G.56 (2020)

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

2020 ANNUAL REPORT

www.gcsb.govt.nz

PREFACE

This is the annual report of the Government Communications Security Bureau (GCSB) for the year ended 30 June 2020, 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.

GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

Contents

Overview of the Year

Director-General's Overview

The Government Communications Security Bureau's (GCSB) response during the COVID-19 pandemic has unsurprisingly been a key focus during this reporting period. The GCSB, along with the New Zealand Security Intelligence Service (NZSIS), was designated an essential service for the purposes of national security and maintained core functions during Alert Levels 4 and 3 of the COVID-19 response.

Like most organisations during this period, the GCSB had to rapidly change the way it operated to minimise the risk to staff while maintaining continuity of essential functions. This required agile and innovative thinking given that much of our work involves highly classified information and systems.

I am proud of how GCSB staff responded to the unique challenges we faced. This enabled us to deliver on our mission whilst still ensuring the health and safety of our staff was prioritised.

There was an increase in demand for pandemic-related intelligence from a range of new and existing customers, and we worked hard to meet this demand, including information and assessments relating to the international contexts of COVID-19.

Remote working quickly became the norm for many organisations during lockdown, both in the public and private sectors. The GCSB, through my role as Government Chief Information Security Officer, provided advice to agencies on secure remote working solutions, including the use of video conferencing tools and communication apps.

COVID-19 has also accelerated the pace of change and adoption of technologies, which in turn increases risks and creates more opportunities for malicious actors. The GCSB's National Cyber Security Centre (NCSC) published a range of advice to customers, much of which was made publicly available, to increase resilience to COVID-19 related threats and vulnerabilities.

The GCSB, on behalf of the New Zealand Government, also added its voice to international condemnation of COVID-19 themed malicious cyber activity. This involved the targeting of critical infrastructure in some countries, although such activity has not been observed in New Zealand. Of particular concern is state sponsored malicious cyber activity aimed at organisations involved in COVID-19 vaccine development.

While many of the cyber security risks and challenges posed by COVID-19 are not new, they illustrate how malicious cyber actors opportunistically exploit the public's desire for information, and use this as a lure for malicious activity.

During the reporting period the NCSC recorded 353 incidents in the 12 months to 30 June 2020, compared with 339 incidents in the previous year. Of these incidents, 30% had links to known state-sponsored actors.

The NCSC also continued to see incidents where malicious cyber actors have exploited known, unpatched vulnerabilities to gain access to systems. This can be prevented through security patching, regular security testing, and taking additional steps to secure critical data.

During the year we responded to a range of cyber incidents involving organisations of national significance or that had a potentially national impact. We also continued to provide high grade cyber security detection and disruption to organisations through our CORTEX services.

This year the GCSB has provided support for the general election to ensure our electoral processes are protected from foreign interference and malicious cyber activity. An updated protocol has been developed in consultation with the Electoral Commission which sets out the principles of how the GCSB and NZSIS would perform their mandated functions should potential threats to the election be detected.

The GCSB has continued to respond to several ongoing inquiries during the reporting period, including the Royal Commission of Inquiry into the Attack on Christchurch Mosques, the Government Inquiry into Operation Burnham and the Inspector-General of Intelligence and Security (IGIS) Inquiry into the role of the GCSB and the NZSIS in relation to certain specific events in Afghanistan, which ran in parallel with the Operation Burnham inquiry.

The inquiries have at times involved significant GCSB resources, however such oversight is essential to the Government and the public having trust and confidence that the intelligence agencies act within New Zealand law and with propriety. The IGIS's report found that the intelligence agencies provided essential support to New Zealand Defence Force operations in Afghanistan, and that the GCSB appropriately shared information, however the IGIS considered that more could have been done with that information.

It is essential that we reflect the communities we serve and the GCSB has continued to focus on the diversity of its workforce. While there is still work to do I am pleased to note that our gender pay gap at the end of the 2019/20 financial year was 4.9%, which is well ahead of the 12.2% public service average.

The strength of the GCSB is its people, and I am privileged to lead a team which has risen admirably to the unique challenges of this reporting period. The nature of our work means much of what we do cannot be disclosed, but this report reflects what we can say publicly and what the GCSB team has achieved this year.

Andrew Hampton
Director-General of the Government Communications Security Bureau

Such oversight is essential to the Government and the public having trust and confidence that the intelligence agencies act within New Zealand law and with propriety.

