Industries, New Zealand Police, New Zealand Customs Service and Immigration New Zealand all have intelligence units. The core NZIC works with these other intelligence units, and the wider New Zealand government sector, to ensure the security of New Zealand and 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;
- Communications Security Establishment, Canada;
- Government Communications Headquarters, United Kingdom; and
- 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 intelligence than would otherwise be available to us.

A year of consolidation

Completing the Compliance Review recommendations

Since April 2013, GCSB has undertaken a significant amount of activity to implement the 76[2] recommendations contained in the Review of Compliance at GCSB (the Kitteridge report).

During 2014/15, GCSB implemented the remaining three recommendations, which involved the development of new staff training and examination modules. These modules have been integrated into the wider staff training programme led by the Learning and Development Team. All staff now receive compliance briefings as part of their induction programme and more specialist training programmes have been developed and delivered to operational staff, including one on how to ensure compliance with GCSB's obligations under sections 14 and 15(A)(b) of the GCSB Act (which regulate activities with respect to the interception of the private communications of New Zealanders).

As a result of implementing the Kitteridge report recommendations, GCSB now has a comprehensive framework of processes, tools and structures in place to support the effective management of compliance obligations. This framework is administered by GCSB's Compliance Team who are an important source of advice and information for staff relating to issues of legislative and policy compliance. On a quarterly basis, the Compliance Team reports to the IGIS on developments relating to each of its functions including investigations, policy matters, audits and training.

In addition, during 2014/15 the Chief Legal Adviser was established as a permanent position. The Chief Legal Adviser is the principal legal adviser to the Director GCSB, and provides legal advice on all matters relating to the operational, compliance and administrative activities of GCSB.

Working with the strengthened Office of the Inspector-General of Intelligence and Security

Since 1996, both GCSB and NZSIS have been subject to oversight by the Inspector-General of Intelligence and Security (IGIS). The statute governing the office and functions of the IGIS was amended in 2013 alongside the GCSB Act. A number of changes were made to strengthen the Office of the IGIS, including increasing the

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

resources of the office to enable a greater range of activities to be carried out, and expanding the IGIS's statutory work programme and enhancing the corresponding reporting requirements.

The current IGIS, Cheryl Gwyn, was appointed in May 2014. During the 2014/15 year, GCSB has worked with Ms Gwyn and her office to ensure that we are facilitating the work of the IGIS to the best of our abilities. This has included regular monthly meetings to ensure that the IGIS is aware of GCSB policy development, and to facilitate prompt responses to any inquiries the IGIS or her office makes. The IGIS and her staff also make unscheduled visits to conduct audits.

During 2014/15, GCSB has responded to the IGIS's formal inquiries into allegations concerning GCSB's interception activities in the South Pacific, and GCSB's process for determining its intelligence activity. GCSB also responded to a formal inquiry by the IGIS into whether there was any engagement by New Zealand's intelligence agencies with the Central Intelligence Agency's detention and interrogation of detainees between 17 September 2001 and 22 January 2009. All inquiries are ongoing.

The first full year of the Telecommunications (Interception Capability and Security) Act 2013

The Telecommunications (Interception Capability and Security) Act 2013 (TICSA) came into effect on 11 May 2014. It established new obligations for New Zealand's telecommunications network operators in the area of network security and made some changes to existing obligations around interception capability. GCSB is responsible for administering the network security provisions of TICSA, which are set out in Part 3 of the Act.

Part 3 of TICSA established a framework under which network operators are required to notify GCSB (through the National Cyber Security Centre - NCSC) about changes and developments within their networks, as these changes can impact New Zealand's national security.

Prior to the commencement of TICSA, GCSB began engagement with network operators to establish a guidance document to assist them in understanding their new obligations under the Act. In May 2015, at the one year anniversary of TICSA, GCSB began work to review and refresh that guidance.

