



# 2019

## Annual Report

**Government Communications Security Bureau**  
**Te Tira Tiaki**

## Preface

This is the annual report of the Government Communications Security Bureau (GCSB) for the year ended 30 June 2019, presented for consideration and scrutiny by the Intelligence and Security Committee.

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

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



GOVERNMENT  
COMMUNICATIONS  
SECURITY BUREAU  
TE TIRA TIAKI

# Contents

<b>Overview of the Year</b>	<b>4</b>
Director-General's Overview	5
Notable Achievements	7
<b>GCSB Strategic Context</b>	<b>10</b>
The New Zealand Intelligence Community	11
The Role of the GCSB	13
Investing in our Future	13
Strategic Operating Environment	14
Warrants and Authorisations	16
<b>Impenetrable Infrastructure</b>	<b>18</b>
Cyber Security	19
Information Assurance	22
Secure Technology	24
<b>Indispensable Intelligence</b>	<b>26</b>
Intelligence Collection	27
Regional Security	28
Working with government agencies	29
Continuous Improvement	29
International Partnerships	30
<b>Our People</b>	<b>32</b>
Our Values	33
Leadership	34
Retain, Develop and Recruit the Best People	35
Diversity in the Workforce	38
Locations	41
<b>Oversight and Legal Compliance</b>	<b>42</b>
The Intelligence and Security Act 2017	43
Office of the Inspector General Intelligence and Security	43
The Intelligence and Security Committee	44
The Justice Select Committee Inquiry	44
Official Information and Privacy Act Requests	45
<b>Financial Statements</b>	<b>46</b>
Independent Auditor's Report	47
Statement of Responsibility	50
Statement of expenses and capital expenditure against Appropriation for the year ended 30 June 2019	51



| Overview  
of the Year

# Director-General's Overview

The horrific terrorist attacks in Christchurch on 15 March were a challenge to everything New Zealand holds dear. How New Zealanders responded showed the best of us as a country as we rallied to support and care for those affected by the attacks.

The Government Communications Security Bureau (GCSB) deployed its signals intelligence capabilities to assist the New Zealand Police and the New Zealand Security Intelligence Service. We stood up a 24/7 team immediately after the attacks and provided intelligence in support of our colleagues as they worked on the investigation and wider response.

While the Christchurch attacks have been a major focus for the intelligence community, 2018/19 has been a very busy year for GCSB's other functions, including its cyber security and regulatory roles.

In 2018/19 we detected 339 cyber security incidents involving organisations of national significance, 131 of which had links to state-sponsored actors.

The GCSB again added New Zealand's voice to international condemnation of malicious cyber activity. We joined likeminded partners in attributing two malicious cyber threat campaigns to particular actors from foreign countries, further demonstrating this country's commitment to upholding the rules-based international order.

We continued to provide network defence capabilities to nationally significant organisations through our CORTEX services. The Government approved the expansion of our Malware-Free Networks initiative to a much larger number of nationally significant organisations, further enhancing protection to critical national infrastructure against malicious cyber activity.

In 2018/19 the GCSB responded to several significant incidents that were not the result of a cyber intrusion as such, but of inadequate information management. These incidents have highlighted the need for basic information management practices and good data hygiene.

GCSB received its first 5G telecommunications network change notification for assessment in 2018/19.

The telecommunications sector is a core piece of New Zealand's infrastructure. It is critical to the daily lives and wellbeing of New Zealanders and is a key part of the country's economic stability and national security.



The GCSB has an important role in supporting the sector to have robust and resilient infrastructure and strong information security.

The GCSB has an important role in supporting the sector to have robust and resilient infrastructure and strong information security. As 5G starts to drive significant technological change, the GCSB's part in ensuring the telecommunications industry manages and mitigates security risks will become increasingly critical.

Independent oversight of the GCSB is essential to New Zealanders having confidence in our activities. GCSB's oversight obligations continued to be an important area of focus during 2018/19. We have prioritised resources to respond to a number of inquiries, for the Inspector-General of Security and Intelligence (IGIS), the Royal Commission into the Christchurch Terrorist Attacks and the Inquiry into Operation Burnham.

The IGIS report into the GCSB's involvement in the CIA's detention and interrogation programme 2001–2009 determined the GCSB was not complicit in any unlawful conduct. The IGIS acknowledged the performance and judgement of the deployed GCSB staff, finding they performed their roles to the standard required. The report identified areas for improvement in the support, training and supervision of deployed staff, and while much has changed since that time, these recommendations will be taken on board and changes made where appropriate.

I am very pleased with our efforts to reduce the GCSB's gender pay gap. This year it reduced to 5.4 percent, meaning we effectively met our five percent maximum target three years ahead of schedule.

We were delighted to receive 143 applications for our 'Women in STEM' scholarship to tertiary students studying science, technology, engineering and mathematics. The calibre of the applicants was extraordinary and we offered three scholarships of \$10,000 each. This is a practical way of encouraging more women into our workforce.

Our staff have shown outstanding commitment and dedication over this very productive and demanding year. Thanks to them, the GCSB was able to achieve a great deal in 2018/19 and I am privileged to reflect their efforts in this report.



**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

### Malicious Cyber Activity

During 2018/19 the GCSB recorded 339 cyber security incidents involving organisations of national significance. These incidents were identified through a combination of self-reporting, detection by our own cyber security capabilities and information shared by international partners.

Of the recorded incidents 131, or 38 per cent, had links to state-sponsored actors. While this is the same proportion as the previous year a greater number were characterised as 'post compromise' compared to the previous year. This suggests that New Zealand networks are facing increasing risk of successful compromise by state-sponsored actors.

In 2018/19 the detection and disruption of malicious cyber activity, by CORTEX capabilities, has prevented \$27.7 million dollars worth of harm to New Zealand's nationally significant organisations. This means that over the last three years, CORTEX capabilities have reduced harm from hostile cyber activity by around \$94.7 million.

### Attributions

GCSB continues to work closely with partner agencies across Government and internationally to call out malicious cyber activity that is counter to internationally accepted norms of behaviour in cyber space.

In 2018/19 this has resulted in the Director-General of GCSB, on behalf of the New Zealand Government, twice attributing campaigns of malicious cyber threats to nation states.

In December the Director-General attributed links between the Chinese Ministry of State Security and a global campaign of cyber-enabled commercial intellectual property theft. The long running campaign targeted the intellectual property and commercial data of a number of global managed service providers, some operating in New Zealand.

In October, the GCSB publicly reported that it had established clear links between the Russian government and a campaign of malicious cyber activity targeting overseas political institutions, businesses, media and sporting organisations.

Our assessment found it was highly likely the Russian military General Staff Main Intelligence Directorate (GRU) was behind the campaigns and that a number of cyber proxy groups associated with these incidents are actors of the Russian state.

### Expansion of Malware-Free Networks

Malware-Free Networks provides a cyber threat intelligence feed enabling potentially malicious activity to be detected and disrupted. Malware-Free Networks was piloted as part of the initial CORTEX delivery.

The Malware-Free Networks pilot involved GCSB sharing cyber threat information and technology with an Internet Service Provider (ISP) to help them mitigate malware. The information shared with ISPs focuses on foreign-sourced malware that is particularly advanced in terms of technical sophistication and/or persistence.

Work on the expansion of Malware-Free Networks continued throughout 2018/19, with significant customer engagement to ensure that Malware-Free Networks meets their needs and can be effectively integrated into their network security systems. It is expected that the GCSB will be able to offer the Malware-Free Networks capability by 30 June 2020.

### Cyber Security Customer Engagement

Through its outreach and engagement team the National Cyber Security Centre helps organisations increase their cyber security resilience by promoting cyber security dialogue at executive level, facilitating security information exchanges, and advising organisations about new cyber threats and vulnerabilities. This team had more than 800 customer engagements in the 2018/19 year.

### Cyber Security Resilience Survey

We surveyed 250 nationally significant organisations to establish their cyber security resilience and the potential impacts if they were compromised. We developed a range of reporting setting out actions organisations can take to help increase their resilience including areas such as governance, investment, their readiness to respond to incidents, and their management of security in their supply chain and with third party vendors.

### **Telecommunications (Interception Capability and Security) Act 2013 (TICSA)**

The GCSB performs a role in regulating network security under TICSA. During the reporting period the GCSB received 158 notifications from telecommunications network operators about proposed changes to networks that could undermine their security.

In late 2018 the GCSB received the first notification for fifth generation mobile networks (5G) assessment under TICSA. The advent of 5G mobile technology will drive broad technological change across the telecommunication sector. This is essential, generational change for New Zealand's telecommunications.

The regulatory process relating to this notification is ongoing as the network operator assesses options to mitigate the risks identified in the notification.

