G.56 (2018)

Annual Report

Government Communications Security Bureau
Te Tira Tiaki

GCSB.GOVT.NZ

2018

Preface

This is the unclassified version of the annual report of the Government Communications Security Bureau for the year ended 30 June 2018. This version will be tabled in Parliament and made available to the public on the GCSB internet site (www.gcsb.govt.nz).

Much of the detail of the work undertaken by the GCSB has been omitted from this unclassified version of the report for reasons of security. This is necessary to protect the ongoing ability of the GCSB to be effective in its role as prescribed in the Intelligence and Security Act 2017.

Presented to the House of Representatives pursuant to section 221 of the Intelligence and Security Act 2017.

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

Contents

Overview of the Year

01

Minister's Foreword

New Zealanders enjoy an enviable way of life. The values we hold dear, such as democratic government, the rule of law, and freedom of speech, define our character as a nation and underpin our economic and social wellbeing.

The development of new technologies provides citizens and countries with real opportunities and greater connectivity but even so - and to some extent because of this - the world is becoming increasingly challenging and uncertain. New Zealand's intelligence and security agencies must be agile to adapt to this changing environment.

The Government needs timely, relevant and actionable intelligence in order to protect and promote national interests. The intelligence provided by the Government Communications Security Bureau (GCSB) is critical to these efforts and informs the actions of relevant decision makers and government agencies. Over the past year the GCSB has put a lot of effort into ensuring that its intelligence reporting is timely and relevant for its customers.

Another area where there has been an increased focus on value for customers is the GCSB's cyber security services. A key way that the GCSB does this is through its CORTEX cyber security capabilities for organisations of national significance. The GCSB's significant work in this area was this year recognised with the agency awarded the Deloitte Institute of Public Administration of New Zealand award for 'Building Trust and Confidence in Government'. This is an achievement that the GCSB should be proud of, and New Zealanders should draw confidence from.

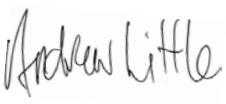
I am also pleased with the results of the State Services Commission's 2018 'Performance Improvement Framework Follow Up Review' of the New Zealand Intelligence Community. The review found that the community, including the GCSB, is delivering fundamentally better advice, services, and products than in previous years and has gained public trust and confidence in their work.

The Government has approved the expansion of CORTEX cyber security capabilities to a much larger group of organisations through the Malware-Free Networks project. Work is already underway, and I look forward to seeing this project progress over the coming years.

A significant focus of the year for the GCSB and also the New Zealand Security Intelligence Service (NZSIS) has been completing the implementation of the Intelligence and Security Act 2017. The new legislation provides clarity about the roles and responsibilities of the agencies and supports greater collaboration between them. A unique instrument under the Act is the use of Ministerial Policy Statements, which provide guidance on how the agencies should undertake certain aspects of their activities. Importantly, they are publicly available so help to further increase transparency of what and how the agencies carry out their work.

Over the past year, I have seen the proactive efforts of the Directors-General of both the GCSB and NZSIS to increase public awareness about the work done by the intelligence and security agencies, and the role they play in safeguarding our country and institutions. Sharing what they can is an important part of building and maintaining the trust and confidence of the New Zealand public, and this is something we will continue to see.

New Zealand should be confident the work the GCSB and NZSIS undertake to understand, mitigate and manage threats will continue to keep New Zealand and New Zealanders safe and secure.



Hon Andrew Little
Minister Responsible for the Government Communications Security Bureau

Director-General's Overview

The Government Communications Security Bureau (GCSB) is a SIGINT or signals intelligence agency that specialises in intelligence derived from electronic communications. We also have a statutory role in cyber security and information assurance.

Historically there has been far more focus on the agency's intelligence roles and lesser focus on its protective security functions. I believe this is changing in part due to the GCSB's focus on increased transparency and openness, but also due to global circumstances. These changes are particularly noticeable in the reporting period covered by this Annual Report.

New Zealand organisations continue to be subject to both direct and indirect cyber threats, and are being used as staging points by threat actors to target systems in other countries. To help keep the information and intellectual property of New Zealand's nationally significant organisations safe and secure, the GCSB can now provide cyber security services with their consent.

A key way we protect these organisations is through a service we call CORTEX. It is focused on detecting and disrupting complex and persistent foreign-sourced malware that is typically beyond the capabilities of commercially available tools. Over the last two years CORTEX helped avoid damage of around $67 million. The Government has agreed to expand services to a larger group of organisations through the Malware-Free Networks project. The GCSB's work during this reporting period on CORTEX was recognised at the 2018 Deloitte Institute of Public Administration of New Zealand (IPANZ) Awards receiving the award for 'Building Trust and Confidence in Government'.

During the past year the GCSB, on behalf of the Government, added New Zealand's voice to international condemnation of two malicious cyberattacks carried out by state-sponsored actors. Although New Zealand was not the direct target of these campaigns, this sort of malicious activity is against our values. To support each condemnation the GCSB carried out a robust attribution process. These attacks include NotPetya, which was attributed to Russia and WannaCry, which was attributed to North Korea. Work to attribute a third malicious cyber campaign which targeted overseas political institutions, businesses, media and a sporting organisation was also carried out. The GCSB recently attributed this activity to the Russian Military General Staff Main Intelligence Directorate (GRU).

The important intelligence work undertaken by the agency directly contributes to the safety and security of New Zealanders and our national advantage. The world continues to be a challenging and ever changing place in which the Government needs timely, relevant and actionable intelligence in order to protect and promote the national interests. All of the GCSB's work is guided by the Government's intelligence priorities. Key areas of the GCSB's intelligence effort include cyber-threats, counter-terrorism and security threats in our region.

The GCSB has been engaged in a significant change process to improve the value and usability of its intelligence products for our customers. During 2017/18 the GCSB provided intelligence products to 19 Ministers and agencies. The intelligence was generated through the GCSB's own capabilities, as well as partner reporting.

Another significant focus of the year has been the implementation of the Intelligence and Security Act 2017. The new legislation provides clarity about the roles and responsibilities of the GCSB and NZSIS and supports greater collaboration between them. Under the legislation the GCSB must satisfy the Minister Responsible for the GCSB that sharing intelligence with foreign agencies, including our Five Eyes partners, accords with all human rights obligations recognised by New Zealand law.

Establishing the systems, policies and processes that support staff to undertake their roles and be compliant with new legislation has been a major undertaking. As with any new legislation, there is no existing case law, which means extra care is required when establishing a working understanding of the law.

The independent oversight provided by the Inspector-General of Intelligence and Security was strengthened under the Intelligence and Security Act. I am pleased that for the fourth year in a row she has found the GCSB's systems and processes to be fully compliant and that our staff have a strong culture of legal compliance.

The GCSB welcomed the release of the Inspector-General's report about its intelligence activity in relation to New Zealand's interests in the South Pacific region. The report found the GCSB operated within the statutory authorisations for it to lawfully undertake collection of signals intelligence.

In order to be successful in our mission, the GCSB requires the best and brightest minds and the broad range of perspectives that come from having a diverse workforce. To accomplish this, the GCSB has taken a proactive approach to increase its diversity. While more work still needs to be done, I am pleased with the progress we have made in a relatively short time.

New Zealand benefits greatly from the work dedication, talent and professionalism of the GCSB staff. The work they do is demanding and I am incredibly proud of their ability to consistently rise to the challenge.

Andrew Hampton
Director-General of the Government Communications Security Bureau

The GCSB has been engaged in a significant change process to improve the value and usability of its intelligence products for our customers.

Notable Achievements

Impenetrable Infrastructure

- **CORTEX has continued to reduce harm from hostile cyber activity** — Analysis undertaken by the GCSB has determined that detection and disruption of cyber incidents by CORTEX capabilities has conservatively prevented in the order of $27 million in harm to New Zealand's nationally significant organisations in 2017/18. This means that CORTEX has reduced around $67 million of harm caused by malicious cyber activity over the last two years.
- **Expansion of the Malware-Free Networks cyber security service** — In early 2018, Cabinet approved the expansion of the GCSB's Malware-Free Networks project to become a fully formed cyber security service. The expansion of the Malware-Free Networks is a milestone in ensuring we have the tools and authority to provide active cyber protections to a much greater range of New Zealand's organisations.
- **Calling out Russia and North Korea Cyber Activity** — In 2017/18, the GCSB joined international partners in calling out the Russian Government and North Korean cyber actors for indiscriminate cyber-attacks. The NotPetya (Russia) cyber-attack and WannaCry (North Korean actors) ransomware campaign caused substantial harm and disruption to computer systems around the world in 2017. This was the first time a New Zealand Government agency has attributed hostile cyber activity to a foreign power.