Throughout the 2014/15 year, GCSB presented to network operators and others involved in the telecommunications industry at a series of conferences and industry events. This provided the opportunity for GCSB to provide regular updates on the implementation of TICSA and to demonstrate to industry partners our commitment to involve them in the ongoing review of both the implementation and application of the

new legislation. GCSB has welcomed the open and honest feedback provided by network operators through this engagement.

During 2014/15, GCSB received a number of notifications from network operators. In each case, GCSB was able to share information about the identified risk with the network operators involved to enable them to amend their proposals and mitigate the potential risk.

Completing the rebalance of the Intelligence Directorate

In late 2013, GCSB initiated a Functional Review (the Review) of some operational arrangements. The Review resulted in a series of recommendations to rebalance and modernise GCSB's Intelligence Directorate, in order to ensure GCSB remains capable of meeting the New Zealand Government's intelligence needs.

One of the outcomes of the Review was a restructuring of the Intelligence Directorate to enhance its ability to focus on the analytic challenges of contemporary signals intelligence. This implementation was completed in the 2014/15 year.

Strategic initiatives

Countering advanced cyber threats

To provide cyber security services to the most significant national information infrastructures in New Zealand, GCSB has developed 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, and adds greatest value through its focus on the threats that are particularly advanced in terms of technical sophistication and/or persistence. The harms at issue – e.g. theft of intellectual property, espionage or damage to IT systems – are caused by malicious software ('malware') that cannot be meaningfully countered by commercial tools. Advanced malware is being directed against networks or systems owned by: key economic generators; niche exporters including in knowledge-intensive industries; major IT service providers; and government agencies.

In July 2014, Cabinet approved the development of a malware detection service to a number of organisations, and a further malware disruption service to a subset of these (Project CORTEX). All services of warranted capabilities may be provided only after receiving the express consent of the participating parties.

Project CORTEX will deliver a number of separate capabilities, of which some were in place, under warrant, at the end of the 2014/15 financial year. Focus has now shifted to increasing the infrastructure necessary to implement the remaining capabilities.

In addition to providing services to approved organisations, GCSB distributes cyber threat alerts and advisories to all government departments, and significant national organisations including key economic generators, niche exporters, research institutions and operators of critical national infrastructure.

New Zealand's high-grade cryptographic infrastructure

GCSB operates high-grade cryptographic infrastructure, which allows communications across government classified higher than restricted to be protected through advanced encryption. Components of the system will become unsupported when the support contract ceases on 31 December 2017.

In 2013/14, GCSB prepared an indicative business case for Government with a range of options for New Zealand's high-grade cryptographic infrastructure. The detailed business case, focusing on the preferred option, will be presented to the Government by the end of the 2015/16 financial year.

GCSB has undertaken this work with a strong focus on stakeholder engagement, because the cryptographic infrastructure will enable an all-of-government service. The Project Board is made up of representatives from the principal customer agencies.

Strengthening management of our information and communication technology

The Functional Review sought to bring about improvements to the heart of GCSB – the areas that provide our technical capabilities. One of the resulting recommendations was to create a directorate to take ownership for GCSB's existing corporate ICT, issues of ICT governance, and enterprise-grade mission software applications. It was envisaged that this new directorate would be one of three essential business pillars of GCSB, alongside that of the Intelligence and Information Assurance and Cyber Security directorates.

During the 2014/15 year, GCSB initiated and completed a project to establish a new Capability Directorate. This will enable us to pursue an integrated approach to technology and information management, resulting in effective investments that maximise our capabilities.

The Capability Directorate is now the owner, developer and operator of the common capability for GCSB. It is also positioning itself to deliver future services to a wider set of NZIC customers, and participate in any initiatives that are looking to consolidate functions or improve interoperability within the NZIC.

The Capability Directorate also now leads engagement with domestic and external agencies on technology infrastructure matters in order to ensure community-wide programmes are delivered effectively.

Capability Review

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

In 2015/16, the NZIC will provide options to Ministers on the NZIC's future configuration and activities.