### **Outer Space and High-Altitude Activities Act (OSHAA) 2017**

OSHAA came into effect in 2017 and provides a regulatory framework for 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 29 assessments on space-related activities.

### **Improving New Zealand's Secure Technology**

GCSB is responsible for the delivery of secure information technology infrastructure to the New Zealand Intelligence Community, and the wider sector. This includes GCSB being New Zealand's national authority for communications security.

In 2018/19 the GCSB Cryptographic Products Management Infrastructure (CPMI) project and the New Zealand Top Secret Network (NZTSN) project have made significant progress towards the long term resilience of New Zealand's classified Government information.

### **Government Chief Information Security Officer**

As awareness of the rapidly growing nature of cyber threats and risk grows across the public sector, the demand for protective security services is increasing. Government agencies need to 'go digital', but also do it in a secure manner. In response, to this the Director-General of the GCSB was formally designated as the Government Chief Information Security Officer (GCISO) in 2018/19.

This role provides support to New Zealand government agencies to better deal with information security issues in the face of the ongoing evolution of threats, and technology changes.

### **Security of New Zealand's Elections**

The Director-General appeared before the Justice Select Committee, alongside the Director-General of the NZSIS, to discuss how well New Zealand is positioned to protect our electoral system from foreign interference.

## **Indispensable Intelligence**

### **Response to the Christchurch attacks**

In the aftermath of the March 15 terrorist attacks the GCSB received tasking from the NZSIS and New Zealand Police. The GCSB used its capabilities to make a unique and material contribution to the investigation into the attacks, extreme right wing activity in New Zealand and the risk of any copycat or retaliatory attacks. Following the initial period, with GCSB staff working 24/7 in support of the operation, significant support for the Royal Commission of Inquiry has also been a focus.

### **Provision of intelligence**

Throughout 2018/19 the GCSB continued to supply intelligence to 17 government agencies, various Ministers and decision makers, in accordance with the priorities set by the Government. This intelligence was obtained through the GCSB's own capabilities, and from international partner agencies. The provision of this intelligence is one way that the GCSB contributes to the safety and security of New Zealand and our interests.



### **Working with government agencies**

In 2018/19 the GCSB continued to work closely with a variety of government agencies, including Police, New Zealand Customs and Immigration New Zealand. This work contributes to the protection of New Zealand's national security and wellbeing.

### **Support to Military Operations**

The GCSB continued to provide support to the New Zealand Defence Force (NZDF) for the purposes of its operations. The GCSB contributes to NZDF efforts to detect and counter threats to New Zealand military personnel deployed overseas.

### **Findings from the Senate Inquiry**

Throughout 2018/19 the GCSB continued to contribute to the Inspector General of Intelligence and Security inquiry into possible New Zealand intelligence and security agencies' engagement with the CIA detention and interrogation programme 2001 – 2009. The final report found that the GCSB had no direct involvement in the CIA's detention and interrogation programme and was not complicit in any unlawful conduct.

## **Organisational Health**

### **Budget 2019**

In Budget 2019 the GCSB and NZSIS received an additional \$50 million dollars over four years. Of that, \$39 million was allocated to the GCSB. The funding boost reflects in part that the GCSB houses a number of functions that are shared by both the GCSB and the NZSIS. The funding received from Budget 2019 will go towards ensuring we can continue to respond to the changing threat environment and support Government priorities.

### **Improving gender and diversity representation**

For the GCSB to deliver on its mission it is important that our staff reflect the diversity of New Zealand. We recognise that diversity is central to innovation. It brings forth new and better ways of doing things and improves the efficiency and quality of our services. Having people from a range of backgrounds, who bring different skills and perspectives, helps us to be more effective in achieving our mission.

It is important for trust and confidence in the GCSB that we continue to improve gender and diversity representation, to reflect the community we serve. In 2018/19 the GCSB undertook a 'Women in STEM (science, technology, engineering and mathematics) scholarship programme. We received 143 applications, which was a significant increase from 79 applications in 2017. The calibre of applications was extraordinary, resulting in three scholarships being awarded. Our three winners respectively identify as New Zealanders of Māori, Pasifika or Asian ethnicity.

### **The Gender Pay Gap**

Closing the gender pay gap has been a focus for the GCSB, with a target of reducing the gap to a maximum of five percent by 2021. In 2018/19 the GCSB gender pay gap was 5.4 per cent, nearly achieving our goal in three years, rather than five.

### **Launch of new staff networks**

While the recruitment of a diverse workforce is an area of focus for the GCSB, it is also important that we support our staff to be able to come to work as their authentic selves. As a part of this work the GCSB has established staff networks such as the Women of the New Zealand Intelligence Community (WNZIC) network. In 2018/19 the Ethnicity Network, to celebrate ethnic diversity in the NZIC, and Standing Out, to support our LGBTQI+ community, were launched in 2018/19.



GCSB

Strategic Context

# The New Zealand Intelligence Community

The New Zealand Intelligence Community (NZIC) is dedicated to working together to contribute to the national security and well-being of New Zealand and New Zealanders.

The work of the NZIC is a key contributor to the national security of New Zealand, and by extension, to the current and future wellbeing of New Zealand and New Zealanders. The NZIC has a crucial role to play in understanding the threats New Zealand faces and how to guard against those threats.

The core New Zealand Intelligence Community (NZIC) agencies are:

## **Government Communications Security Bureau**

GCSB ensures the integrity and confidentiality of government information, collects intelligence bearing on New Zealand's interests, and assists other New Zealand government agencies to discharge their legislative mandate.

## **New Zealand Security Intelligence Service**

NZSIS investigates threats to New Zealand's national security, and provides a range of protective security advice and services to the New Zealand Government.

## **Department of the Prime Minister and Cabinet: National Security Group**

The National Security Group produces intelligence assessments on events and developments that have a bearing on New Zealand's interests, to help inform government decision making. The National Security Group is also responsible for promoting excellence in intelligence analysis across the New Zealand government.

The NZIC contributes to building a safer and more prosperous New Zealand. NZIC agencies work to ensure that New Zealand is protected from harm, that New Zealand policy makers have intelligence to support good decision making, and that advances New Zealand's international reputation and interests.



New Zealand  
Security Intelligence  
Service  
Te Pā Whakamarumarū



GOVERNMENT  
COMMUNICATIONS  
SECURITY BUREAU  
TE TIRA TIAKI



DEPARTMENT OF THE  
PRIME MINISTER AND CABINET  
TE TAIRĀ O TE PIRIHĀ HE TE KŌWHIRI MATUA

## National Security and Intelligence Priorities

The National Security and Intelligence Priorities (NSIPs) direct the GCSB's intelligence collection and analysis. The NSIPs outline key areas of national security interest to the New Zealand government. The priorities assist agencies that have a national security role to make informed, joined-up decisions, and define key areas of focus.

New Zealand takes an 'all hazards, all risks' approach to national security. This means the priorities cover a large range of potential risks to New Zealand's security and wellbeing.

The NSIPs are coordinated by the Department of Prime Minister and Cabinet (DPMC) and a range of agencies, including the GCSB, work toward achieving them. The priorities include risks to our environment, health, biosecurity, economy, trade, international relations, computer networks, regional stability, borders, the use of space and space based technologies, and to New Zealand's people and institutions from terrorism, crime, foreign interference, conventional weapons and weapons of mass destruction.

Customs Service, the Ministry of Business, Innovation and Employment, and the Ministry of Foreign Affairs and Trade.

The current priorities were approved in December 2018 and are listed below in alphabetical order:

- **Biosecurity and human health** – Threats to New Zealand's biosecurity and human health arising from human activity.
- **Environment, climate change and natural resources** – International environment, climate change and natural resources challenges that may impact New Zealand's interests and national security.
- **Foreign influence, interference and espionage** – Acts of interference, influence and espionage in and against New Zealand that would erode New Zealand's sovereignty, national security or economic advantage.
- **Global economy, trade and investment** – Developments in international trade governance, and New Zealand's bilateral, plurilateral and multilateral trading relationships.
- **Implications of emerging technology** – The implications of emerging technology and innovation trends for New Zealand's national security, international relations and economic wellbeing.
- **International governance, geopolitics and global security** – Developments in international governance, geopolitics and global security that may impact New Zealand's interests.
- **Malicious cyber activity** – Cyber threats to New Zealand from state-sponsored and other malicious actors.
- **Middle East regional security** – The implication of events in the Middle East region on New Zealand's national security, international relations and economic wellbeing.
- **New Zealand's strategic interests in the Asia region** – The implications of events in the Asia region on New Zealand's national security, international relations and economic wellbeing.
- **Pacific regional stability** – Protecting and promoting stability, security and resilience in the Pacific region.
- **Proliferation of weapons of mass destruction and conventional weapons** – Non-proliferation and counter-proliferation of weapons of mass destruction and conventional weapons.
- **Space security** – The implications of the exploitation of space and space-based technology on New Zealand's national security, international relations and economic wellbeing.
- **Territorial security and sovereignty** – Threats to New Zealand's territorial security and sovereign rights arising from illegal, unregulated, negligent, harmful (or potentially harmful) human activity.
- **Terrorism** – Threats to New Zealand, New Zealanders and New Zealand's interests from terrorism (ideology, politically or religiously motivated violence) at home and abroad.
- **Threats to New Zealanders overseas** – Threat to the safety and success of New Zealand people, platforms and missions (military, police, diplomatic and civilian) overseas.
- **Transnational organised crime** – Threats to New Zealanders and New Zealand's interests from transnational organised crime, including trafficking, irregular migration, financial crime, fraud and corruption.