Protecting New Zealand's Interests

- **Telecommunications (Interception Capability and Security) Act 2013 (TICSA)** — The GCSB has responsibility for the network security provisions set out in TICSA. During the reporting period the GCSB received 123 notifications from telecommunication network operators about proposed changes to networks that could undermine their security. The GCSB assessed these notifications on average within seven working days, a significant improvement on last year's average processing time of 10.2 days.
- **The Outer Space and High-altitude Activities Act (OSHAA) 2017** — OSHAA came into effect on 21 December 2017. The Act allows agencies, including the GCSB and NZSIS, to manage risks to New Zealand's space-related national interests and security. During the reporting period, the GCSB conducted 24 assessments on space-related activities.
- **Improving New Zealand's secure technology** — In 2017/18, the GCSB made significant progress on the Cryptographic Products Management Infrastructure (CPMI) project and the New Zealand Top Secret Network (NZTSN). Both of these are complex, multi-year projects. The CPMI project will replace parts of the system currently used to protect classified New Zealand Government information. The GCSB has completed the initial installation of this new infrastructure and the system is expected to be operational in 2019. The NZTSN will provide an enhanced suite of secure information communication technology services for a number of agencies. The GCSB has completed a design stage of this project and have commenced development of some of the core activities.

Indispensable Intelligence

- **Provision of intelligence** — The GCSB continued to supply timely and insightful intelligence to 19 government agencies and various Ministers and decision makers in accordance with priorities set by the Government. This intelligence was generated through the GCSB's own capabilities and partner reporting, and contributed to the safety and security of New Zealanders and our national advantage.
- **Inquiry into the GCSB's intelligence activity in relation to the South Pacific** — In 2017/18, the Inspector-General of Intelligence and Security (IGIS) carried out an inquiry on matters related to the GCSB's intelligence gathering activities in relation to the South Pacific. The GCSB cooperated fully with this inquiry, demonstrating ongoing efforts to be as transparent as possible about the vital work the agency undertakes. The IGIS found that the GCSB has, and operates within, statutory authorisations that allow it to lawfully collect signals intelligence in relation to New Zealand's interests in the South Pacific.
- **Countering Transnational Crime** — Since the Intelligence and Security Act (ISA) came into force in late 2017, the GCSB has expanded the support it provides to New Zealand's law enforcement and border protection agencies. The GCSB is now able to collect intelligence against New Zealanders involved in transnational crime and share that intelligence with other government agencies. The GCSB also acts as a conduit for intelligence and reporting provided by international partners. This growing partnership has enhanced New Zealand's effectiveness at countering criminal activity targeting New Zealand and its regional interests.
- **Support to Military Operations** — The GCSB continued to provide support to the New Zealand Defence Force (NZDF) in relation to their operations overseas. The GCSB contributes to the NZDF efforts to detect and counter threats to New Zealand military personnel deployed overseas.

Organisational Development

- **The Intelligence and Security Act 2017** — Since the ISA came fully into force on 28 September 2017, the GCSB and the NZSIS have devoted significant resources to successfully implementing, and being fully compliant with, the legislation. The ISA provides clarity about the roles and responsibilities of each agency and supports greater collaboration between the GCSB and the NZSIS. It has also enabled the GCSB to provide greater support to other government agencies on issues impacting New Zealand's national security, like transnational crime.
- **Performance Improvement Framework (PIF)** — In 2018, a PIF Follow Up Review found that NZIC agencies, including the GCSB, are delivering fundamentally better advice, services, and products than in previous years that now connect directly to the Government's priorities.
- **Improving Gender and Diversity Representation** — In 2017/18, the GCSB began to see positive results in efforts to improve diversity through its recruitment and employment practices. The GCSB's gender pay gap continued to trend downwards to 7.4 per cent by 30 June 2018, less than half of what it was four years ago. The GCSB's graduate recruitment programme also enjoyed an improvement in the number and calibre of women candidates applying to the programme (with just under half of the 300 applicants being women). The successful applications also featured a 50/50 gender split for the first time.

Strategic Vision

Having a strong strategy is critical to the success of any organisation, including the GCSB. With this in mind, in 2016 the GCSB established a strategic plan based on delivering two primary outcomes to New Zealand and New Zealanders.

Impenetrable Infrastructure

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

Indispensable Intelligence

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

The GCSB has recently refreshed its Strategy for 2018-2022. The refresh was undertaken to ensure that the GCSB is focussing on the right things over the next four years and is adapting to changes in its operating environment.

The two primary outcomes of Impenetrable Infrastructure and Indispensable Intelligence endure, but there have been changes to the underlying focus areas that underpin the GCSB's efforts. The GCSB's renewed focus areas are:

- Retain, develop and recruit the best people;
- Products and services that are used and valued;
- Relationships with purpose;
- Government's information security authority;
- Specialist intelligence tradecraft; and
- Trusted technology.

These focus areas are driving our planning activities for the 2018/19 financial year and beyond.

The Performance Improvement Framework

A key driver for the initial development of the GCSB's Strategic Plan was the PIF review of the New Zealand Intelligence Community (NZIC) undertaken in 2014. That review highlighted a number of significant issues for the NZIC to address and the need for the intelligence and security sector to form a closer relationship with the wider public service.

In 2018, the NZIC underwent a 'PIF Follow Up Review' led by the State Services Commission. The reviewers found that NZIC agencies are on the right track and had undertaken an "impressive catalogue of organisational change" in response to the 2014 PIF process. The PIF Follow Up Review also notes the NZIC is now delivering fundamentally better advice, services, and products than in previous years that now directly connect to the Government's priorities. The NZIC is seen as adding value to its customers and has regained public trust and confidence.

Warrants and Authorisations

The ISA repealed the Government Communications Security Bureau Act 2003 on 28 September 2017. This year's report addresses warrants and authorisations issued under both Acts.

Government Communications Security Bureau Act 2003

A total of 13 interception warrants were in force during the 2017/18 year. A total of three interception warrants were issued during the 2017/18 year.

A total of 33 access authorisations were in force during the 2017/18 year. A total of 13 access authorisations were issued during the 2017/18 year.

During the 2017/18 year, there were 14 instances where advice and assistance was provided under an authorisation by the Director of the GCSB in accordance with section 8C of the GCSB Act 2003. They were to:

- NZDF – two instances;
- NZSIS – 11 instances; and
- New Zealand Police – 1 instance.

Intelligence and Security Act 2017

Under the ISA, the GCSB warranted activity is covered by two types of intelligence warrants. A Type 1 warrant is issued for the purposes of collecting information about, or to do any other thing in relation to, New Zealanders. A Type 2 warrant is for conducting intelligence collection against non-New Zealanders. In each case, warrants may only be issued if they will contribute to the protection of national security, or the international relations and well-being, or economic wellbeing of New Zealand.

A total of 19 intelligence warrants were applied for and approved in 2017/18, of which ten were Type 1 intelligence warrants and nine were Type 2 intelligence warrants. No warrant applications were declined.

There were no urgent applications for an intelligence warrant sought under sections 71 or 72.

No applications for a joint intelligence warrant with the NZSIS were made under section 56.

There were no occasions on which the GCSB provided assistance under section 14.

No authorisations were made by the Director-General under section 78.

No applications were made to access restricted information under section 136.

A total of two business records approvals were applied for and issued. A total of 13 business records directions were issued by the GCSB to agencies under section 150.

The GCSB provided advice and assistance under section 13(1)(b) to:

- New Zealand Police, one instance; and
- NZDF, one instance.

19

intelligence warrants were issued in 2017/18.