Notable Achievements

COVID-19 RESPONSE

The GCSB was designated an essential service and maintained core functions over Alert Levels 4 and 3.

Intelligence collection and dissemination

The GCSB provided a significant amount of intelligence to New Zealand government customers in response to the evolving global COVID-19 pandemic. The GCSB continued to deliver critical intelligence relating to the pandemic and other national security matters; and maintained its 24/7 watch and warn service during the COVID-19 lockdown.

Cyber security

The GCSB's National Cyber Security Centre (NCSC) provided COVID-19 cyber threat intelligence to inform national intelligence products, and published advice to customers to help increase their resilience to COVID-19 related threats and vulnerabilities.

Supporting Working Remotely

In our role as Government sector leaders for information security, the Director-General, as the Government's Chief Information Security Officer (GCISO), provided advice to agencies to quickly enable them to set up remote working solutions for their organisations while understanding security risks and mitigations.

Contact Tracing Technology

The NCSC provided technical advice to support the Ministry of Health on the development of a contact tracing app. This work is on-going.

Call-out of COVID-19 Malicious Actors

In mid-May, the Director-General made a statement on behalf of the Government condemning international cyber actors taking advantage of the COVID-19 pandemic to carry out malicious cyber activity.

IMPENETRABLE INFRASTRUCTURE

Cyber security incidents

The NCSC recorded 353 incidents in the 12 months to 30 June 2020, compared with 339 incidents in the previous year. The NCSC was able to identify indicators linking state-sponsored cyber actors to 30% of total incidents recorded in 2019/20.

The GCSB also 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.

Information Assurance and Cyber Security strategic refresh

As part of an ongoing strategic review, the GCSB has completed a refresh of its Information Assurance and Cyber Security strategic plan and priorities. The four year strategy to 2024 defines the GCSB's purpose to "create a safer digital world for New Zealand to prosper" and establishes a strategic vision to "enable the protection, wellbeing and prosperity of New Zealand through trusted information security services".

CORTEX

CORTEX continues to be a key tool we use to support nationally significant organisations (NSOs) to protect their networks from malicious, advanced, persistent and sophisticated cyber security threats.

Government Chief Information Security Officer

Through the Director-General's role as GCISO, the GCSB takes a strategic approach to identifying security risk and working across agencies to help enable effective responses. This includes identifying technical responses and making sure we have effective policy settings across government.

The GCISO continues to support ongoing work led by the Government Chief Digital Officer around the system setting and leadership needed to improve how the public service operates in the digital environment. This work included an assessment of ICT capability of public service departments, and led to a Cabinet directive for smaller agencies around ICT procurement, accreditation, security standards and policy.

Election security

The integrity of New Zealand's electoral process is at the heart of our democratic society and elections must be free and fair. Relevant agencies take all the appropriate steps to be prepared for any activity that might affect New Zealand's elections.

A protocol was in place for the New Zealand Security Intelligence Service (NZSIS) and GCSB should they suspect interference in the 2017 General Election. The protocol was never activated. In the lead-up to the 2020 election, the protocol was reviewed and revised in consultation with the Electoral Commission.

The GCSB has worked closely with New Zealand's security partners on their experiences of elections and is constantly considering threats and vulnerabilities.

The NCSC has engaged directly with the Electoral Commission to provide cyber security advice and support to reinforce its cyber security resilience.

Cyber security customer engagement

The NCSC's Cyber Resilience Unit (CRU) works closely with more than 250 NSOs to understand their cyber resilience and vulnerability to attack, providing advice, support and cyber threat alerts to help organisations lift their overall cyber security resilience.

During the reporting period, the CRU recorded 1,770 engagements with customers across the broad spectrum of public and private sector organisations.

Security information exchanges

The CRU facilitates security information exchanges where participants can share information in a confidential and trusted environment. In the current reporting period, the CRU facilitated 20 security information exchanges, which enhanced collaboration on cyber security challenges and opportunities across all sectors.

Cyber security advisories

In the 12 months to 30 June 2020, the CRU published 24 reports for general customers identifying specific cyber security vulnerabilities, providing cyber threat mitigation advice and reinforcing cyber security best practice to assist raise overall cyber security resilience.

In late 2019, the NCSC published guidance for executive boards to help improve cyber security governance. The guidance, Charting Your Course: Cyber Security Governance, is intended to support executive decision making around cyber security resilience and risk.