# The Role of the GCSB

The GCSB is New Zealand's lead organisation for signals intelligence (SIGINT). We use our intelligence collection capabilities, supplemented by intelligence received from partners, to support government agencies in their operations, decision making and to discharge their legislatively mandated functions.

The GCSB is a crucial part of how New Zealand makes sense of the world and manages national security threats and in doing so contributes to the wellbeing of the nation and its citizens. The GCSB Strategy 2018 – 2022 focuses on two primary outcomes; Impenetrable Infrastructure and Indispensable Intelligence.

These areas of focus contribute to New Zealand's national security by:

- Providing information assurance and cyber security services, advice and assistance.
- Producing and disseminating signals intelligence in accordance with the Government's Priorities.
- Performing regulatory roles under the TICSAs and OSHAA.
- Co-operating with, and assisting NZSIS, Police and the New Zealand Defence Force in the performance of their functions.

## Investing in our Future

### Strategic Capability and Resourcing Review

The NZIC is three years in to a four year investment programme that has lifted capacity and capability across all core functions.

Investment received in Budget 2016 built a foundation for the NZIC to prioritise operational effort to keep New Zealanders safe, to protect and grow the economy, and provide intelligence and assessment about issues that matter most to New Zealand.

A 2018 follow up Performance Improvement Framework review of the NZIC agencies confirmed positive progress from the 2016 investment. The NZIC is now delivering fundamentally better advice, services and products that connect directly to the Government's National Security and Intelligence Priorities.

### Budget 2019

In Budget 2019, the GCSB and NZSIS received an additional \$50 million, over four years. Of that funding, the GCSB received \$39 million. The investment in GCSB includes funding for a number of shared functions that are housed in the GCSB, but benefit the wider intelligence and security community.

The funding received from Budget 2019 will go towards ensuring the GCSB can continue to respond to the changing environment and support Government priorities.

# Strategic Operating Environment

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

## Cyber Security

Cyber threats to New Zealand's nationally significant organisations continued to evolve in scope and scale throughout 2018/19. The GCSB's National Cyber Security Centre recorded 339 incidents in the 2018/19 reporting period (compared to 347 in the previous year). Hostile actors are actively targeting New Zealand and the work of the GCSB to detect and disrupt those actors has become more important than ever.

State-sponsored cyber-attacks are occurring in an increasingly complex security environment. The rise of great power competition and challenges to the rules-based order is resulting in more governments openly developing offensive cyber capabilities.

In the financial year 2018/19, 131 (38%) of the NCSC's cyber incidents had links to state-sponsored actors – the same proportion as the previous year. However, a greater number of state-sponsored linked incidents were characterised as "post compromise" compared to the previous year. This suggests New Zealand networks are facing an increasing risk of successful compromise by state-sponsored actors. State-sponsored cyber activity is generally more sophisticated than criminal or non-state activity, a reflection of the greater resources and motivations of the state.

State-sponsored linked activity impacts a variety of types of New Zealand organisations in multiple industries. Organisations in the public and private sectors hold a wealth of information that is attractive to others, from intellectual property for new technology innovations through to customer data, business and pricing strategies or government positions on sensitive topics.

As more New Zealanders rely on the internet to work and live, the amount of cyber-enabled crime also increases. Malicious actors, both individuals and state-sponsored, are also becoming more sophisticated as they gain access to advanced tools and techniques.

Throughout 2018/19 the GCSB contributed to the development of New Zealand's Cyber Security Strategy 2019, as part of our efforts to keep New Zealand secure online. This cross agency piece of work emphasises the need for individuals, businesses, community organisations, and the private sector to work together to minimise harm from cyber security threats.

## Changes in Technology

Technological acceleration represents a significant challenge for the GCSB and as new technologies emerge we must be able to react quickly. This includes the increasing use of the Internet of Things, along with Artificial Intelligence in our daily lives.

Digital transformation continues to evolve internationally, with ever more devices connected to the internet, and organisations increasingly reliant on technology for everyday activities.

Malicious cyber actors, including both state-sponsored and criminal actors, continue to target computer systems for an ever increasing range of reasons, utilising the continually evolving range of technologies and tools at their disposal.

This rate of technological change results in an increasingly complex cyber threat environment, both in New Zealand and internationally; where everyone; individuals, organisations and nations must be conscious about cyber security.

The international threat landscape has seen an increased use of cyber operations to advance nation states' goals, such as the disinformation or influence campaigns intended to disrupt other nations' political systems, like that seen in the 2016 US presidential election.

Large-scale public breaches of personal information have promoted the issue of data privacy amongst the public consciousness, and developing technologies continue to increase the attack surface available to cyber actors.

## Counter-Terrorism

The threat of harm from all types of violent extremism continues to be a security issue both internationally and for New Zealand. The GCSB's role in domestic counter-terrorism is to provide technical expertise and access to intelligence to support other agencies.

The unprecedented events of 15 March 2019 proved that New Zealand is not immune to the threat of extreme right-wing terrorist threats. The spread of extremist content and ideologies online remains a threat to New Zealand's safety and security.

In response to the terrorist attacks the GCSB received tasking from the NZSIS and New Zealand Police to support the investigation into the alleged perpetrator, right wing extremism in New Zealand and the risk of any copy cat or retaliatory attacks.

While 2018/19 saw the end of Islamic State of Iraq and the Levant territorial 'caliphate', the group remains active as an extremist organisation capable of inspiring terrorist attacks in the West. The group remains active internationally, seeking to spread radicalising propaganda online. Other groups, such as al-Qai'da also remain an active security threat.

## Foreign Interference

All states engage in foreign influence activity in seeking to shape perceptions and decision making in another country. This activity becomes foreign interference when it is purposely misleading, deceptive, covert or clandestine.

Foreign interference is a growing threat globally and domestically, with wide-ranging impacts on New Zealand's economic wellbeing and democratic norms and values. The scale and aggressive nature of this activity is on the rise around the world.

## Security in the Pacific

The security of the South Pacific has been an enduring area of focus for New Zealand. As competition between states increases, so do the efforts of those states to project influence and power into the Pacific region. These actions have the potential to impact New Zealand's national and regional security.

2018/19 has seen an increase in transnational organised crime in the Pacific region, with foreign criminal networks targeting the Pacific and seeking to increase their activities. Transnational crime has the ability to rapidly spread and affect other countries including New Zealand.

# Warrants and Authorisations


## Intelligence and Security Act 2017

Under the Intelligence and Security Act 2017 (ISA), GCSB's main warranted operational activity is covered by two types of intelligence warrants. A Type 1 warrant is issued for the purpose of collecting information about or to do any other thing directly in relation to New Zealanders. A Type 2 warrant is for activities done for other purposes. In each case, warrants may only be issued if the activities authorised by the warrant:

- will enable GCSB to contribute to the protection of national security, the international relations and well-being, or the economic well-being of New Zealand;
- are necessary for GCSB to perform its functions of intelligence collection and analysis or providing protective security services, advice, and assistance (including information assurance and cybersecurity activities);
- are proportionate to the purpose for which the activities are carried out; and
- meet the other statutory tests.

# 33

intelligence warrants were approved in 2018/19, of which:

18  were Type 1 intelligence warrants.

15  were Type 2 intelligence warrants.

A total of 33 intelligence warrants were applied for and approved in 2018/19, of which 18 were Type 1 intelligence warrants and 15 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. Joint intelligence warrants authorise the Directors-General of GCSB and NZSIS to carry out the activities authorised by the warrant, and to exercise all of the powers of either agency to give effect to the warrant. While no occasion arose where GCSB and NZSIS considered it necessary to seek such authority, GCSB and NZSIS closely co-operate on operational matters.

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

One very urgent authorisation was made by the Director-General under section 78. An application for an intelligence warrant was made within 24 hours of that authorisation, and that warrant was subsequently issued.

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 12 business records directions were issued by GCSB to agencies under section 150.