This included:

10
Type 1 intelligence warrants.

9
Type 2 intelligence warrants.

Our Work in Detail

02

The New Zealand Intelligence Community

A dedicated community working together to contribute to the security and well-being of New Zealand and New Zealanders.

The core New Zealand Intelligence Community (NZIC) includes:

- Government Communications Security Bureau;
- New Zealand Security Intelligence Service; and
- Department of the Prime Minister and Cabinet: National Security Group.

The NZIC exists to protect New Zealand as a free, open and democratic society. The intelligence-based insights and advice this community provides to the Government enables decisions to be made which protect and enhance New Zealand's security and well-being. The NZIC contributes to the following policy outcomes:

- Keeping New Zealand and New Zealanders safe by giving the 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 Government and key economic entities to protect their information, assets and people.
- Advancing New Zealand's interests internationally through the collection and assessment of intelligence pursuant to New Zealand's foreign policy goals.

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

National Intelligence Priorities

Everything the intelligence community does is carried out in response to the National Intelligence Priorities (NIPs). These priorities are set by the Government periodically and drive intelligence collection, assessments and reporting activities.

Success in delivering against the expectations set out in the NIPs requires cross-sector intelligence work and involves other New Zealand agencies such as the New Zealand Defence Force, New Zealand Police, New Zealand Customs Service, the Ministry of Business, Innovation and Employment, and the Ministry of Foreign Affairs and Trade.

Strategic Operating Environment

New Zealand's security and intelligence agencies operate in a complex, challenging and uncertain domestic and international security environment.

Cyber Security

New Zealand's cyber threat environment is complex and far from benign. The threats we see are both direct (deliberate attacks on New Zealand organisations and people) and indirect (indiscriminate international cyber threat campaigns). We continue to see a range of international threat actors targeting New Zealand systems and infrastructure for financial gain or as a means of advancing their own position.

Additionally, an increasing number of international incidents creates collateral victims or economic consequences in New Zealand. New Zealand's cyber adversaries continue to use cyber operations for a variety of purposes. Motivation varies from espionage to revenue generation and stealing intellectual property or sensitive information.

Foreign Interference

While many states promote a positive image, cultivate influence abroad and conduct intelligence activities, the scale and aggressive nature of this activity is on the rise around the world. The method, technologies and defences used to undertake and obscure espionage and foreign interference activities have continued to change over time. Hostile cyber activities, in particular, are increasingly a key tool for foreign states to project their influence abroad, including into New Zealand.

Security in the Pacific

The Pacific is becoming an increasingly contested international region, with various states seeking to project influence and power into the region. These efforts have the potential to have a detrimental effect on regional security and could negatively impact New Zealand's interests in the region.

Foreign criminal networks are also targeting the Pacific and seeking to scale-up their activities. Transnational crime has the ability to rapidly proliferate and affect other countries in the region, including in New Zealand.

Violent Extremism

Threat of harm from violent extremism continues to be a security issue both internationally and for New Zealand. While the Islamic State of Iraq and the Levant has experienced significant losses of territory and capability over the last year, the group remains active on the world stage, seeking to spread radicalising propaganda online and inspire terrorist attacks around the world. Additionally, other groups, such as al-Qai'da, also remain an active threat to security.

The online proliferation of extremist content and ideologies remains a threat to the safety of New Zealanders. Such material is accessible in New Zealand, and is known to be read and distributed by New Zealanders.

Impenetrable Infrastructure

03

Cyber Security

The Government Communications Security Bureau works to make New Zealand's information infrastructure impenetrable to technology-borne compromise.

The GCSB's efforts to provide impenetrable infrastructure is undertaken through its cyber security and information assurance services, and through the provision of secure information technology infrastructure to the New Zealand Intelligence Community (NZIC). We also play a role in regulating telecommunications network operators to ensure the security of nationally significant infrastructures.

By providing these services across government agencies and to other nationally significant organisations, the GCSB enables New Zealand to operate while protecting its most sensitive information.

New Zealand's systems and infrastructure have been targeted by threat actors as a means of advancing their own political, social or economic interests. International incidents that do not specifically target New Zealand have resulted in collateral victims or consequences in New Zealand nonetheless.

During the reporting period, the GCSB recorded 347 cyber security incidents. These incidents were recorded through a combination of our own cyber security capabilities and information shared with us by our international partners. Each incident represents an effort by a hostile actor to breach the cyber defences of a government agency, nationally significant organisation or key business.

These incidents included:

- A New Zealand company's systems communicating with a server likely compromised by a hostile state-sponsored actor;
- Two organisations of national significance experienced their information systems being compromised by an unknown malicious cyber actor; and
- A New Zealand organisation's IP address connecting with a webserver compromised by a sophisticated hostile cyber actor.

Over a third of the incidents recorded were likely conducted by state-sponsored actors.

In 2016/17, the GCSB recorded 396 incidents, which was 49 more than in 2017/18. The number of incidents recorded will fluctuate from year to year for a variety of reasons, including the technology and techniques used by hostile cyber actors, or the cyber security capabilities deployed by the GCSB, international partners and customers.

This year the GCSB also joined international cyber security partners in calling out Russia for the NotPetya cyber-attack and North Korean cyber actors for the WannaCry ransomware campaign respectively. While not directly targeting New Zealand organisations these sort of reckless and malicious cyber activities have the potential to cause substantial harm and disruption on a global scale.

National Cyber Security Centre

The GCSB's National Cyber Security Centre (NCSC) deals with advanced cyber threats that have the potential to affect New Zealand's national security and the economy. The NCSC provides advanced cyber threat detection and disruption services and cyber threats analysis and assessment to our customers and partners.

The NCSC works with government departments, key economic generators, niche exporters, research institutions and operators of critical national infrastructure to counter these threats.

The NCSC also works closely with the Computer Emergency Response Team New Zealand (CERT NZ), to provide guidance and assistance with cyber threats. NCSC works primarily with nationally significant organisations. CERT NZ helps businesses, organisations and individuals wanting prevention and mitigation advice on day-to-day online security issues.

Outreach and Customer Engagement

A key part of NCSC's role is to raise awareness of cyber security risks in New Zealand. This includes explaining how the GCSB and other agencies such as the CERT NZ provide assistance to those affected by malicious cyber activity. The focus is on helping key stakeholders develop their own understanding of cyber security best practice.

2017/18 NCSC's customer engagement included:

- Issuing monthly Cyber Threat Summaries and monthly Cyber Bulletins.
- Introducing a series of sector focussed reports and a quarterly Cyber Security Insights for Executives report specifically for senior executives.
- Co-hosting four regional forums and 21 Security Information Exchanges.
- Conducting 250 customer cyber security resilience assessments.