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

Under TICSA, the GCSB assesses any changes to public telecommunications networks that may introduce network security risks.

During the reporting period, the GCSB received 145 notifications from network operators regarding proposed changes to their networks. Many of these notifications included proposals related to the rollout of fifth generation mobile services (5G).

Outer Space and High-altitude Activities Act 2017 (OSHAA)

The GCSB, in conjunction with the NZSIS, assesses any application for a license or permit submitted under OSHAA for national security risks. During the reporting period, 31 national security risk assessments were conducted, which provide the basis for advice provided by the Minister responsible for the GCSB and NZSIS to the Minister responsible for OSHAA.

Overseas Investment (Urgent Measures) Amendment Act 2020 (OIAA)

On 16 June 2020, a new emergency notification regime for foreign investment came into force, overseen by the Overseas Investment Office. The GCSB supports NZSIS in the assessment of transactions that may raise a national security risk.

The GCSB, working in conjunction with the NZSIS, created systems and processes to undertake these assessments. No notifications were referred for review within the reporting period.

INDISPENSABLE INTELLIGENCE

Provision of intelligence

Throughout 2019/20 the GCSB continued to supply intelligence to 22 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 2019/20 the GCSB continued to work closely with a variety of government agencies, including New Zealand Police, New Zealand Customs Service and Immigration New Zealand. This work contributes to the protection of New Zealand's national security and wellbeing.

Establishment of a joint customer services team

In 2019/20, the GCSB agreed to establish a joint business unit with the NZSIS and Department of the Prime Minister and Cabinet (DPMC) to improve our approach to provision of intelligence and assessments to support our customers. The joint team will know our customers and what matters to them, sharing a common understanding of their business needs and how to best provide high impact, tailored intelligence that will shape their decision-making. Implementation of the joint customer services team will be phased over four years commencing in the 2020/21 financial year.

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.

ORGANISATIONAL HEALTH

Budget 2020

In Budget 2020, the New Zealand Intelligence Community (NZIC) received $146 million of new funding, over four years. The GCSB will receive the largest portion ($100 million) of this funding, as it houses services shared with the NZSIS. This funding will ensure the NZIC continues to develop new capabilities and build capacity to respond to the changing strategic environment, particularly as the world recovers from COVID-19.

Improving gender and diversity representation

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.

GCSB undertook a 'Women in STEM' (science, technology, engineering and mathematics) scholarship programme for a third year in 2019/20. This year we received a total of 72 applications for the scholarship. The calibre of applicants was extraordinary, resulting in four scholarships being awarded. Two of our winners identify as New Zealand European, one identifies as New Zealand European and Pasifika, and the other identifies as New Zealand European and Māori.

The gender pay gap

At the end of the 2019/20 financial year, the gender pay gap in the GCSB was 4.9%. This is a decrease of 0.5% from 5.4% in 2018/19, and puts us ahead of our goal of having a gender pay gap no higher than 5% by 2021.

GCSB Strategic Context

The New Zealand Intelligence Community

The GCSB, along with the NZSIS and the National Security Group within the DPMC perform the national intelligence and assessment functions within the NZIC, complementing the specialist intelligence functions of other agencies such as New Zealand Police, New Zealand Customs Service and Immigration New Zealand. The NZIC is dedicated to contributing to the national security and wellbeing 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 NZIC contributes to building a safer and more prosperous New Zealand. NZIC agencies work to ensure that New Zealand is protected from harm and that New Zealand policy makers have intelligence to support good decision making. The NZIC strives to advance New Zealand's international reputation and interests.

The core NZIC agencies are:

Government Communications Security Bureau

The 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

The 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.

New Zealand Security Intelligence Service
Te Pā Whakamarumaru

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

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

NATIONAL SECURITY AND INTELLIGENCE PRIORITIES

The Government's 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 risks to New Zealand's security and wellbeing.