GCSB did not provide any advice and assistance to the New Zealand Defence Force or the New Zealand Police under section 13(1)(b). However, GCSB co-operated with both agencies on a wide range of matters as part of performing GCSB's intelligence collection and analysis and protective security services, advice, and assistance (including information assurance and cybersecurity activities) functions.







| Impenetrable  
Infrastructure

# Cyber Security

The GCSB protects New Zealand's nationally significant information infrastructure from malicious cyber threats.

Improving cyber security is a fundamental enabler for New Zealand to thrive in the digital age. As New Zealand becomes more connected to the world, we face a greater number of technological vulnerabilities. Technology is now exploited in a range of new spheres, including democratic processes (for example, the recent compromise of Australian Federal Parliament and the 2016 compromise of US Democratic National Committee systems) and large scale exhortative action such as the disruption caused by the WannaCry ransomware campaign to the United Kingdom National Health Service in 2017.

Without adequate cyber security, New Zealand will be unable to protect its intellectual property, maintain its reputation as a stable and secure place to do business, and ensure governmental and democratic processes remain free from interference.

New Zealand's systems and infrastructure have been the target of cyber threat actors as a means of advancing their own economic interests. International incidents, which do not directly target New Zealand, have also resulted in collateral consequences here.

During the reporting period the GCSB recorded 339 cyber security incidents. These incidents were identified through a combination, self-reporting, detection by our own cyber security capabilities and information shared by our international partners. Each of these incidents represents an effort by a threat actor to breach the cyber security of a government agency, or other nationally significant organisation.

Of the 339 recorded incidents, 131 (38%) had links to state-sponsored actors – the same proportion as the previous year. However, a greater number of state-sponsored linked incidents were characterised as “post compromise” compared to the previous year. This suggests New Zealand networks are facing an increasing risk of successful compromise by state-sponsored actors. State-sponsored cyber activity is generally more sophisticated than criminal or non-state activity, a reflection of the greater resources and motivations of the state.

State-sponsored linked activity impacts a variety of types of New Zealand organisations in multiple industries. Organisations in the public and private sectors hold a wealth of information that is attractive to others, from intellectual property for new technology innovations through to customer data, business and pricing strategies or government positions on sensitive topics.

## National Cyber Security Centre

The GCSB's National Cyber Security Centre (NCSC) plays a vital role in protecting government agencies and New Zealand's nationally significant institutions from cyber threats that have the potential to affect New Zealand's national security and the economy. The NCSC does this by detecting and disrupting cyber threats and by providing cyber threat analysis to customers and partners.

The NCSC operates a suite of cyber defence capabilities developed as part of its award winning CORTEX initiative, and provides incident response support to help nationally significant organisations address potentially high impact cyber events.

The NCSC works with a range of customers, including government agencies, institutions of national significance, key economic generators, niche exporters and research institutions to counter cyber threats.

## Who we work with

In order to effectively protect New Zealand and New Zealanders from advanced cyber threats, the NCSC works closely with a range of domestic and international partners.

The NCSC, CERT NZ (New Zealand's Computer Emergency Response Team), and New Zealand Police work together to ensure the New Zealand Government's response to cyber events is effective and comprehensive.

New Zealand Police is responsible for responding to crimes occurring online and CERT NZ works to support businesses, organisations and individuals who are affected by cyber security incidents. The NCSC responds to cyber incidents involving organisations of national significance or where the security and/or economic prosperity of New Zealand may be impacted.

The GCSB recorded

# 339

cyber-security incidents.

# 131 (38%)

With links to State sponsored actors

## CORTEX Cyber Security Services

### CORTEX

Our CORTEX cyber defence capabilities continue to be a key tool to support nationally significant organisations, to protect their networks from malicious, advanced, persistent and sophisticated cyber security threats.

Analysis undertaken by the GCSB shows that in 2018/19 the detection and disruption of this cyber activity, by CORTEX capabilities, has prevented \$27.7 million in harm to New Zealand's nationally significant organisations. This means that, over the last three years, CORTEX capabilities have reduced harm from hostile cyber activity by around \$94.7 million.

CORTEX provides network defence capabilities, tools and expertise that are not typically available to the public. To provide this service effectively the team draws threat information from a range of sources, including our own intelligence and that provided by international partners, to detect and disrupt this malware.

Throughout 2018/19 the NCSC continued to improve and advance CORTEX capabilities to best support our customers; government departments, key economic generators, research institutes and operators of critical national infrastructure.

### Malware-Free Networks

Malware-Free Networks (MFN) is an 'active disruption' capability that was developed as part of the GCSB's CORTEX cyber security services. The MFN capability is designed to counter cyber threats to organisations of national significance.

The MFN capability was successfully piloted with an internet service provider, which saw the GCSB sharing cyber threat information and technology to help mitigate malware for a subset of consenting commercial customers. The information shared focuses on foreign-sourced malware that is particularly advanced in terms of technical sophistication.

In 2018 the Government approved the expansion of some cyber defence services to a much larger number of nationally significant organisations through MFN.

Since then the NCSC has worked with a range of customers and network operators to identify how best to deliver the service and to establish the technology platform that will enable the most effective cyber threat intelligence sharing and reporting.



Analysis undertaken by the GCSB shows that in 2018/19 the detection and disruption of this cyber activity, by CORTEX capabilities has prevented

# \$27.7 million

in harm to New Zealand's nationally significant organisations.

Customers will be able to receive the MFN threat intelligence either directly from the NCSC or via their network operator. This approach ensures customers with varying levels of capabilities will be able to receive the benefit of MFN.

In May 2019 the NCSC successfully tested the core enabling technology platforms that will enable it to share indicators of compromise directly with both organisations of national significance and network operators.

The NCSC is on track to have the MFN threat intelligence automatically integrated into the systems of network operators and a small set of customers by early 2020. This will enable threat intelligence to be shared and acted on in near real-time.

Following this integration, the NCSC will expand the scope of the service and has already begun gathering information for network operators to work with.

Once this has been achieved the NCSC will be in a strong position to offer the scaled MFN capability to a significant cross section of New Zealand's organisations of national significance by 30 June 2020.

# Information Assurance

One of the GCSB's key functions is to provide 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 infrastructures. It also protects the Government's most sensitive information.

Throughout 2018/19 the GCSB acquired functional leadership for information security as the Government Chief Information Security Officer. This is an area of ongoing development as GCSB, working closely with the Chief Government Digital Officer and the Government Protective Security Lead and other functional leads, to support 'secure digital transformation' across government agencies.

An important achievement in the reporting year has been the establishment of a new Policy and Research Unit, within the IACD. This unit leads the development and promulgation of information security policy across the public service and works closely with other digital functional leads to ensure greater strategic alignment if information security policy and guidance.

## Telecommunications (Interception Capability and Security) Act 2013

The telecommunications sector is a core part of New Zealand's infrastructure, is critical to the daily lives and wellbeing of New Zealanders, and is a key part of New Zealand's economic stability and national security. The GCSB has an important role in supporting the sector to have robust and resilient infrastructure and strong information security.

In 2013 Parliament passed the Telecommunications (Interception Capability and Security) Act, also known as TICSAs. TICSAs provides a legislative framework designed to mitigate, or remove, security risks from the design, build and operation of public telecommunications networks.

Part 3 of TICSAs was enacted to provide a mechanism for addressing telecommunications network security concerns. The GCSB uses provisions of TICSAs to assess potential network security risks on a case by case basis. The Director-General of the GCSB has a regulatory role for network security under Part 3 of TICSAs.

When considering whether a network operator's proposal may pose a network security risk, the Director-General of GCSB must consider what the likelihood is that it will lead to the compromising or degrading of the public telecommunications network.

During the reporting period the GCSB received 158 notifications from telecommunications network operators, up from 123 the previous year. As notifications under TICSAs are made on a commercial in confidence basis, GCSB does not generally comment on the process for individual notifications.

## What is 5G?

### Fifth Generation (5G) technology

The advent of Fifth generation mobile networks (5G) mobile technology will drive broad technological change across the telecommunication sector. These changes will underpin the public telecommunications networks for at least the next decade. 5G promises faster data speeds, lower latency, and the potential for ubiquitous connectivity.

5G represents a significant step-change in the development of telecommunication networks, and the security of those networks is critical for New Zealand.

The design of 5G networks will be significantly different from previous generation networks. As is often the case for new technologies, this new design comes with some security challenges. GCSB TICSAs role is to ensure the telecommunications industry manages and mitigates those risks.

## Space and High-Altitude Activities Act 2017

New Zealand's space industry provides significant economic opportunities for New Zealand.

New Zealand's environment is well-suited for space launches, given its uncluttered air space, which provides clear launch windows.

The Outer Space and High-Altitude Activities Act (OSHAA) 2017 provides a regulatory framework to manage any risks to New Zealand's national security and interests from the space industry.