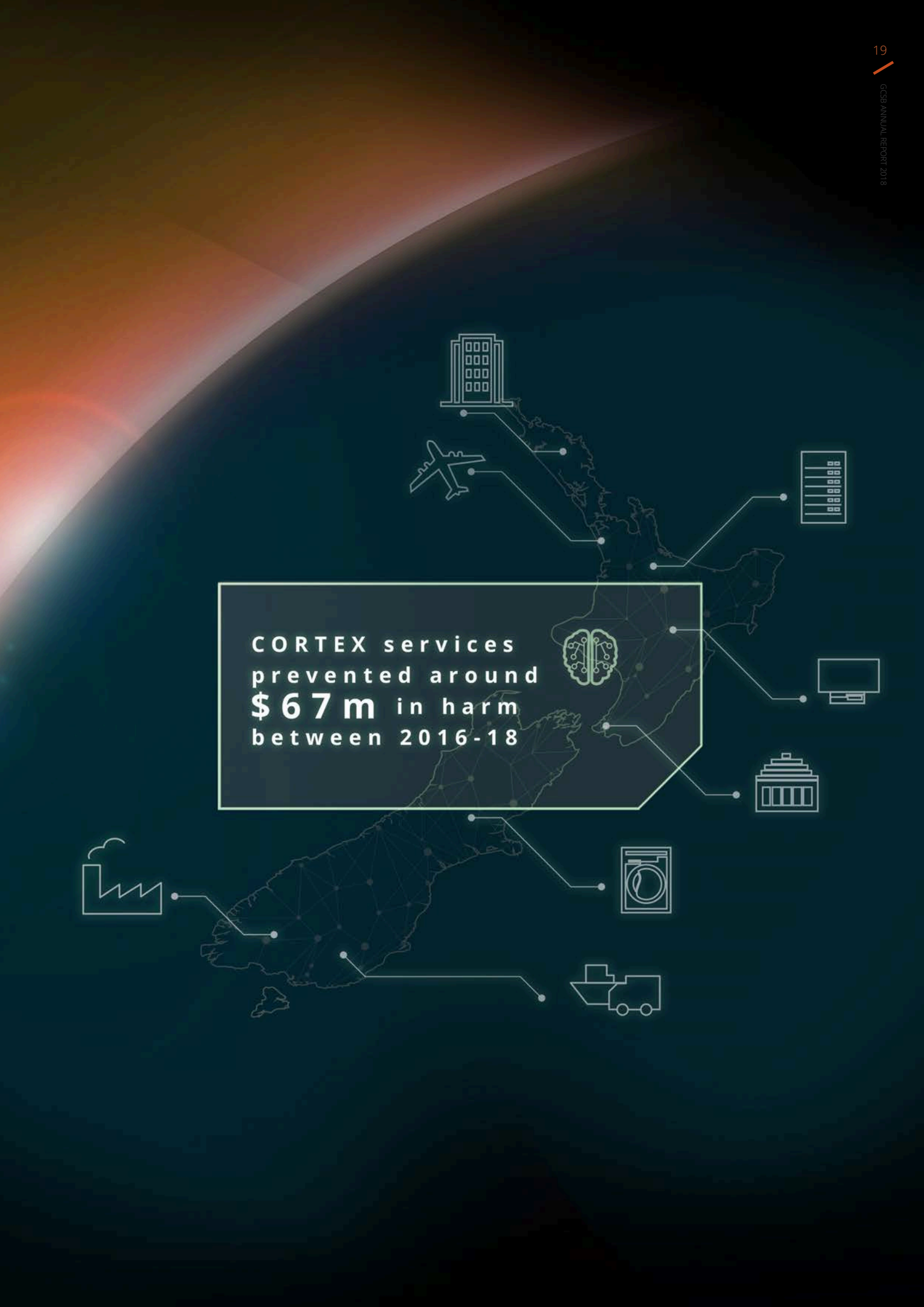
The GCSB recorded

347

cyber-security incidents.

State sponsered incidents

The number of state sponsored incidents detected has increased from last year, from 122 in 2016/17 to 134 in 2017/18.


CORTEX services
prevented around
$67m in harm
between 2016-18

CORTEX Cyber Security Services

The GCSB supports nationally significant organisations to protect their networks from malicious, advanced, persistent and sophisticated cyber security threats through network defence capabilities, tools and expertise that are not typically available to the public. This suite of capabilities is collectively known as CORTEX. The NCSC only provides these services with the express consent of the organisations involved.

CORTEX began life as a three-year project that was completed during 2016/17. This project represented a significant achievement for the GCSB and provided a sizable uplift in New Zealand's cyber defence capabilities. After the successful implementation of the initial project, the CORTEX capabilities have become a key tool in the GCSB's cyber defence arsenal.

Independent analysis has determined the harm reduced to CORTEX customers by the detection and disruption of cyber incidents to be in the order of $27 million in the year to June 2018.

Since transitioning CORTEX into an ongoing service, the GCSB has focussed on broadening its engagement with nationally significant organisations to increase their overall network resilience security posture.

Malware-Free Networks

As part of the CORTEX development, in 2015 the GCSB gained Cabinet approval to pilot an 'active disruption' capability to counter cyber threats to organisations of national significance. This Malware-Free Networks capability was successfully trialled with an internet service provider.

In March 2018, Cabinet approved the GCSB to continue the development and implementation of Malware-Free Networks in order to provide the cyber security service to a wider range of New Zealand's organisations of national significance by June 2020. The expansion of Malware-Free Networks is a milestone in ensuring we have the tools and mandate to provide active cyber protections to a much greater range of New Zealand's organisations of national significance.

Reducing the harm caused by hostile cyber activity

Independent analysis conservatively estimates that over the last two years, CORTEX services have prevented around

$67 million

in harm caused by sophisticated hostile cyber activity against nationally significant organisations.

Information Assurance

The GCSB provides protective security advice and information assurance services to the New Zealand Government. This includes providing technical expertise, specialised technology, and regulatory oversight to protect New Zealand's most important information and infrastructure and to enable the Government to protect its most sensitive information.

The GCSB also began planning for acquiring functional leadership for information security as the Government Chief Information Security Officer (GCISO). This builds upon GCSB's existing mandate and role. The GCSB has established an Information Security Policy and Research unit to provide additional policy advice about information security best practice across government.

High Assurance Services

The GCSB's High Assurance Services (HAS) unit provides technical inspection services and advice during the establishment of New Zealand Government facilities that are designed to hold classified information. These inspections seek to ensure that such facilities are free from vulnerabilities that would allow unauthorised access to information. The HAS unit also has a mobile capability to inspect existing facilities for signs of technological efforts to compromise security.

Additionally, the Director-General of the GCSB is the New Zealand Government's accreditation authority for highly-classified information systems and sites. This means that the Director-General provides accreditation of the information security standards for such systems and sites.

Space and High-altitude Activities

Space is an exciting and fast-evolving industry which is providing a number of economic opportunities for New Zealand.

There are a number of space-related enterprises developing in New Zealand, including Rocket Lab's launch activities in Mahia, projects being led by local universities and foreign companies wanting to establish space-related industries here.

New Zealand is perceived to be an ideal location to conduct space-related research and development. This is in part due to positive official support towards enabling space enterprise.

In order to provide regulation and oversight to this rapidly growing sector, the Outer Space and High-altitude Activities Act (OSHAA) 2017 was enacted in December 2017.

An important purpose of OSHAA is to manage risks to New Zealand's national security and national interests. The Act enables the GCSB and the NZSIS to conduct national security risk assessments for all activities licensed or permitted under OSHAA. These assessments inform consultation between the Minister responsible for OSHAA (the Minister for Economic Development) and the Minister Responsible for the GCSB and NZSIS about the security risks associated with each activity.

During the reporting period, the GCSB and the NZSIS conducted 24 assessments on space-related activities from New Zealand. These assessments covered multiple launches, space payloads and high-altitude vehicles.

Telecommunications (Interception Capability and Security) Act 2013

The telecommunication industry is a core part of New Zealand's infrastructure and is critical to the daily lives and wellbeing of New Zealanders, and New Zealand's economic strength and national security. The GCSB plays a key role in supporting this sector to have resilient robust infrastructure and a strong standard of information security.

The enactment of the Telecommunications (Interception Capability and Security) Act 2013 (TICSA) gave the GCSB responsibility for administering New Zealand's telecommunications network security. The network security provisions set out in Part 3 of TICSA require network operators to notify the GCSB of proposed changes to their network infrastructure within areas of specified security interest.

In cases where these changes may cause network security risks, the GCSB also assesses the mitigation proposals network operators are required to provide to address the network security risk.

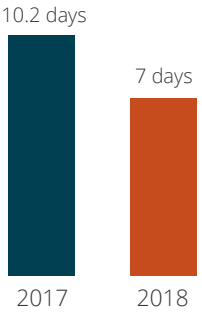
Telecommunications infrastructure is constantly evolving and network operators are always looking for technology to improve the quality of their services. Over the coming years, the advent of 5G mobile technology will drive broad technological change across the telecommunication sector. The breadth and depth of this change will likely test both the TICSA legislation and the ability of the GCSB to administer it. With this in mind, the GCSB are looking at ways to prepare for this change to the sector.

TICSA Notifications

In 2017/18, the GCSB received

123

notifications under TICSA Part 3.



The GCSB responded to these notifications on average within seven working days. This was a significant improvement on the previous year's average processing time of 10.2 days.

The majority of notifications did not raise a network security risk. With those that did, the GCSB worked with the relevant network operator to ensure that potential risks were either eliminated or mitigated. This engagement allows network operators to change and upgrade their infrastructure in a secure manner.