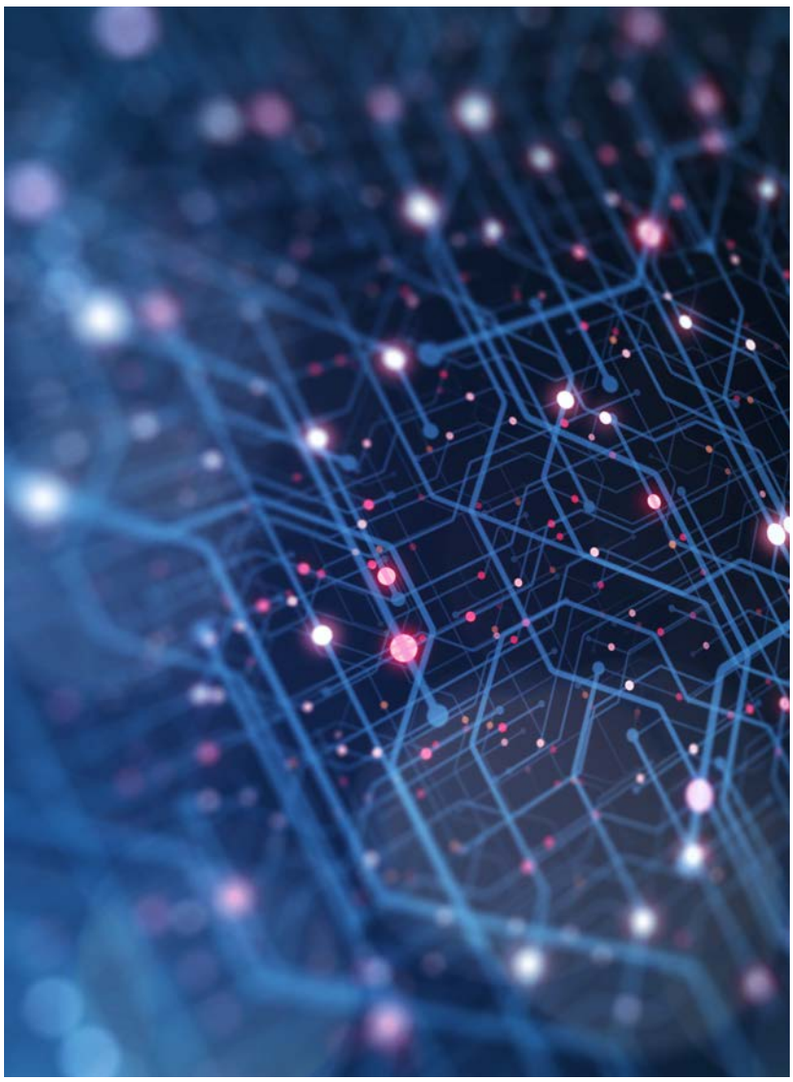
The NSIPs are coordinated by the DPMC and a range of agencies, including the GCSB, work toward achieving them.

The current priorities were approved in December 2018. They 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 and decision making, and to carry out their legislatively mandated functions. We also have a statutory role to provide cyber security and information assurance services to organisations of national significance.



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:

- Producing and disseminating signals intelligence in accordance with the Government's priorities;
- Providing information assurance and cyber security services, advice and assistance;
- Performing regulatory functions relating to the identification and mitigation of national security risks; and
- Co-operating with, and assisting NZSIS, Police and the NZDF in the performance of their functions.