GCSB and NZSIS undertake national security risk assessments for activities under OSHAA. These assessments provide advice to the Minister responsible for OSHAA, the Minister for Economic Trade and Development, and the Minister Responsible for the GCSB and NZSIS about any national security risks that may be associated with each activity.

The space industry in New Zealand continued to grow throughout 2018/19, including Rocket Lab's launch activities in Mahia, work being undertaken by local universities and foreign companies showing interest in establishing space-related programmes here.

In 2018/19, 29 assessments on space-related activities were undertaken, up from 24 in the previous year.

## High Assurance Services

The GCSB High Assurance Services (HAS) exists to provide assurance that New Zealand's most important information is free from technical compromise. HAS provides technical security and emanations security services. Technical Security services are focussed on countering technical surveillance techniques used by hostile actors, including eavesdropping and video surveillance. Emanations Security services are focussed on countering the threat posed by spread of unintentional signals from ICT equipment that could be intercepted and interpreted by hostile threats. In addition to technical and emanations security, HAS also provides recommendations to the Director-General GCSB on the accreditation of sensitive compartmented information (SCI) sites and systems. The Director-General of the GCSB is the New Zealand Government's accreditation authority for highly-classified information systems and sites.

HAS provides a number of services to government, including technical surveillance counter-measure (TSCM) inspections, emanations testing and inspections, as well as advice on the standards required for SCI site and system accreditation to be achieved. The inspections provide technical inspection services and advice, and seek to ensure that these facilities are free from vulnerabilities that would allow unauthorised access to information. The HAS team also has a mobile capability to inspect existing facilities for signs of technological efforts to compromise security.

# Secure Technology

The GCSB delivers secure information technology for the NZIC, and the wider national security sector. This role is crucial as this sector handles some of the Government's most sensitive information. It requires specialist technology, expertise and ongoing effort to ensure the information remains protected.

The GCSB is New Zealand's national authority on communications security. As part of this role the GCSB provides the technology, processes and key material used to protect the country's most sensitive information. Throughout 2018/19 the GCSB has continued to work on this infrastructure through the development of significant, complex, multi-year programmes, including:

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

These projects will secure the Government's most sensitive information into the future.

## High-grade Cryptographic Infrastructure

GCSB is working to update New Zealand's high-grade cryptographic infrastructure through the Cryptographic Products Management Infrastructure project. This allows government communications classified higher than RESTRICTED to be protected through advanced encryption.

GCSB made substantial progress on this project throughout 2019 by completing the installation of initial parts of the new infrastructure.

Due to the complexity and security associated with the systems involved, a lot of planning and consultation has been required to ensure the project is successful.

CPMI was always envisaged to be a multi-year project.







| Indispensable  
Intelligence

# Intelligence Collection

The GCSB is the New Zealand Government's signals intelligence agency; using technology to produce intelligence, which is used by New Zealand's decision makers to enhance New Zealand's national security and other interests.

The GCSB provides intelligence to Ministers, government agencies and international partners in order to support policy development and operational activity for New Zealand. The GCSB primarily collects signals intelligence, or SIGINT. This means that the GCSB collects and analyses electronic communications to produce intelligence. Through its role in collecting and analysing intelligence the GCSB contributes to the protection of New Zealand's national security, international relationships, economic wellbeing, and the safety and security of New Zealanders.

In 2018/19 the GCSB provided intelligence products to 17 government agencies and Ministers' offices. These intelligence products were developed through GCSB's own sovereign collection operations, and partner reporting.

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

Any intelligence collection or analysis undertaken by the GCSB is carried out in accordance with New Zealand law, including its human rights obligations, and is subject to strong independent oversight. The Intelligence and Security Act (ISA) allows the GCSB to collect intelligence under two types of 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.

## GCSB's role in domestic counter-terrorism

The GCSB's role in domestic counter-terrorism is to provide assistance to the NZSIS and the New Zealand Police at their request. This assistance is primarily the provision of technical capabilities and intelligence.

Over the past three years the GCSB has taken a series of deliberate steps to enable us to respond effectively to requests for assistance on domestic counter-terrorism, within the legislative and resource constraints. For example, the GCSB has established processes for responding to changing priorities and requests by other agencies for assistance under the Intelligence and Security Act 2017. As a result GCSB teams can be deployed across a range of intelligence priorities and agency requirements.

In the aftermath of the March 15 terrorist attacks the GCSB received tasking from NZSIS and New Zealand Police. Once tasked, the GCSB was quickly able to utilise capabilities to make a unique and material contribution to the investigation and the wider response.

## Monitoring the internet – what the GCSB does and doesn't do

The GCSB is able to target the communications of New Zealanders for intelligence gathering purposes, if it acquires a Type 1 warrant under the Intelligence and Security Act 2017. To obtain any type of warrant, the GCSB must show that the action is both necessary and proportionate.

One of the steps the GCSB has taken to counter violent extremism is to put in place warrants that allow us to gather intelligence about terrorism that do not differentiate between different forms of violent extremism. However, the GCSB does not have the legal authority, technical means, resourcing, or social licence to monitor all of New Zealand's internet traffic. For example GCSB cannot monitor all traffic to particular web sites and chat rooms, or who is uploading certain types of material.

# Regional Security

Security and resilience in the Pacific region has long been an important area of focus for New Zealand. The Pacific is increasingly becoming an area of strategic competition for great powers, with various states seeking to project influence and power into the region. This competition has the potential to have a detrimental effect on regional security.

Alongside the increase in strategic competition, transnational organised crime affects the security

of the Pacific region, and can easily spread to the surrounding region, including New Zealand.

The GCSB provides signals intelligence in relation to New Zealand's national interests in the South Pacific. This work focuses on providing intelligence products that support other government agencies that have the capability to respond to security issues in our region.

# Working with government agencies

Contributing to the protection of New Zealand's national security and well-being, and supporting the safety and security of New Zealanders at home and abroad, are key objectives of the GCSB.

One way of achieving this objective is by supporting other government agencies, through provision of relevant intelligence, so they can carry out their work. One of the GCSB's functions is to cooperate with the NZSIS, New Zealand Police, and the New Zealand Defence Force (NZDF).

## Working with Police

The GCSB responds to requests for intelligence from, and provides technical assistance to, the NZSIS and New Zealand Police on request. In the aftermath of the 15 March terrorist attacks, GCSB received tasking from NZSIS and New Zealand Police. Once tasked the GCSB was quickly able to make unique and material contributions to the investigation and the wider response.

## Working with New Zealand Customs

The GCSB has worked closely with New Zealand Customs throughout 2018/19. Our focus is on providing intelligence leads that will assist New Zealand Customs to prevent large scale drug importation.

Using GCSB signals intelligence capabilities we are supporting New Zealand Customs to better target drug networks with the aim of disrupting their efforts before they reach our shores.

The GCSB collection and analysis activity has helped to enhance New Zealand Customs' understanding of drug networks that seek to smuggle drugs to New Zealand.

## Supporting New Zealand Defence Force

In 2018/19 the GCSB continued to provide support to NZDF for its operations overseas. This primarily related to providing support to force protection, including keeping deployed New Zealanders safe and secure overseas.

# Continuous Improvement

As the threats New Zealand faces change, and technology becomes more advanced, it is critical that the GCSB continually improves its expertise and knowledge, technology, and reporting products. This work is crucial to achieving our mission.

## Customer Engagement

Throughout 2018/19 the GCSB continued its work on the joint programme, with the NZSIS and the Department of the Prime Minister and Cabinet, to improve how we engage with and deliver intelligence products and services to our customers.

During the year, the Customer Engagement team reviewed outcomes from trials of different ways of engaging with and delivering intelligence to customers. Trials demonstrated that providing customers with unique, tailored and coordinated intelligence that shapes their actions and decision-making will require resources and better systems to understand and tailor intelligence to meet customer needs, enhanced intelligence delivery

mechanisms, and improved support to customers to use intelligence.

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.

## Encryption

Strong encryption is a fundamental element of good cyber security, which is increasingly critical to New Zealand's national security and economic prosperity. The GCSB supports the use of strong encryption; however it can impede the access of law enforcement, and intelligence and security agencies, to communications critical to conducting their investigations.

Developing technologies and enhanced security practices present the GCSB with new and unique challenges to our lawful intelligence collection activities.

# International Partnerships

## Five Eyes

Australia, Canada, the United Kingdom and the United States of America, along with New Zealand, make up an international intelligence and security partnership known as the Five Eyes. Working within this partnership provides New Zealand with greater support, technology and information than it would otherwise have. The community is fundamental to GCSB's work to support New Zealand's national security and interests, and ensure the wellbeing of New Zealanders both at home and abroad. We could not deliver our current level of intelligence and security activity alone.