Secure Technology

The GCSB is responsible for the delivery of secure information technology infrastructure to the NZIC. As this sector, which includes the GCSB, handles the most sensitive information held by government, it requires specialist expertise, capabilities and ongoing support to protect that information.

This role includes the GCSB being New Zealand's national authority for communications security (COMSEC). In this capacity the GCSB provides the technology, processes and key material used to protect the country's most sensitive data at rest and in transit. The GCSB is also leading the development of several significant, complex, multi-year programmes, including:

- The Cryptographic Products Management Infrastructure (CPMI) project; and
- The New Zealand Top Secret Network (NZTSN).

These programmes will improve security arrangements across government, facilitate better collaboration between the NZIC and their domestic and international partners, and improve the reliability and resilience of the tools used by the intelligence and security sector.

The GCSB and NZSIS also began work to establish a shared Technology Directorate to share resources and expertise in order to lead technical innovation and development across the intelligence and security sector. This Directorate, hosted within the GCSB, will work to ensure that the sector's core information infrastructure is fit for purpose.

High-grade Cryptographic Infrastructure

The 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.

In 2017/18 the GCSB made substantial progress on the multi-year CPMI project. This work will replace parts of the infrastructure currently used to protect classified New Zealand Government information. The GCSB completed the initial installation of the new infrastructure. The new infrastructure will support a number of other government agencies in the sector, most notably NZIC, NZDF, MFAT and New Zealand Police. It is expected to be operational in 2019.

Top Secret Network

The NZTSN is a programme to develop a modern secure infrastructure and integrated set of capabilities, which will provide a set of shared information communication technology services for the New Zealand security and intelligence sector.

In 2017/18, the GCSB completed the design stage of the core capabilities for the NZTSN and have commenced build a number of the capabilities. This work will replace a number of legacy systems with infrastructure that is more flexible and easier to maintain. The resilience and interoperability of core systems will be improved as well. The new capabilities will be provisioned and operated by the GCSB.

Indispensable Intelligence

04

Intelligence Collection

The Government Communications Security Bureau (GCSB) provides intelligence to Ministers, government agencies and international partners in order to generate unique policy and operational impacts for New Zealand.

The GCSB is New Zealand's primary source of Signals Intelligence (SIGINT). As a SIGINT agency, we produce intelligence by analysing communications data assessed as having an intelligence value.

In 2017/18, the GCSB supplied intelligence products to 19 government agencies and various Ministers. These intelligence products were generated through the GCSB's own sovereign collection operations and partner reporting.

The GCSB's intelligence collection and analysis role enables us to contribute to the protection of New Zealand's national security, New Zealand's international relationships and economic well-being and the safety, security and well-being of New Zealanders. The GCSB also aims to provide intelligence to support security in our region and support New Zealand agencies to carry out their functions.

The GCSB collects and analyses intelligence in accordance with the policy and priorities set by the New Zealand Government. The GCSB may provide intelligence, and any analysis of it, to the Minister Responsible for the GCSB, the Chief Executive of the Department of Prime Minister and Cabinet, or any person or class of person the Minister authorises to receive it—including other New Zealand agencies and foreign partners.

The act of collecting and examining this information is carried out in accordance with New Zealand law and is subject to strong independent oversight. For any intelligence gathering which takes place under a legal warrant, there is rigorous and robust processes in place to assess the need for a warrant and its contribution to the protection of national security or the international relations and well-being or economic well-being of New Zealand before it can be issued. With the enactment of the Intelligence and Security Act 2017 (ISA), the GCSB's warranted activity is covered by two types of intelligence warrants:

- A Type 1 warrant is required for the purposes of collecting information about, or to do any other thing directly in relation to a New Zealander, and must be issued jointly by both the Minister Responsible for the GCSB and a Commissioner of Intelligence Warrants. The Commissioner must be a former High Court Judge.
- A Type 2 warrant is for targeting non-New Zealanders and is issued by the Minister Responsible for the GCSB.

All warrants are subject to review by the Inspector-General of Intelligence and Security (IGIS) after they are issued.

Regional Security

The Pacific is becoming an increasingly contested international space, with various state actors projecting influence and power into the region. These efforts have the potential to have a detrimental effect on regional security. Additionally, transnational crime has the ability to rapidly proliferate and affect other countries in the region, including New Zealand.

The GCSB provides signals intelligence in relation to our national interests in the South Pacific. This work is focussed on providing insights that support other New Zealand agencies' capabilities to respond to security issues in our region.

In 2017/18 the IGIS carried out an inquiry on matters related to GCSB's intelligence gathering activities in relation to the South Pacific. This report noted that GCSB has statutory authorisations to lawfully collect signals intelligence in relation to New Zealand's interests in the South Pacific.

Government Agencies

One of GCSB's principal objectives is to contribute to the protection of New Zealand's national security and well-being, by supporting the safety of New Zealanders at home and abroad.

A core component to this work is supporting other government agencies to carry out their work. Under the ISA, one of GCSB's functions is to cooperate with the New Zealand Security Intelligence Service (NZSIS), New Zealand Police, and the New Zealand Defence Force (NZDF) for the purposes of facilitating the performance of their duties.

Working with New Zealand's Law Enforcement Agencies

The ISA has enabled GCSB to provide more support to New Zealand domestic law enforcement agencies than was previously possible. Under the ISA's Type 1 intelligence warranting system GCSB can seek authority to collect intelligence against New Zealanders involved in transnational crime and share that intelligence with other government agencies.

GCSB also acts as a conduit for intelligence and reporting provided by international partners for other domestic agencies. We work closely with New Zealand Police, Immigration New Zealand and Customs, as well as with foreign partner agencies to deliver on this priority. This has enabled these agencies and GCSB to be more effective at countering criminal activity targeting New Zealand and its regional interests.

Supporting NZDF

In 2017/18, GCSB continued to provide support to the NZDF in relation to their operations overseas. Support 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.

Countering 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.

Continual Improvements

Continuous improvement of expertise and knowledge, technology and reporting products is critical to the ongoing ability of GCSB to deliver indispensable intelligence to our customers.

Skills and Processes

In 2017/18, GCSB set out to create an innovative and supportive environment that allows operational staff to propose new ways of doing their work. This work included consulting with the United States of America's (USA) National Security Agency and the Australian Signals Directorate to create new methodologies for addressing difficult intelligence collection issues. This work programme led to the development of new vectors for obtaining intelligence and the enhancement of existing intelligence sources. It also led to an enhanced ability to investigate and mitigate cyber-attacks on New Zealand infrastructure.

Customer Engagement

Since early 2017, GCSB has continued a joint programme of work with the NZSIS and Department of the Prime Minister and Cabinet to improve our approach to provision of intelligence and assessments to support customers. This year our efforts have focussed on four areas for improvement:

- Understanding the customers' needs and tailoring intelligence to respond to that need;
- Distributing intelligence effectively (as and when the customer needs it);
- Building customers' capability to understand and use intelligence; and
- Building our own capability to better deliver intelligence that matters to customers.

Since September we have been working with small groups of customers, to address each of these areas and trial different ways of delivering intelligence in response to the particular demands of each group of customers. Our cross-agency team has trialled changes which has ensured that services are coordinated and leverage the strengths each agency brings.

Trials have shown us that customers prefer the New Zealand Intelligence Community to operate as one team, and they value opportunities to discuss intelligence and assessments with our subject matter experts. Positive feedback was also received for our efforts to provide more material at lower classifications and for the provision of a regular programme of capability building to assist customers to understand and use intelligence in their own work.

Intelligence Collection Capabilities

Encryption is foundational to the security of communications and is important to help ensure privacy and to protect sensitive communications. GCSB is a strong supporter of New Zealanders' use of encryption technology to protect their privacy and sensitive information. However, encryption also poses challenges for law enforcement and national security as it can be used to conceal unlawful activity such as terrorism or organised crime.

To address the challenge that developing technologies and enhanced security practices present to GCSB's lawful intelligence gathering activities, we persist with significant endeavours in technology and tradecraft that allow us to collect useful intelligence in accordance with the priorities of the New Zealand Government. GCSB has continued efforts to design and deliver the capabilities that will allow us to remain a highly effective intelligence agency today and into the coming years.