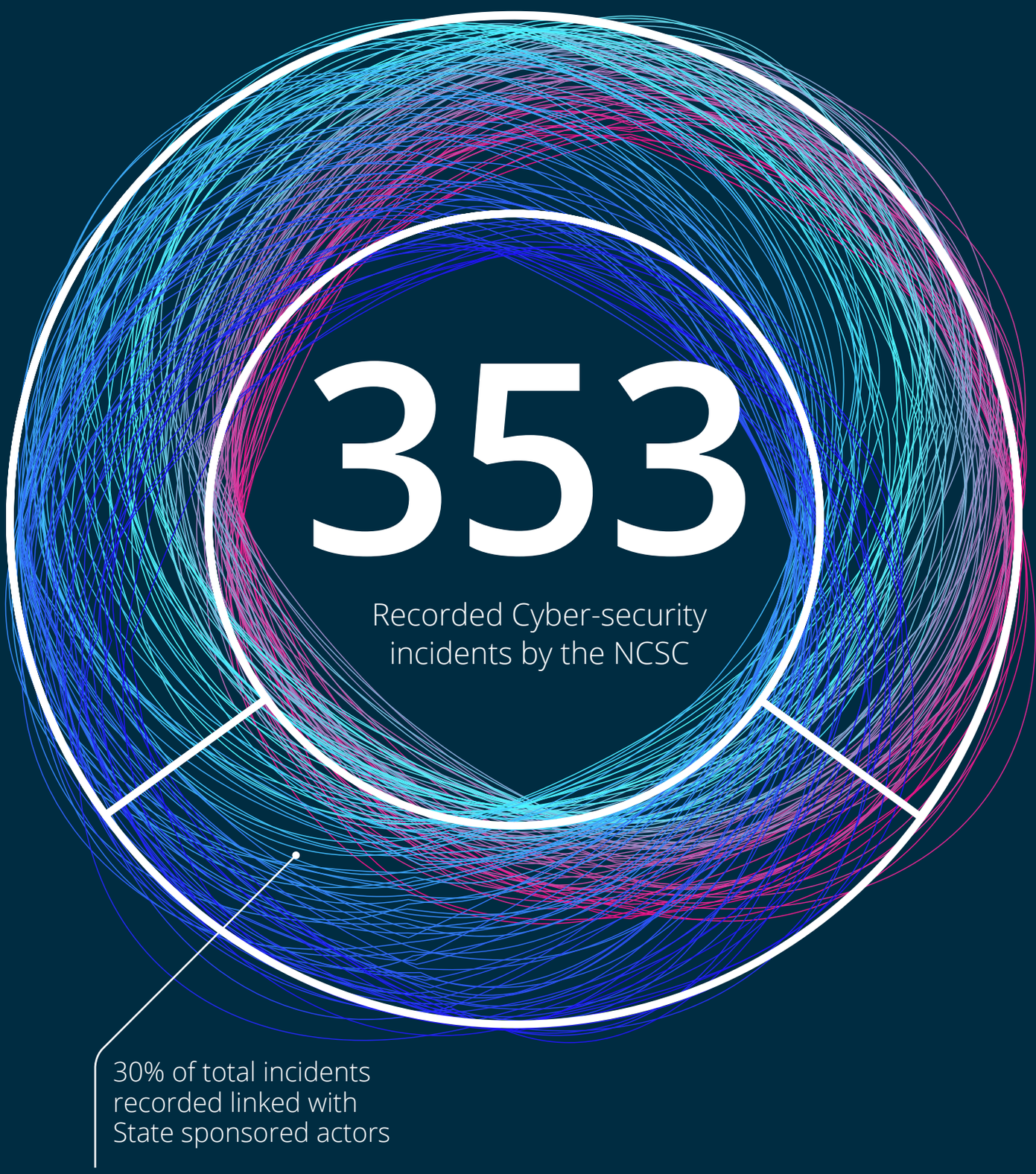
Investing in our Future

The NZIC saw the end of a four year investment programme in 2020. That programme has seen a lift in 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.

In 2019, the NZIC undertook a review of its functions, in order to identify opportunities for improvements in the effectiveness and efficiency of capabilities. Using the outcomes of this review, the NZIC identified its highest priority investments based on their alignment and expected benefit towards Government priorities, and their ability to meet the challenges facing the NZIC.

In Budget 2020, the NZIC received $146 million of new funding, over four years. Of this funding, the GCSB will receive $100 million. The GCSB received a higher proportion of this funding as it houses services shared with the NZSIS. This funding will ensure the NZIC continues to develop new capabilities and build capacity to respond to the changing strategic environment, particularly as the world recovers from COVID-19.

These initiatives follow the delivery of key capabilities funded through an additional $50 million, over four years, provided to the GCSB and NZSIS in Budget 2019. Of that funding, the GCSB received $39 million.


353
Recorded Cyber-security incidents by the NCSC
30% of total incidents recorded linked with State sponsored actors

Strategic Operating Environment

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

CYBER SECURITY

Unlike some other countries, New Zealand has not seen a significant increase in COVID-19 related cyber security incidents. We have however seen an increase in malicious COVID-related cyber activity such as phishing campaigns seeking to exploit concerns around COVID-19.

A number of cyber security incidents seen affecting New Zealand's NSOs during the 2019/20 year, particularly those linked to state-sponsored actors, have had a high impact.

The National Cyber Security Centre (NCSC) continues to see incidents where malicious cyber actors have exploited known, unpatched vulnerabilities to gain access to systems. This can be prevented through security patching, regular security testing, and taking additional steps to secure critical data.

In the international cyber security environment, the frequency of public reporting about cyber security incidents resulting in significant data breaches involving personally identifiable information has continued to increase. The range of industries impacted is indicative of the high value of personal information, targeted by both state-sponsored and criminal actors.