Operational performance

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

Identifying and reducing New Zealand's vulnerabilities

The National Cyber Security Centre (NCSC), which sits within GCSB, provides enhanced cyber security services to New Zealand government and private sector organisations to assist them in defending themselves from cyber-borne threats. As much of New Zealand's critical infrastructure is highly interconnected and interdependent, cyber threats could have significant economic ramifications or result in environmental damage or loss of life.

During 2014/15, the NCSC acquired new access authorisations, which have strengthened GCSB's ability to assess and respond to events. These authorisations enable NCSC to:

- evaluate cyber security incidents affecting important public and private sector entities and provide timely remediation or mitigation advice;
- evaluate and investigate (where necessary) cyber security incidents affecting the information infrastructures of public and private sector entities, and provide timely remediation or mitigation advice; and
- understand the tactics, techniques and procedures of advanced and sophisticated cyber threat actors in order to assist protection of important New Zealand information infrastructures against the activities of those actors.

In addition to providing enhanced services to government agencies and critical infrastructure providers, the NCSC regularly issues cyber threat advisories on its public website. These advisories help New Zealand organisations by alerting them to risks such as vulnerabilities in commonly used software and operating platforms, through to risk and mitigation information relating to the use of mobile electronic devices.

Cyber security in action

In the 12 months to 31 December 2014 there were 147 incidents[3] recorded by the National Cyber Security Centre.

In the first six months of 2015 we recorded 132 incidents and expect that by the end of 2015 this figure will be in excess of 200.

Of the incidents recorded in the first half of 2015, 79 were reported by government agencies and 33 by private sector organisations.

A further 20 incidents were reported to us by our cyber security partners where the nature of the organisation was not identified.

These incidents range in seriousness from the targeting of small businesses with 'ransom ware' and attempts to obtain credit card information through to serious and persistent attempts to compromise the information systems of significant New Zealand organisations.

Roughly 0.5% of the data analysed through GCSB's recently developed (CORTEX) capabilities has a signature associated with some form of cyber threat.

Each month GCSB and our international cyber security partners identify around 900 new signatures.

Some of these threats come from well-resourced, sometimes state supported, foreign threat actors. While at times they are directly targeting significant New Zealand organisations, we also see them use and attempt to use New Zealand-based systems to host malware that is used to target overseas networks.

Examples of threats identified through GCSB's capabilities include:

- The use of a malware package, probably available for purchase on the internet, to target six significant New Zealand organisations. The threat was detected and mitigated through our CORTEX capabilities.
- These capabilities also helped us identify and trace the source of a new cyber attack method from a known major foreign threat source. The attack targeted several significant New Zealand organisations. The signatures of this new threat were able to be passed on to our international partners, helping to reduce the global vulnerability to this particular attack.
- We detected the large scale targeting of a nationally significant organisation as part of a global campaign by a known foreign threat source. We were able to work closely with the New Zealand organisation to contain and mitigate the threat, with no evidence of any successful compromise.
- The same capabilities enabled us to identify a previously unknown threat technique originating from a region which has long been regarded as a significant foreign threat

[3] GCSB records a cyber security incident as an occurrence or activity that impacts on the confidentiality, integrity or availability of an information system. Some variability in the number of recorded incidents year to year may relate to changes in reporting or recording practice rather than any significant change in the pattern or occurrence of actual incidents advised to or detected by us.

source. This New Zealand discovery, through our CORTEX capabilities, was internationally significant.

Another way in which GCSB helps to reduce New Zealand's vulnerabilities is through the maintenance and publication of the New Zealand Information Security Manual (NZISM).

The NZISM is the New Zealand Government's manual on information assurance and information systems security. It is published by GCSB as part of the Government's Protective Security Requirements (PSR) framework, which sets out the New Zealand Government's expectations for managing personnel, physical and information security effectively.

The NZISM is a practitioner's manual – designed to meet the needs of agency information security executives as well as vendors, contractors and consultants who provide services to agencies. It includes minimum technical security standards for good system hygiene, and provides other technical and security guidance for government departments and agencies to support good information governance and assurance practices.