International Partnerships

Five Eyes

Alongside Australia, Canada, the United Kingdom and the USA, New Zealand is a member of an international intelligence partnership known as the Five Eyes. This partnership allows New Zealand to draw on greater support, technology and information than would otherwise be available to us. Participation in this community is fundamental to GCSB's efforts to progress New Zealand's national interest and ensure the wellbeing of New Zealanders. We could not deliver our current level of security and intelligence activity alone.

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's participation in the Five Eyes partnership is always in accordance with New Zealand law and with the law of the country which is sharing information or other support with us.

Other International Partners

Alongside participation in the Five Eyes partnership, GCSB works with a range of other nations that share New Zealand's commitment to human rights and the rule of law. GCSB's partnership with other nations or participation in multilateral organisations is dependent on an assessment of the other state's human rights record.

Cooperation extends to the sharing of intelligence and intelligence collection capabilities, best-practice, knowledge and expertise. These efforts are undertaken to help the states involved (including New Zealand) counter threats like violent extremism and hostile cyber activities.

GCSB has procedures in place to ensure that any intelligence sharing with other countries in these groups is managed in compliance with New Zealand's law, including all human rights obligations recognised by New Zealand law.

Our People

05

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

The Director-General

Andrew Hampton began his term as 'Director, Government Communications Security Bureau (GCSB)' in April 2016. With the enactment of Intelligence and Security Act 2017 (ISA) the title of the Director the GCSB changed to Director-General of the GCSB.

Beyond the specific responsibilities set out in the ISA 2017, the Director-General has the following responsibilities (set out in section 32(1) of the State Sector Act 1988):

- Stewardship of the 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 Director-General of the GCSB;
- The tendering of free and frank advice to Ministers, as well as the integrity and conduct of the employees for whom the Director-General is responsible; and
- The efficient and economical delivery of the GCSB services and the effective provision of those services, ensuring they contribute to intended outcomes.

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

Senior Leadership Team

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

The SLT meets regularly to focus on the 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, the SLT includes the following roles:

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

The roles of Director Technology, Chief Financial Officer, and Chief People Officer lead functions that are shared with the New Zealand Security Intelligence Service (NZSIS).

Recruit the Best People

The GCSB is a Public Service Department with 431 full-time equivalent staff.

The GCSB is able to deliver positive security and intelligence results for New Zealanders because of the unique skills, innovation and drive of its people.

Attracting and retaining a high calibre workforce through recruitment and ongoing professional development remains crucial to the ongoing success of the New Zealand Intelligence Community (NZIC). Over the last year, work programmes have been initiated to foster an inclusive and diverse workplace which reflects the changing landscape of the environment we operate in. The GCSB employs people from a wide range of disciplines, including foreign language experts, communications and cryptography specialists, engineers, technicians and support staff.

Over the long term it is people, more than technology, that generate the unique value the GCSB's customers are seeking. The technical expertise that the GCSB requires is in high demand and is drawn from an increasingly competitive market. Accordingly, efforts to attract and provide fulfilling career options for New Zealand's top talent are critical to our ongoing success.

Workforce Planning

In 2017/18, the GCSB and the NZSIS have been working to a National Security Workforce programme which sets out our current and future workforce requirements. This workforce planning is based on providing the capability and capacity to deliver the security and intelligence outcomes expected by the Government.

The skillset needed in the intelligence community has changed over the years and this is something that is continually assessed to make sure we have the right capability in place. In 2017/18, the GCSB has focussed on establishing a robust approach to workforce and resource planning to ensure all recruitment activity is aligned with the GCSB's strategic objective of providing capability to deliver today and in the future.

Beyond Ordinary Careers

In 2017/18, the GCSB refocussed its 'Beyond Ordinary' recruitment brand to place greater emphasis on career pathways and to appeal to diverse range of candidates. This change of approach has also led to an increase in the quantity of NZIC applicants applying through the Beyond Ordinary website.

This has included the GCSB sending representatives to career fairs held at New Zealand universities, encouraging applicants from our 'Women in STEM' scholarship programme to consider applying to the GCSB Graduate Recruitment programme, and developing recruitment advertisements to appeal to people from a diverse range of backgrounds.

Work has begun to better understand the experience of potential recruits seeking to join the NZIC. This work is aimed at developing better ways to maintain candidate interest in joining the NZIC and on improving our approach to recruiting women and people from ethnically diverse communities.

Pipeline of Talent

The GCSB runs a graduate recruitment programme to attract exceptional new talent into the organisation. It encourages graduates to get a wide range of experiences within the GCSB before they areto a permanent role.

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

Over 2017/18, the GCSB has been working to attract a more diverse range of candidates through the graduate recruitment programme, including people from diverse ethnicities and more women candidates. Of the 300 people who applied to the 2017/18 graduate recruitment programme, just under half were women. The successful applications for the 2019 graduate intake features a 50/50 gender split.

Career Pathways

The Career Pathways and Career Board systems were introduced within the GCSB in 2015/16. 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.

The GCSB continues to grow and develop staff through the Career Pathways framework. Between 1 July 2017 and 30 June 2018, the GCSB had 37 applications for progression through the Career Board system. Thirty one staff progressed through, recognising their higher level of technical competence.

GCSB Core Unplanned Staff Turnover (2014 to 2018)

GCSB staff	2014/15	2015/16	2016/17	2017/18
Staff Turnover	9.8%	9.3%	6.9%	7.1%
Public Service	10.9%	11.1%	11.5%	12.1%

Skilled staff

The GCSB and the NZSIS support staff to develop and maintain the most up-to-date skills, knowledge and capability so they can support and deliver complex and technically challenging operations.

This year work was done to increase the number and quality of internal and external professional development courses available to staff. Key relationships were formed and strengthened with universities, New Zealand Police, New Zealand Defence Force (NZDF) and several independent training providers to develop learning opportunities that are especially relevant to the intelligence community.

Leadership Development

Equipping and developing leaders as the organisation grows and evolves remains a priority across the NZIC. In the last financial year, the NZIC revised and updated the leadership competency framework to align with the State Services Commission's Leadership Success Profile. The core competencies expected of leaders have been included within their performance and development review.

A leadership training and development prospectus was created to outline development and training available to staff. A mentoring framework for leaders is also in the early stages of implementation.

To support and inspire the careers of women in the wider intelligence community, a mentoring programme began in June 2018. The programme comes under the National Security Workforce programme led by Department of Prime Minister and Cabinet to create pathways and is part of our work to retain women working in the security sector.

Staff Retention

Staff retention is critical for the GCSB, particularly given the unique and demanding environment staff operate in and the time involved in recruiting, vetting and training suitable personnel.

Both the GCSB and NZSIS continue to look at further opportunities to retain talented people. Providing staff with a clear view of career pathways, and increased focus on learning and development throughout the intelligence and security sector has been a positive way to retain skills in the sector and foster career progression.

Diversity in the Workforce

The GCSB seeks to ensure its workforce reflects the diverse population that we 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 will be better able to build trust and confidence in the communities we serve with a workforce that is more representative and reflective of the make-up of New Zealand.

The GCSB is committed to developing a diverse, dynamic and agile workforce able to harness the benefits of different ideas, perspectives and cultural experiences. We have identified that there is an opportunity for us to make significant inroads with gender, Māori, and Pasifika.

In November 2017, the GCSB and NZSIS jointly launched the Diversity and Inclusion Strategy. This provides a blueprint of the steps the organisations are committed to take and clearly defines four goals around workforce diversity, leadership diversity, workforce inclusion and sustainability and accountability.

GCSB Staff Ethnicity (2014 to 2018)

Ethnicity	2014/15	2015/16	2016/17	2017/18
New Zealand European & European	66.0%	69.0%	68.7%	67.6%
New Zealander	N/A	N/A	N/A	27.5%
New Zealand Māori	7.5%	6.5%	7.2%	7.8%
Asian	6.75%	5.8%	5.4%	4.9%
Pacific Peoples	3.17%	1.6%	1.8%	2.8%

A 'total response' method has been used when calculating the ethnicity distribution, counting employees who identify with multiple ethnicities, once for each ethnicity declared. In earlier years, not every ethnicity identity was reported on. Metrics are taken 'as at 30 June' of the relevant year. This year is the first time GCSB has reported "New Zealander" ethnicity. Accordingly, the figures for 2017/18 add up to over 100%.