The NCSC recorded 353 incidents in the 12 months to 30 June 2020, compared with 339 incidents in the previous year.

These figures represent a small proportion of the total cyber security incidents impacting New Zealand, as the NCSC's focus is on potentially high impact events and those affecting organisations considered to be of national significance.

The NCSC was able to identify indicators linking state-sponsored cyber actors to 30% of total incidents recorded in 2019/20.

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.

COVID-19 has had an impact on the technological landscape, as organisations increasingly move to enable remote working. Many of the cyber security risks and challenges this presents are not new, however they have increased in size and have created new opportunities for malicious actors.

Organisations were already adopting new technologies, such as moving portions of their IT infrastructure to cloud-based platforms, however COVID-19 has accelerated the pace of change and the adoption of technologies that will enable them to be as flexible as possible. This has led to a rapid uptick in the use of tools to support staff in remote working, such as Zoom, Microsoft Teams, or unmanaged corporate devices such as laptops, which can expose organisations to security risks.

It is important that organisations continue to adhere to strong data hygiene measures, such as regular patch cycles, user account audits and security considerations, to help ensure their new technologies are not susceptible to malicious cyber actor activity.

2019/20 saw other countries report on opportunistic malicious cyber agents targeting systems and infrastructure central to the COVID-19 response. While New Zealand's critical infrastructure was not compromised by COVID-19-themed malicious activity, there was a rise in activity such as COVID-19-themed phishing campaigns, which sought to exploit concern around COVID-19 to gain access to systems.

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.

ENCRYPTION

Encryption is the process of encoding data so that it can only be read by the intended audience. Encryption is a fundamental element of good information security, which is increasingly critical to New Zealand's national security and economic prosperity. The GCSB supports New Zealand's use of encryption technology to help ensure privacy and protect sensitive communications.

Encryption can, however, be an impediment to law enforcement and intelligence and security agencies, in their efforts to access communications critical to conducting their investigations. Developments in encryption technology and increasing security challenges continue to present new and unique challenges to the GCSB's lawful intelligence collection activities.

COUNTER-TERRORISM

The threat of harm from all types of violent extremism continues to be a security issue both internationally and for New Zealand. An elevated threat environment remains in New Zealand following the unprecedented events of 15 March 2019 and the spread of violent extremist content and ideologies online remains a threat to New Zealand's safety and security.

The GCSB's primary counter-terrorism focus is to contribute to global efforts to counter all forms of violent extremism which pose a threat to New Zealand's national security and international security. The GCSB's domestic counter-terrorism role is to provide technical expertise and intelligence to assist other agencies including the NZSIS and New Zealand Police.

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 potentially 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.

REGIONAL SECURITY

The security of the South Pacific is a continuing focus area 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.

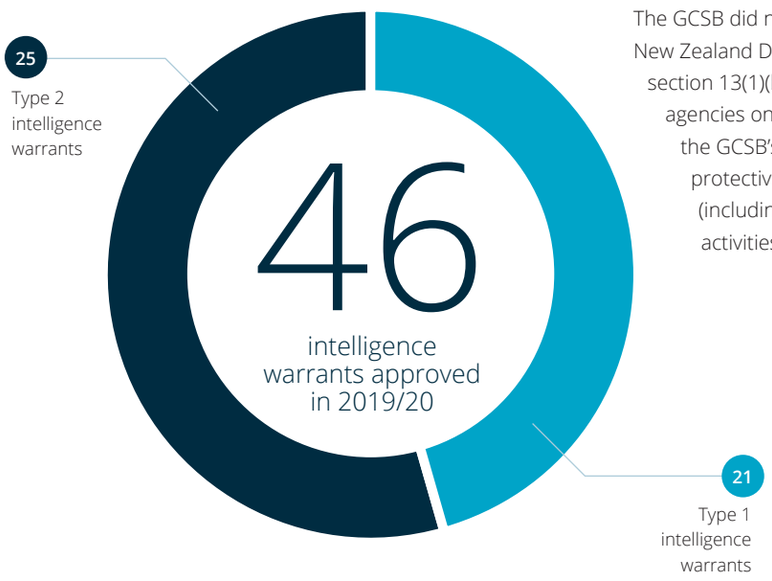
Warrants and Authorisations

INTELLIGENCE AND SECURITY ACT 2017

Under the Intelligence and Security Act 2017 (ISA), the GCSB's 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 the GCSB to contribute to the protection of national security, the international relations and wellbeing, or economic wellbeing of New Zealand;
- are necessary for the GCSB to perform its functions of intelligence collection and analysis or providing protective security services, advice, and assistance (including information assurance and cyber security activities); and
- are proportionate to the purpose for which the activities are carried out.