The Five Eyes partnership has been at the core of New Zealand's intelligence and security activities since World War Two. Initially the partnership was a cryptographic venture to share efforts and results in code breaking, and code making, during the war. Following that work a wider partnership was established, involving all aspects of security and intelligence, which continues today.

The GCSB's participation in the Five Eyes partnership is subject to New Zealand law, including human rights obligations, and to the laws of partner countries that share information or other support with us.

## Other International Partners

As well as our participation in the Five Eyes partnership the GCSB collaborates with a range of other nations. The GCSB has procedures in place to ensure that any intelligence sharing with other countries is managed in compliance with New Zealand's laws, including all human rights obligations.

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 hostile cyber activities, transnational organised crime and violent extremism.





| Our  
People



# Our Values



## Respect

We respect the role that each individual plays in the organisation.

We value diversity in thought and approach.

We treat each other with dignity.



## Integrity

We act lawfully and ethically.

We are accountable for our actions – both personally and organisationally.

We act professionally and with respect.



## Commitment

We are committed to our purpose.

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

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

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



## Courage

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

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

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

We perform at pace, are flexible and responsive to change.

# Leadership



## Director-General of the Government Communications Security Bureau

Andrew Hampton began his term as Director-General (formerly the Director) of the Government Communications Security Bureau (GCSB) in April 2016.

Beyond the specific responsibilities set out in the ISA 2017, the Director-General has the below responsibilities (set out in 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 GCSB services and the effective provision of those services, ensuring they contribute to intended outcomes.

In 2018 the Director-General became the Government Chief Information Security Officer, or GCISO.

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 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).

## Leadership Development

Equipping and developing leaders as the organisation grows and evolves remains a priority across the NZIC. The NZIC leadership competency framework aligns with the State Services Commission framework and the core competencies expected of leaders are included in all people managers' performance and development reviews.

The majority of our managers have attended face to face training on unconscious bias. Managers and staff have also had the opportunity to attend courses on neuro-diversity, Crown and Māori Relations and Te Reo.

# Retain, Develop and Recruit the Best People

The GCSB is a Public Service Department with 476.3 full-time equivalent staff, as at 30 June 2019.

The GCSB is able to deliver on its mission to protect and enhance New Zealand's security and wellbeing because of the unique skills and innovation of our people.

Our people, and their varied skill sets, are what make the work of the GCSB possible. Throughout 2018/19 the GCSB has focused on retaining the existing workforce and providing opportunities for growth and development.

Recruiting the best people has also been a priority of the GCSB throughout 2018/19. The GCSB employs people from a wide range of disciplines, including foreign language experts, communications and cryptography specialists, engineers and technicians and support staff. Over the past year efforts have been focused on ensuring that recruitment resources reflect that we want a more diverse workforce.

Work has begun to better understand the perceptions 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.

## 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.

In the past the GCSB has benefited from relatively low rates of staff turnover. In 2018/19 the turnover rate has increased by five per cent, which brings it in line with the public sector average from 2017/18. A contributing factor for this is that we operate in an increasingly competitive environment where the skills we use (particularly in technology) are also highly sought after in the private sector. This is an ongoing challenge for us.

As part of the effort to improve staff retention the GCSB provides staff with a clear view of career pathways, and has increased our focus on learning and development throughout the intelligence and security sector as a positive way to retain skills and foster career progression.

## GCSB Core Unplanned Staff Turnover (2015 to 2019)

GCSB staff	2015/16	2016/17	2017/18	2018/2019
Staff Turnover	9.3%	6.9%	7.1%	12.0%
Public Service	11.1%	11.5%	12.1%	Not yet available

## Skilled staff

The GCSB supports staff to develop and maintain the most up-to-date skills, knowledge and capabilities so they can deliver on their complex and technically challenging work.

Throughout 2018/19 we have increased the number of face to face internal and external professional development courses. We have trained nine anti-harassment advisors and developed online training on anti-bullying and harassment. Key relationships have been strengthened with Victoria University, the Combined Legal Agencies, Massey University Research Network, New Zealand Police, and the New Zealand Defence Force. We have also worked with several independent training providers to develop learning opportunities that are especially relevant to the intelligence community.

To support and inspire the careers of women in the wider intelligence community, a women's mentoring programme was established in June 2018 under the Department of the Prime Minister and Cabinet's National Security Workforce programme. The programme is part of our work to retain and develop women working in the intelligence and security sector.

Twenty four of our female staff took part in the programme as mentorees and seven as mentors.

## Career Pathways

The Career Pathways and Career Board system was introduced within 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.

This year the GCSB reviewed the Career Boards to ensure it is still meeting the agency's needs. Between 1 July 2018 and 30 June 2019, GCSB had 22 staff progressing to a higher level of technical competence through the Career Boards.

## Workforce planning

The NZIC continues to work to a National Security Workforce programme, which sets out current and future workforce requirements. This work programme seeks to ensure the NZIC has the workforce in place to deliver the intelligence and security outcomes expected by the Government and New Zealanders.

The skillset needed in the GCSB has changed over the years. This is something that is continually assessed to make sure we have the right capability in place. Over the past year, we have continued our focus on establishing a robust approach to workforce and resource planning to ensure all recruitment activity is aligned with the GCSB's strategic objectives.

## Pipeline of Talent

A key part of ensuring the ongoing resilience of the GCSB workforce is the graduate recruitment programme. In 2018/19 the GCSB ran the graduate recruitment programme to attract new talent into the organisation. The graduate programme is designed to ensure graduates get a wide range of experiences within GCSB before they are appointed to a permanent role.

Throughout 2018/19, 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 female candidates.

The number of female graduates applying for the annual GCSB intake in 2018/19 is reasonably consistent with last year's. We received a total of 299 applications, of which 134 (44.8%) were females. The low numbers of female science, technology, mathematics and engineering (STEM) students continues to be of concern, which is why GCSB sponsors and participates in events which target women who study STEM subjects.

## Supporting Women in STEM

GCSB undertook a 'Women in STEM' (science, technology, engineering and mathematics) scholarship programme for a second year in 2018/19. 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.

This year we received a total of 143 applications for the scholarship, which was a significant increase from the 79 applications received in 2017. Applications came from all of our main universities in New Zealand, with good numbers from University of Auckland (35), Victoria University of Wellington (29), University of Otago (20) and University of Waikato (19). We also received a small number from polytechnics throughout New Zealand.

# Diversity in the Workforce

To better protect and enhance New Zealand's security and wellbeing, our workforce must reflect the diverse community that we serve. The GCSB and the wider NZIC is committed to developing a dynamic and agile workforce to harness the benefits of different ideas, perspectives and cultural experiences. A diverse workforce is essential for better decision making and a key contributor to improving public trust and confidence.

The Diversity and Inclusion Strategy for the NZSIS and the GCSB was launched in March 2018 and provided a roadmap of the steps the organisations are committed to take.

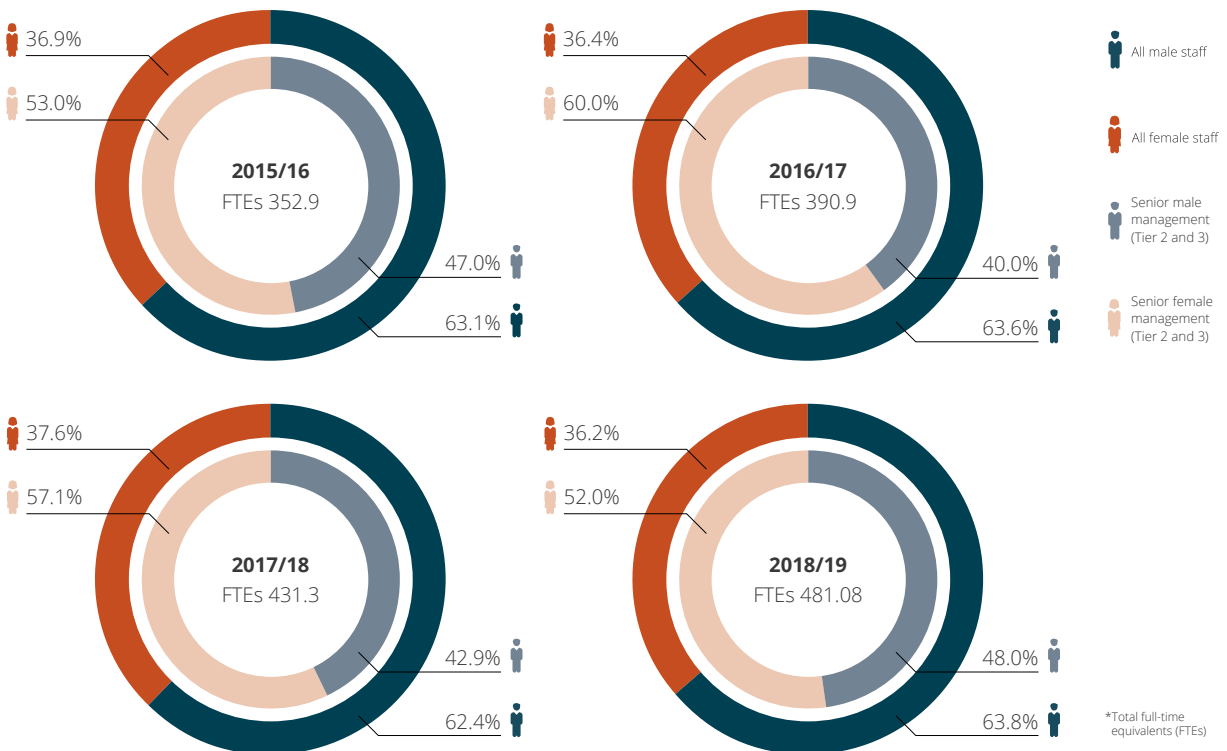
The strategy defines four goals around workforce diversity: diversity through workforce, leadership, workforce inclusion, and sustainability and accountability.