Supporting Women in STEM

The GCSB is undertaking a Women in STEM (science, technology, engineering and mathematics) scholarship programme for a second year in 2017/18. This initiative, is aimed at female tertiary students who were undertaking science, technology, engineering, and mathematics related degrees. The scholarship is a one off grant of $10,000.

The GCSB had nearly 80 applications from students at universities throughout New Zealand and awarded four scholarships.

This scholarship also benefitted the GCSB's recruitment profile with many of the scholarship candidates also applying to enter the GCSB's graduate recruitment programme.

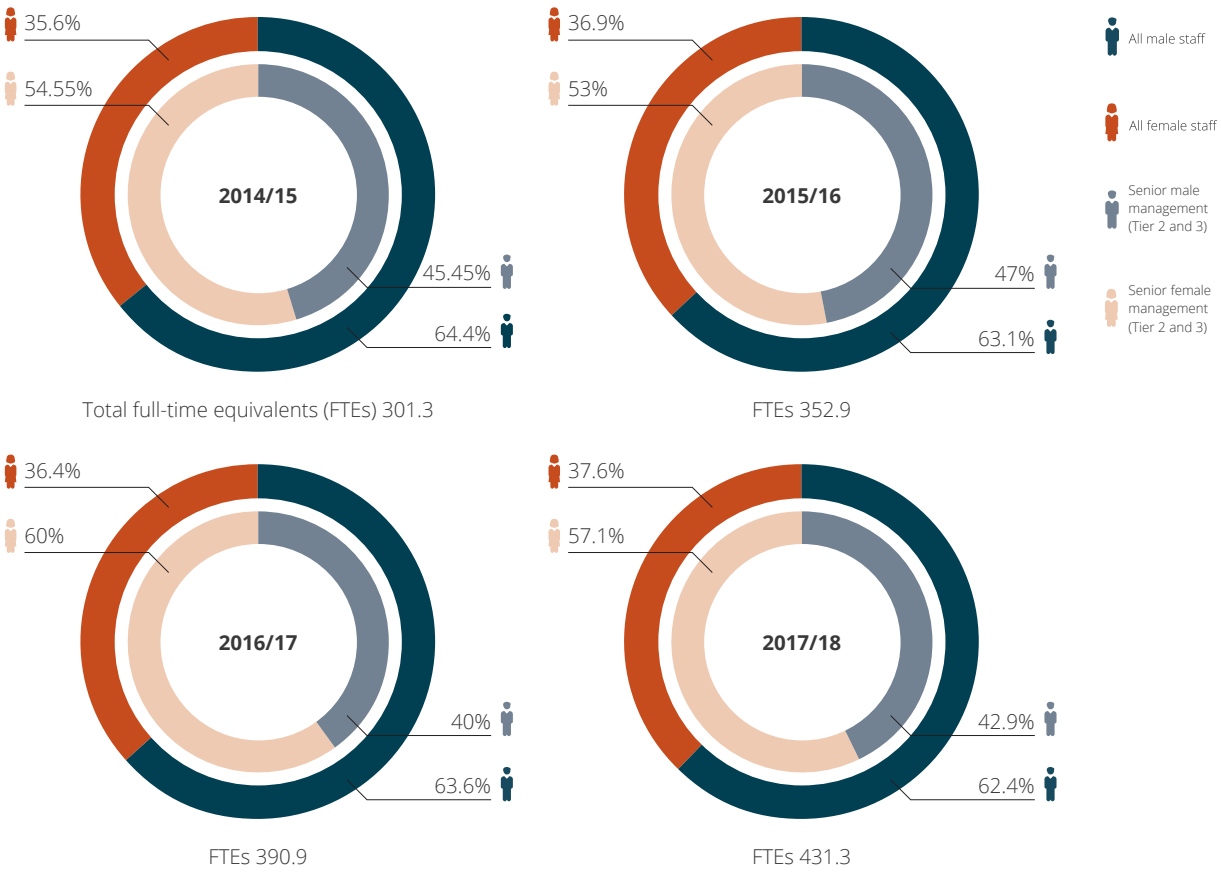
Ethnic Diversity

The GCSB is committed to improving the ethnic representation of its workforce, and has achieved modest improvement in some areas. However, it will take time for new recruitment strategies to be reflected in workforce statistics.

Gender Diversity

Women make up more than half of the GCSB's senior management group. The GCSB has also continued to gradually improve the representation of women across the whole of the organisation.

GCSB Gender Representation (2014 to 2018)



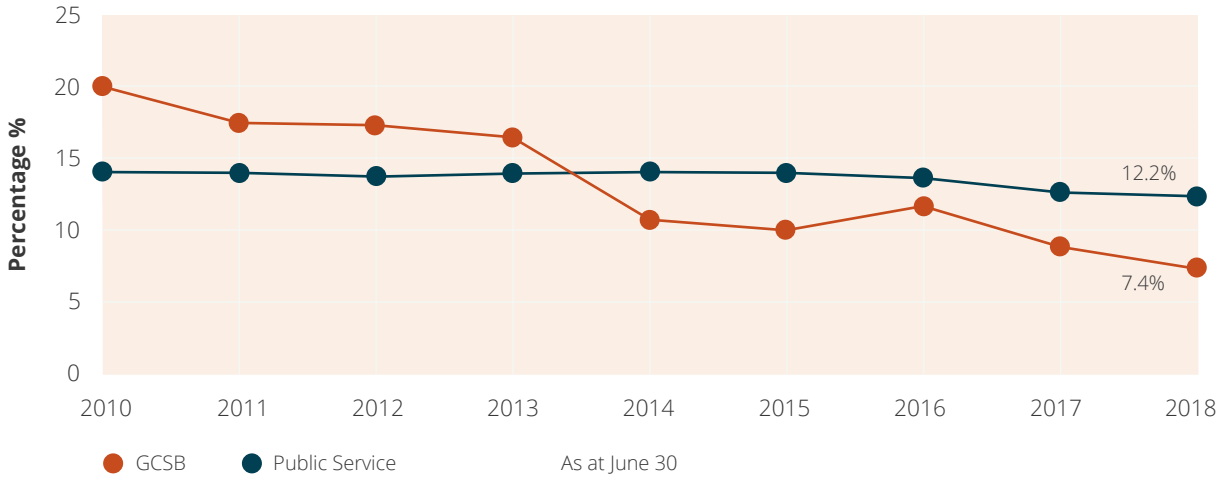
Gender Pay Gap

The GCSB continues to make progress towards achieving its goal of reducing its gender pay gap to 5 per cent by 2021. Overall the gender pay gap continues to trend down, and has reduced to almost a third since 2010.

In early 2017/18, the GCSB undertook a gender pay gap review as part of developing our Diversity and Inclusion Strategy. This analysis undertaken by band has found that males and females doing the same jobs and performing comparatively are being paid equally.

Over the last few years, the annual gender pay gap figure has varied quite a bit. This is due to the relatively small size of the GCSB, where relatively few staff changes can impact the organisation's measures. Despite this, the GCSB's gender pay gap has continued to trend down.

Despite the positive trend and the findings of the internal review, this remains a priority area for GCSB.



Our Organisation

06

History of GCSB

The Government Communications Security Bureau (GCSB) strives to protect and enhance New Zealand's security and well-being.

The GCSB is the New Zealand Government's specialist agency for applying technology to produce intelligence that informs decision makers and enhances New Zealand's national security. The GCSB also provides information security services and advice that protects New Zealand's most important information and information infrastructures.

The GCSB was formed in 1977 but its existence was kept secret until publicly acknowledged in 1984. In 2003, the Government Communications Security Bureau Act took effect, consolidating the legal framework under which the GCSB operated as the national authority for signals intelligence and information systems security. Through this legislation, the GCSB also became a public service department.

The Intelligence and Security Act (ISA) came into force in 2017, enabling better collaboration between the GCSB and the New Zealand Security Intelligence Service (NZSIS) by bringing the agencies under a single warranting regime and providing clarity about the role of each agency.