During 2014/15, the third major rewrite of the NZISM took place. The revised version, published in May 2015, incorporates a substantial amount of new material including guidance on new technologies such as personal wearable devices and cloud computing. Whilst primarily intended for the use of government departments and agencies, and their service providers, it is equally useful for private sector organisations.

Increasing the security of New Zealand deployments

For the New Zealand Defence Force (NZDF), signals intelligence support is crucial to delivering force protection to deployed personnel. Throughout 2014/15, GCSB provided assistance to NZDF with SIGINT testing and training through a series of ongoing exercises. By providing access to toolsets, facilities and technical knowledge, GCSB enabled NZDF personnel to maintain and improve their skills and capability.

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

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

In 2014/15, GCSB continued to collect, process and analyse foreign intelligence to produce reports covering topics of national interest.

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

Safeguarding New Zealand against threats of violent extremism and espionage

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

Throughout the last financial year GCSB worked with NZSIS on a number of its operations relating to counter-terrorism and other matters of national security. In these instances, GCSB used its capabilities to provide technical assistance and analysis to help NZSIS achieve its objectives.

The New Zealand SIGINT Operations Centre (NZSOC)

During 2014/15, NZSOC continued its provision of a 24 hour 7 day a week watch and warn service, which alerted customers when it obtained information that could have affected the safety and/or security of New Zealanders and New Zealand entities both at home and abroad.

While the rest of the country is sleeping, the NZSOC Watch Officers are undertaking a host of tasks including:

- monitoring classified and unclassified sources to identify potential threats to New Zealand or New Zealand interests;
- assisting organisations who suspect a cyber security incident has occurred;
- talking to members of the public who call the NZSIS 0800 line to report information of security concern; and
- assisting customers with urgent requests to meet operational requirements.

Security and stability in the South Pacific

In 2014/15, GCSB maintained reporting lines focusing on regional trends and resource issues.

Statements on Interception Warrants

A total of 15 interception warrants were in force during the 2014/15 year.

A total of 9 interception warrants were issued during the 2014/15 year.

Statements on Access Authorisations

A total of 43 access authorisations were in force during the 2014/15 year.

A total of 26 access authorisations were issued during the 2014/15 year.

Advice and assistance provided to other entities

During the 2014/15 year, there were 17 instances where the Director GCSB approved the provision of advice and assistance in accordance with section 8C of the GCSB Act. In each case, the advice and assistance was approved for a period of time associated with operational needs.

Warrants and authorisations

The GCSB Act 2003 enables GCSB to secure formal authorisation to intercept communications in pursuit of two of its three functions: 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 a 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 the NZDF, NZSIS or Police with their functions (section 8C). This is because any activity carried out by GCSB with respect to section 8C of the 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.

Organisational health and capability

Performance Improvement Framework review

GCSB, along with the other core NZIC agencies, had their first Performance Improvement Framework (PIF) review in 2013/14. The findings of the PIF review confirmed those of other recent assessments, most notably the Review of Compliance, and helpfully set out a series of recommendations that, once implemented, will result in a fully fit-for-purpose GCSB.

During 2014/15, GCSB made progress in addressing a number of recommendations under the three broad PIF categories of Government priorities, core business, and organisational management.

Government priorities

With the other NZIC agencies, GCSB explored options for a collective intelligence dissemination business model to better meet the needs of customers. This work, led by DPMC, resulted in a framework that is intended to be implemented in 2015/16. GCSB proposes to introduce a new tool that will improve the presentation of intelligence reports, as well as increasing oversight and security of information. GCSB also developed an Intelligence Customer Engagement Strategy to better understand the needs of policy-makers.

Core business

The recruitment of Engagement Managers within the Information Assurance and Cyber Security Directorate, and the implementation of customer feedback mechanisms, is driving continuous improvement in the quality and delivery of GCSB products and services.