There is also an opportunity for us to make significant inroads with increased representation from those who identify as Māori or Pasifika. By 2020, the GCSB aims to be recognised as an inclusive, diverse and progressive organisation which maximises capability through its workforce. Further to this we want to embrace, promote and encourage diversity in our workforce and our thinking.

## Gender Diversity

Women make up more than half of GCSB's senior management group. While it is encouraging to see gender diversity in the senior management group it remains an area of focus for the GCSB to improve the representation of women across the whole of the organisation. Initiatives such as the scholarship supporting women in STEM subjects are a part of our efforts to improve this representation.

### GCSB Gender Representation (2015 to 2019)



## Closing the Gender Pay Gap

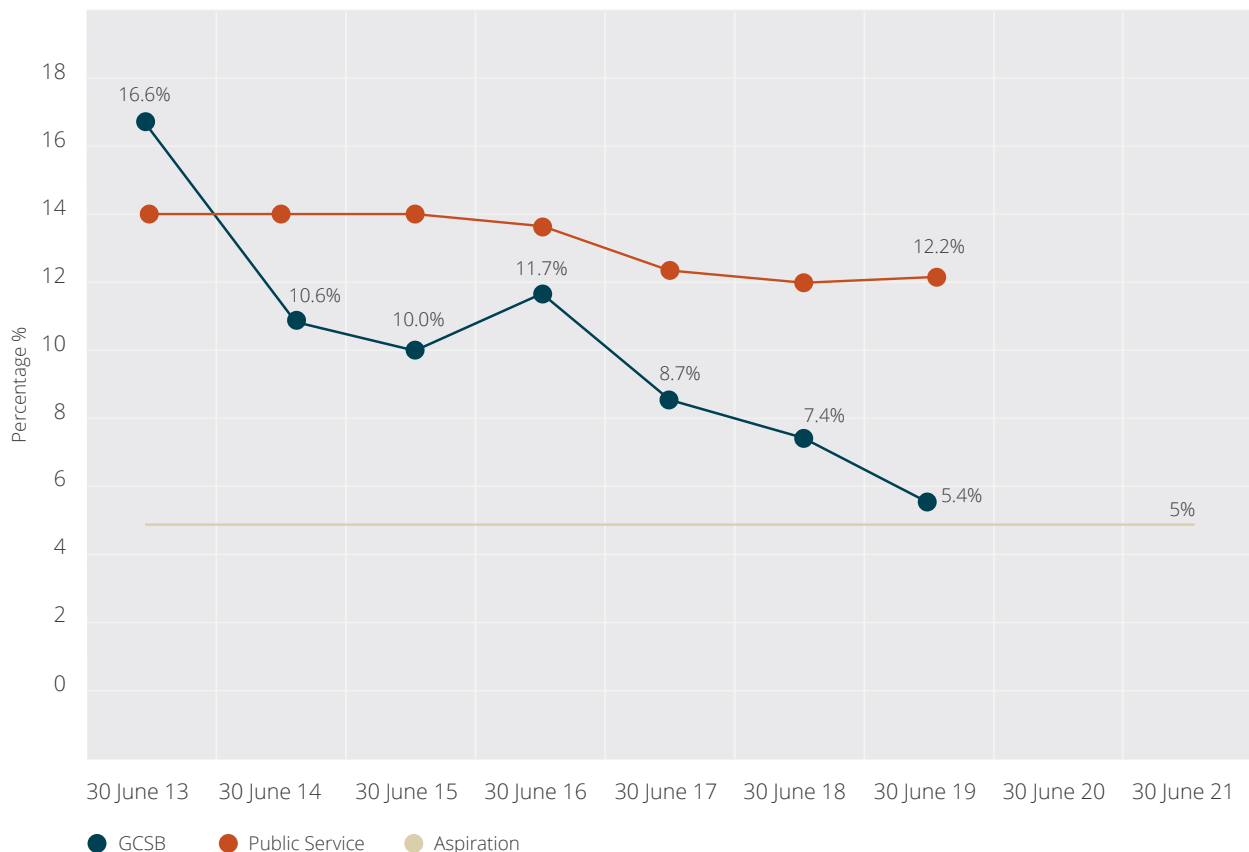
Closing the gender pay gap has been a focus for the GCSB with a target of reducing the gap to a maximum of five per cent by 2021. At the end of the financial year, the gender pay gap in the GCSB was 5.4 percent.

Work to reduce the gender pay gap is being undertaken in collaboration with staff associations and network groups throughout the NZIC. The gender pay gap work feeds into the wider programme established by the State Services Commission seeking to resolve the gender pay gap across the public service.

## Ethnic Diversity

GCSB is working to improve the ethnic representation of its workforce, and has achieved modest improvement in some areas. In 2018/19 the GCSB continued to implement the Diversity and Inclusion strategy. The strategy ensures we have diverse talents, views and thinking, which is critical to achieve our mission. It will take time for new recruitment strategies to be reflected in workforce statistics; however the GCSB is committed to this work.

### Gender Pay Gap – no higher than 5% by 2021



## GCSB Staff Ethnicity (2015 to 2019)

	2015/16	2016/17	2017/18	2018/19
New Zealand European & European	69.0%	68.7%	67.6%	67.8%
New Zealander	N/A	N/A	27.5%	29.4%
New Zealander Māori	6.5%	7.2%	7.8%	7.2%
Asian	5.8%	5.4%	4.9%	5.4%
Pacific Peoples	1.6%	1.8%	2.8%	2.3%
MELAA	0.3%	0.3%	0.3%	0.9%

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

## Launching new staff networks

The GCSB is committed to supporting its staff to come to work as their authentic selves. As a part of this commitment the GCSB continues to support the Women of the New Zealand Intelligence Community (WNZIC) network.

In 2018/19 the WNZIC was joined by Standing Out, which is our LGBTQI+ network. Standing Out was launched by Hon Andrew Little, Minister Responsible for GCSB and NZSIS.

In doing so we raised the Rainbow flag at Pipitea House to mark the Wellington Pride festival.

We established an ethnicity network and a health and well-being network in 2018/19. These groups work with leadership to improve the diversity, inclusion and culture of our agencies.

The networks have been actively involved in organising events, providing speakers and supporting staff. We have celebrated and acknowledged a number of special days and events, including Pink Shirt Day, Sign Language Week, Māori Language Week, and Mental Health Week.

## Rainbow Tick Accreditation

The NZSIS and GCSB have been working on acquiring the Rainbow Tick certification for the past year as part of our Diversity and Inclusion work plan.

The evaluation of policies and procedures and facilitation of focus groups occurred between April and June 2019 and were conducted by Kāhui Tū Kahu the charitable company that manages the Rainbow Tick. Accreditation of the Rainbow Tick has been achieved and will be effective from 12 July 2019. While there is more we can do, we are very proud of this achievement.



## Mental Health and Wellbeing

We take the mental health and wellbeing of our staff very seriously. In the past year we have established an in-house Psychological service, as well as run weekly counselling and psychological clinics. We are conscious that the work our staff undertakes can be challenging and we want to ensure they feel, and are, well supported. We have also provided resources for staff to manage health including online programmes such as practising mindfulness.



# Locations

The GCSB head office is located in Wellington, with a regional office in Auckland. The GCSB has two communications collection and interception stations; one, a high frequency radio interception and direction-finding station near Palmerston North and the other, 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).





# | Oversight and Legal Compliance

# The Intelligence and Security Act 2017

Oversight is of fundamental importance to the GCSB and is something that we value highly.

Strong oversight, comprehensive legal frameworks and good governance all contribute to New Zealanders trust and confidence in their intelligence agencies.