Under this legislation, our principal objectives are to contribute to the protection of New Zealand's national security, the international relations and economic well-being of New Zealand.

Investing in Our Future

Over the past four years, a number of initiatives have been underway to strengthen and build the New Zealand Intelligence Community's (NZIC) capabilities.

These initiatives were sparked by:

- the Performance Improvement Framework (PIF) in 2014;
- the Independent Review of Intelligence and Security in 2015;
- the Strategy, Capability and Resourcing Review (SCRR) and subsequent Budget 2016 decisions; and
- the implementation of the Intelligence and Security Act 2017 (ISA).

Change has been necessary to ensure we are fit-for-purpose and significant resources have been devoted to adapting our systems, policies, processes and organisational structures.

In 2016/17, activity around the Budget 2016 investment was focussed on preparing the NZIC agencies for future growth while maintain a high-standard of service the New Zealand government. In 2017/18, the focus shifted to lifting the NZIC agencies capability to deliver on the Government's expectations.

The NZIC has completed the second year of a four-year growth path and are now focussed on lifting the operational outcomes and impacts delivered by the agencies.

Organisational Change

As part of the NZIC's ongoing development, the GCSB has adapted elements of its organisational structure to reflect new operating realities, such as a closer working relationship between the GCSB and the NZSIS.

The Technology Directorate

As a result of a NZIC Information Communication Technology review in 2017, the GCSB and the NZSIS began work to establish a shared Technology Directorate. This work was driven by the need to share resources and reduce duplication between the GCSB and the NZSIS and to ensure we are prepared for sector-wide implementation of the New Zealand Top Secret Network programme.

The Joint Directors'-General Office

The Joint Directors'-General Office (JDGO) has now been in place for one year. The core role of the JDGO is to support the Directors-General to perform their roles as agency heads and public sector Chief Executives and to support the provision of advice from the NZIC to the Minister Responsible for the GCSB and NZSIS.

Over the course of this year the JDGO has been focussed on improving alignment between the GCSB and the NZSIS and supporting the NZIC to be more influential across the public sector. The JDGO has played a critical role in representing the views of the NZIC during the development of policy.

Intelligence Community Shared Services

The GCSB hosts the Intelligence Community Shared Services; a shared directorate that provides people and capability and finance services to the GCSB and NZSIS. These functions are key enablers to the mission of both agencies.

Risk and Assurance Committee

The GCSB also has a Risk and Assurance Committee. This committee is an independent body reporting to the Director-General of the GCSB. 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; and
- Internal and external audit system.

Locations

Aside from a head office in Wellington, the GCSB also has an office in Auckland and maintains two communications collection and interception stations. These are a high frequency radio interception and direction-finding station near Palmerston North, and a satellite communications interception station near Blenheim.

The GCSB has liaison offices in Australia; the United Kingdom, and the United States of America (this mission is also accredited to Canada).

Governance and Oversight

07

The Intelligence and Security Act 2017

The GCSB and the New Zealand Security Intelligence Service (NZSIS) have worked to successfully implement the ISA which came into force during the reporting period.

The new legislation provides clarity about the roles and responsibilities of each agency and supports greater collaboration between the GCSB and NZSIS. The ISA is supported by 11 Ministerial Policy Statements (MPS) which set out the Minister's expectations and guidance for the agencies on how certain lawful activities should be conducted.

Establishing the systems, policies and processes that support staff to undertake their roles and be compliant with the new legislation and MPS has been a major undertaking. The NZSIS and the GCSB ran a joint programme to transition to the new legislation.

The intelligence and security agencies have regularly engaged with the Inspector-General of Intelligence and Security (IGIS) on issues arising from interpreting the Intelligence and Security Act 2017 and carefully considered her recommendations and observations in developing new policies and processes under the new legislation.

As with any new legislation, there isn't existing case law which means extra care is required when establishing a working understanding of the law. When there is a lack of clarity about the correct interpretation of the law, as with any Government department, the intelligence and security agencies turn to Crown Law for a definitive view.

Since September 2017, both agencies have updated operational policies and procedures to reflect ISA requirements. The GCSB and the NZSIS have also worked to improve co-operation and consistency where possible by establishing a number of joint policies. This includes a new human rights risk management joint policy statement.

The Intelligence and Security Committee

By necessity most of the GCSB 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 New Zealand's democratic principles.

The Intelligence and Security Committee (ISC) has parliamentary oversight over the intelligence agencies. It looks at the value of the intelligence and security agencies and examines the policy, administration and expenditure of each organisation. The current ISC is comprised of the Prime Minister, three Members of Parliament nominated by the Prime Minister, the Leader of the Opposition, and two Members of Parliament nominated by the Leader of the Opposition.

Office of the Inspector-General

The Inspector-General of Intelligence and Security (IGIS) and her office is a key New Zealand Intelligence Community oversight body. The IGIS provides assurance for the public to have confidence the GCSB complies with the law. The IGIS also acts as a mechanism to investigate public complaints against the activities of the GCSB. The 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 past four years the IGIS has found the GCSB to have sound compliance systems and processes in place.

The GCSB Intelligence Activity in Relation to the South Pacific, 2009-15

During 2017/18, the IGIS undertook an inquiry into complaints about the GCSB's intelligence gathering activities in relation to the South Pacific. This report noted that the GCSB had, and operated within statutory authorisations for it to lawfully collect signals intelligence in relation to New Zealand's interests in the South Pacific.

The GCSB cooperated fully with this inquiry. The IGIS noted that she was particularly appreciative of the professional and constructive approach adopted by the GCSB to support her inquiry. These comments are demonstrative of the effort that the GCSB is making to increase transparency and to build trust with the New Zealand public.

Official Information and Privacy Act Requests

Like other public service agencies, the 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.

For the period from 1 July 2017 to 30 June 2018, the GCSB:

- Completed 70 OIA requests, with eight requests not completed within the legislated timeframe.
- Completed 17 Privacy Act requests, with seven requests not completed within the legislated timeframe.

The GCSB aspires to complete all of these information requests within the legislated timeframe. However during the early part of 2017/18, resource constraints prevented the GCSB from achieving our desired result in this area. To address this the GCSB has directed more support to processing these requests and has greatly improved our compliance with legislated timeframes.

The Office of the Ombudsman and the Office of the Privacy Commissioner also provide important oversight of the GCSB's activities.

For the period of 1 July 2017 to 30 June 2018, 5 OIA complaints were completed by the Office of the Ombudsman during the period. All of the closed complaints led to a finding in favour of the GCSB. In all cases, the GCSB worked proactively with the Office of the Ombudsman to quickly resolve the complaints and to explain the reasons behind its decisions.

No complaints were raised with the Office of the Privacy Commissioner during the period.

Financial Statements

08

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 2018

The Auditor-General is the auditor of the Government Communications Security Bureau (the GCSB). 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 GCSB for the year ended 30 June 2018, which is made up of the statement of expenses and capital expenditure on page 51.

Opinion

In our opinion the statement of expenses and capital expenditure of the GCSB on page 51 is presented fairly, in all material respects, in accordance with the requirements of section 45A of the Public Finance Act 1989 and section 221(4)(a) of the Intelligence and Security Act 2017.

Our audit was completed on 28 September 2018. 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 GCSB for preparing the financial statements, which are made up of the statement of expenses and capital expenditure of the GCSB, 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 GCSB for assessing the GCSB's ability to continue as a going concern. The Director-General of Security 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 GCSB, 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, 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 Estimates of Appropriations 2017/18 for Vote Communications Security and Intelligence, and the 2017/18 forecast financial figures included in the GCSB's 2016/17 financial statements.

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 GCSB'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 GCSB'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 GCSB 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 to 46 and page 50, 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 GCSB in accordance with the independence requirements of the Auditor General'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 GCSB.

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 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 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; 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 2018 and its operations for the year ended on that date.

Andrew Hampton
Director-General of the GCSB

28 September 2018

Statement of Expense and Capital Expenditure Against Appropriation

For the year ended 30 June 2018

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

	$000
Total appropriation	$158,029
Actual expenditure	$103,446

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.

GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

New Zealand Government