Organisational management

During 2014/15, GCSB developed a mobility programme for a structured programme of secondments for staff development purposes. The programme is expected to be implemented in September 2015 for tier 3 and 4 managers. Guidelines and tools were put in place to improve internal communications across the Bureau, and new communications products were implemented to share staff and organisational successes on operational matters.

Working together – Intelligence Community Shared Services

The Intelligence Community Shared Services (ICSS) Team had its second anniversary in April 2015. ICSS was created to improve efficiency, effectiveness and service levels, as well as greater resilience to cope with the NZIC's current and future challenges. While ICSS provides services to GCSB, NZSIS and the Ministry of Defence, GCSB is the employer of staff in the ICSS Team.

Over 2014/15, ICSS continued to provide financial, procurement, human resources, recruitment, learning and development, facilities and physical security services to GCSB and NZSIS. In March 2015, ICSS implemented a new Financial Management Information System (FMIS) to provide a single financial system for GCSB and NZSIS. FMIS gives budget managers improved tools for management and enables:

- more timely access to financial and contracting information;
- better financial forecasting; and
- improved decision making.

All three of the above areas were identified as areas for improvement in the PIF review.

Workforce planning

During 2014/15 the NZIC continued its implementation of the *One Workforce Strategy* – a programme of initiatives to facilitate lateral movement across the agencies, but also develop careers more broadly in the NZIC.

A key part of the Strategy is a single remuneration policy for GCSB and NZSIS, where jobs are equitably sized and pay ranges applied to comparable roles for both agencies. In the year under review, over 300 roles across the two agencies had been evaluated and placed in the proposed new banding structures. In addition, consultation over the new framework commenced with staff and their respective associations, with a view to full implementation being achieved in the 2015/16 year.

To support the move toward *One Workforce* and leverage opportunities for enhanced efficiency, in 2014/15 GCSB and NZSIS migrated to a single human resources information management system. This has enabled improved internal and external management reporting, increased automation of business processes, and reduced administrative and support costs.

To facilitate staff movement across the community, a number of initiatives have been undertaken to define transparent career progression opportunities for staff. One such example is the Career Pathways project, which commenced development in 2014/15 (based on arrangements already in place in GCSB's Intelligence Directorate) and will be implemented in the 2015/16 year. Under this initiative, a collective of Career Boards

will be established to meet for the purpose of considering applications from those who wish to advance their career within six different job families. This will become an increasingly important avenue for talent management and workforce planning within the NZIC.

The NZIC has continued to invest in attracting talented staff to the community. In 2014/15, work was undertaken to refresh the employment brand marketing and image of the NZIC, which was subsequently incorporated into NZIC websites, external advertising, and the materials provided to potential applicants for vacancies. As a result, we have noticed an increase in both the number and calibre of candidates that are applying for vacancies and they arrive with an enhanced understanding of the culture and functions of the NZIC.

In addition, in 2014/15 GCSB commenced an intern programme to recruit and train highly talented intelligence and cyber security graduates. The long-term objective of this programme is to build a skilled security talent pool in areas with limited skilled professionals available to us. Even in its first year of operation, it was evident that this approach is resulting in an increase in the number and calibre of applicants. This programme will continue to be nurtured, with the intention of providing further opportunities for high-potential graduates in 2015/16.

The NZIC continued to provide leadership opportunities to staff through a number of different avenues, including the Manager as Coach programme that saw approximately 100 managers participate in training aimed at enhancing their ability to act as effective coaches to their staff. This training received exceptional feedback from participants, and evidence is emerging of this capability being strengthened.

Equal employment opportunities

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

The NZIC employs on merit, as well as the ability to meet the standards required for the highest level of security clearance. The NZIC workforce is less diverse than the rest of the public sector because it is more difficult to confirm the personal information of people who have not been resident in New Zealand, or in the countries of our Five Eyes partners, for a long period of time.