The ISA provides the legal framework for GCSB and NZSIS activities.

The ISA sets out objectives and functions of the GCSB and NZSIS, and provides the mechanism for the agencies to carry out otherwise unlawful activities. There are 11 Ministerial Policy Statements that set out Ministerial expectations and guidance for the agencies on how certain lawful activities should be conducted.

## Office of the Inspector General Intelligence and Security

The Inspector-General of Intelligence and Security (IGIS) and her office are a fundamental oversight body for the GCSB and NZSIS. The IGIS provides assurance to the New Zealand public that the activities of the GCSB are lawful and proper. The IGIS also provides an avenue for public complaints against the agencies. The GCSB regularly engages with the Office of the IGIS to discuss issues and provide information and resources to support IGIS investigations and queries.

The 2018/19 year was a significant one for oversight inquiries and the GCSB prioritised significant resource to meet our obligations. This engagement often involves extensive searches of our resources and engagement with foreign partners.

### Compliant systems and processes

Over the past five years the IGIS has certified in her annual report the GCSB has sound compliance systems and processes in place.

### Type 1 and Type 2 Warrants Report

GCSB had extensive discussions with the IGIS, NZSIS and Crown Law about the law on when Type 1 warrants are required. There were differences in approach to interpretation of the law between the agencies and the IGIS. GCSB reached a considered view of what the law required before it came into effect, and obtained Crown Law advice on that view. After the IGIS suggested a different interpretation of the law, GCSB and NZSIS sought further advice from Crown Law. The advice provided by the Solicitor-General to the agencies differed to that of the IGIS, and the IGIS accepts GCSB and NZSIS are obliged to follow the advice of the Solicitor-General.

### Inquiry into possible New Zealand intelligence and security agencies' engagement with the CIA detention and interrogation programme 2001-2009

The GCSB contributed significantly to this IGIS inquiry and we are pleased that the report found that the GCSB had no direct involvement in the CIA's detention and interrogation programme 2001–2009 and was not complicit in any unlawful conduct.

The findings are a testament to the professionalism, integrity and good judgement of the GCSB staff that provide intelligence support to New Zealand's military deployment to Afghanistan, in very difficult circumstances.

We acknowledge the IGIS' recommendations for improvement in the support, training and supervision for deployed staff. Much has changed in the 10 to 15 years since the deployments covered in the Senate report and training and supervision has improved significantly. The recommendations included in the report will be considered and changes made where appropriate.

### Ongoing inquiries

The GCSB is also responding to several ongoing inquiries, working with both the IGIS and other external inquiries. These include the Royal Commission into the Christchurch Terrorist Attacks and the Inquiry into Operation Burnham.

## The Intelligence and Security Committee

Due to the nature of the GCSB's work a significant amount of our activities are classified. This means that the agency is unable to talk about much of our work in public.

Strong and effective oversight of GCSB activities is a crucial to assure the New Zealand public and the government of the day that the agency acts within the law and adheres to New Zealand's principles.

The Intelligence and Security Committee (ISC) undertakes parliamentary oversight of the GCSB and NZSIS. The ISC's role is to examine the policy, administration and expenditure of both agencies.

The ISC is currently made up 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.

## The Justice Select Committee Inquiry

In 2019 the Directors-General GCSB and NZSIS appeared before the Justice Select Committee inquiry into the 2017 General Election and the 2016 Local Election. The two agencies were invited to appear before the inquiry to provide advice and insights into the potential for foreign interference in New Zealand's elections.

The GCSB will continue to work with the Justice Committee, Ministers, Members of Parliament and the Electoral Committee to mitigate foreign interference risks to the next General Election.

# Official Information and Privacy Act Requests

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 transparent as possible. Each request is assessed on a case by case basis, and national security concerns are considered against the public interest using the guiding statutory principles.

For the period from 1 July 2018 to 30 June 2019, the GCSB:

- Completed 76 OIA requests, with 7 requests not completed within the legislated timeframe.
- Completed 31 Privacy Act requests, with all completed within the legislated timeframe.

The GCSB aims to complete all of these information requests within the legislated timeframe. In the 2018/19 year the GCSB has directed more resource to support processing these requests.

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

For the period 1 July 2018 to 30 June 2019, one OIA complaint was completed by the Office of the Ombudsman. While the complaint was made within the time period, the Ombudsman formed their opinion outside the reporting period. The Ombudsman found in favour of the requestor and the GCSB released the requested information as a result.

Two complaints were raised with the Office of the Privacy Commissioner during the period. In both cases the Office of the Privacy Commissioner upheld the decisions made by the agency.



Financial  
Statements

# Independent Auditor's Report

To the readers of  
the Government  
Communications Security  
Bureau's statement of  
actual expenses and  
capital expenditure  
against appropriation  
for the year ended  
30 June 2019.

The Auditor-General is the auditor of the Government Communications Security Bureau (the GCSB). The Auditor-General has appointed me, Stephen Lucy, using the staff and resources of Audit New Zealand, to carry out, on his behalf, the audit of the statement of actual expenses and capital expenditure against appropriation of the GCSB for the year ended 30 June 2019 on page 51.

## Opinion

In our opinion the statement of actual expenses and capital expenditure against appropriation of the GCSB is presented fairly, in all material respects, in accordance with the requirements of section 221(4)(a) of the Intelligence and Security Act 2017.

Our audit was completed on 30 September 2019. This is the date at which our opinion is expressed.

The basis for our opinion is explained below and we draw attention to a contingency for entitlements under the Holidays Act 2003. In addition, we outline the responsibilities of the Director-General of the GCSB and our responsibilities relating to the information to be audited, we comment on other information, and we explain our independence.

## Contingency for entitlements under the Holidays Act 2003

Without modifying our opinion, we draw your attention to the disclosure on page 51 relating to the GCSB's contingent liability to remediate issues associated with the calculation of entitlements under the Holidays Act 2003, which could be significant.

## 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 audit opinion.

## Responsibilities of the Director-General of the GCSB for the information to be audited

The Director-General of the GCSB is responsible on behalf of the GCSB for preparing a statement of actual expenses and capital expenditure against appropriation of the GCSB that is presented fairly, in accordance with the requirements of the Intelligence and Security Act 2017.

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

In preparing the information to be audited, the Director-General of the GCSB is responsible on behalf of the GCSB for assessing the GCSB's ability to continue as a going concern. The Director-General of the GCSB 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 of the GCSB's responsibilities arise from the Public Finance Act 1989 and the Intelligence and Security Act 2017.

## Responsibilities of the auditor for the information to be audited

Our objectives are to obtain reasonable assurance about whether the information we audited, as a whole, is 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 information we audited.

For the budget information reported in the information we audited, our procedures were limited to checking that the information agreed to the Estimates and Supplementary Estimates of Appropriations 2018/19 for Vote Communications Security and Intelligence.

We did not evaluate the security and controls over the electronic publication of the information we audited.

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 information we audited, 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 of the GCSB.
- We conclude on the appropriateness of the use of the going concern basis of accounting by the Director-General of the GCSB 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 information we audited 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 information we audited, including the disclosures, and whether the information we audited represents the underlying transactions and events in a manner that achieves fair presentation in accordance with the requirements of the Intelligence and Security Act 2017.

We communicate with the Director-General of the GCSB 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 of the GCSB is responsible for the other information. The other information comprises the information included in the Annual Report other than the information we audited, and our auditor's report thereon. This other information is expected to be made available to us after the date of this auditor's report.

Our opinion on the information we audited 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 when it becomes available. In doing so, we will consider whether the other information is materially inconsistent with the information we audited 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 communicate the matter to the Director-General of the GCSB.

## 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.



**S B Lucy**  
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 2019 and its operations for the year ended on that date.



**Andrew Hampton**

Director-General of the GCSB

30 September 2019

# Statement of expenses and capital expenditure against Appropriation for the year ended 30 June 2019

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

	<b>\$000</b>
Total appropriation	\$180,002
Actual expenditure	\$129,849

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.

## Variance Explanation

The majority of the underspend this year relates to the timing of the Cryptographic Products Management Infrastructure project which is spanning multiple financial years.

## Holidays Act entitlements

GCSB is aware of a wide-spread issue where some agencies have identified issues with calculating and paying entitlements under the Holidays Act 2003. GCSB is currently reviewing its compliance under the Act. The initial review phase has now been completed and has identified uncertainties in the application of parts of the Act to GCSB staff and therefore the requirement for a full review. GCSB's liability cannot be reliably estimated at this time and therefore no provision has been recognised at 30 June 2019. The GCSB acknowledges that the potential liability could be significant as the issue affects current and past employees and covers a number of years.



GOVERNMENT  
COMMUNICATIONS  
SECURITY BUREAU  
TE TIRA TIAKI

New Zealand Government