In 2013/14, the ICSS examined the representation of Pacific Island and Maori people, as well as women, in leadership roles in GCSB and NZSIS. A number of recommendations out of that undertaking were addressed in 2014/15, including a DPMC-led NZIC Recruitment Strategy to target under-represented audiences, and the establishment of the *Women of NZIC* forum. The latter was introduced to provide a

networking forum for women staff, as well as to develop informal mentoring opportunities and raise awareness of contemporary issues facing women in the workforce.

GCSB STAFF	2012/13	2013/14*	2014/15*
Staff turnover	7.7%	12.1%	9.9%
EEO information			
Women	40%	36%	36%
Men	60%	64%	64%
European	48%	52%	53%
Maori	6%	6%	6%
Pacific Island	5%	2%	3%
Other/undeclared	41%	40%	38%
Equivalent full-time staff at year end	304.6	315.7	301.3

*Staff turnover figures for 2013/14 and 2014/15 include planned redundancies.

Climate survey

A climate and engagement survey was undertaken for NZIC staff in September 2014. With a 70% response rate, these results provided valuable feedback and insights for the executive teams.

Following the survey, GCSB ran a series of workshops to create action plans to address the main themes coming through in feedback:

- workload;
- reward and recognition;
- clear direction;
- flexibility and structure; and
- morale.

The workshops generated a number of concrete ideas and enabled us to take immediate steps to make positive changes. This included the introduction of a people leadership charter to guide best practice leadership behaviour and sit alongside our organisational values of courage, commitment, respect and integrity. Other changes included new or revised policies on delegations, travel, and non-financial rewards, as well as changes to aspects of the recruitment process and workforce management.

GCSB is committed to continuous improvement on staff engagement and to ensuring GCSB is recognised as a great place to work.

Financial statements

Independent Auditor's report

AUDIT NEW ZEALAND
Mana Arotake Aotearoa

Independent Auditor's Report

To the readers of the Government Communications Security Bureau's financial statements for the year ended 30 June 2015

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

We have audited:

- the financial statements of the Bureau on page 31, that comprise the statement of expenses and capital expenditure against appropriation for the year ended 30 June 2015.

Opinion

In our opinion:

- the statement of expenditure and appropriation of the Bureau on page 31 fairly reflects the Bureau's expenses and capital expenditure incurred for the financial year ended 30 June 2015 against the Bureau's appropriation for that financial year.

Our audit was completed on 30 September 2015. 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 all 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.

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.
- statements of budgeted and actual expenses and capital expenditure incurred against appropriation for 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 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 section 15 of the Public Audit Act 2001 and the Public Finance Act 1989.

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

This audit report relates to the financial statements and statement of service performance of the Government Communications Security Bureau (GCSB) for the year ended 30 June 2015 included on the GCSB's website. The Director is responsible for the maintenance and integrity of the GCSB's website. We have not been engaged to report on the integrity of the GCSB's website. We accept no responsibility for any changes that may have occurred to the financial statements and statement of service performance since they were initially present on the website.

The audit report refers only to the financial statements and statement of service performance named above. It does not provide an opinion on any other information which may have been hyperlinked to or from the financial statements and statement of service performance. If readers of this report are concerned with the inherent risks arising from electronic data communication they should refer to the published hard copy of the audited financial statements and statement of service performance and related audit report dated 30 September 2015 to confirm the information included in the audited financial statements and statement of service performance presented on this website.

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

Independence

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

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

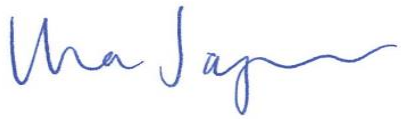
Kelly Rushton
Audit New Zealand
On behalf of the Auditor-General
Wellington, New Zealand

Statement of Responsibility

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; and
- 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 2015 and its operations for the year ended on that date.



Una Jagose, Acting Director GCSB

30 September 2015

Countersigned by:

Karen Robertson, Chief Financial Officer

30 September 2015

Statement of expenses and capital expenditure against appropriation for the year ended 30 June 2015

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

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

	$000
Total appropriation	$ 95,187
Actual expenditure	$ 86,834

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.