A total of 46 intelligence warrants were applied for and approved in 2019/20, of which 21 were Type 1 intelligence warrants and 25 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 the 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 the GCSB and NZSIS considered it necessary to seek such authority, the GCSB and NZSIS closely co-operate on operational matters.

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

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

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

A total of two business records approvals were applied for and issued. A total of eight business records directions were issued by the GCSB to agencies under section 150 (three of these related to business records directions issued in the previous financial year).

The 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, the GCSB co-operated with both agencies on a wide range of matters as part of performing the GCSB's intelligence collection and analysis and protective security services, advice, and assistance (including information assurance and cyber security activities) functions.

Impenetrable Infrastructure

Cyber Security

The GCSB protects New Zealand's nationally significant information infrastructure from malicious cyber threats. It is our mission to ensure that New Zealand's most important information infrastructures are impenetrable to technology-borne compromise.

Improving cyber security is a key component that is necessary 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.

Without fit-for-purpose 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.

THE NATIONAL CYBER SECURITY CENTRE

The GCSB's National Cyber Security Centre (NCSC) plays a vital role in protecting government agencies and 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 CORTEX initiative and provides incident response support to help nationally significant organisations (NSOs) address potentially high impact cyber events.

Who we work with

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.

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

The NCSC, New Zealand's Computer Emergency Response Team (CERT NZ), and New Zealand Police work 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.

Strategic focus refresh

As part of an ongoing strategic review, the GCSB has completed a refresh of its Information Assurance and Cyber Security strategic plan and priorities. The four year strategy to 2024 sets out new strategic purpose, vision and objectives and redefines the services we deliver and our approach to service delivery. It takes into account the changing operating environment brought about by COVID-19 and the need to support New Zealand's economic recovery, while enhancing cyber resilience and supporting digital transformation.

The strategy to 2024 defines the GCSB's purpose to "create a safer digital world for New Zealand to prosper" and establishes a strategic vision to "enable the protection, wellbeing and prosperity of New Zealand through trusted information security services". It aligns with the wider NZIC strategic outcomes that contribute to protecting the overall wellbeing and prosperity of New Zealand by creating a safer digital/technological world for New Zealand organisations to operate within.

CYBER SECURITY SERVICES

CORTEX

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

In the past year the NCSC has continued work to improve the use of CORTEX data and tools to more effectively defend New Zealand.

In the 12 months to 30 June 2020, the NCSC has adopted a continual service improvement approach to help mitigate risks associated with customers' evolving use of technology.

Work to improve CORTEX capabilities has included the creation and refinement of analytic processes to identify vulnerabilities being exploited by foreign threat actors to compromise networks.

MALWARE-FREE NETWORKS

The Malware Free Networks (MFN) capability is a malware detection and disruption service that enables the GCSB to significantly scale our cyber defence effort across a broad range of New Zealand organisations.

MFN will partner with network operators to detect and disrupt threats to NSOs. It will deliver an active disruption capability that is scalable, through the provision of a threat intelligence feed that can be consumed by organisations either directly, via a managed service provider, or through their Internet Service Provider.

During 2019/20, the NCSC continued to develop the MFN product. This included engineering work such as solution design and implementation, and the development of operating procedures and standards.

NCSC also worked towards the Certification and Accreditation of MFN and supporting systems.

NCSC staff have also engaged with NSOs to generate interest in the MFN product either as a direct customer or through network operators.

Analysis under taken by the GCSB shows that in 2019/20 the detection and disruption of malicious cyber activity, by CORTEX capabilities, has prevented

$70.5 million

worth of harm to New Zealand's nationally significant organisations.

This means that, since June 2016, CORTEX capabilities have reduced harm from hostile cyber activity by around $165.2 million.

Cyber Resilience

Customer engagements

The NCSC's Cyber Resilience Unit (CRU) works closely with more than 250 NSOs to understand their cyber resilience and vulnerability to attack, providing advice, support and cyber threat alerts to help organisations lift their overall cyber security resilience.

During the reporting period, the CRU recorded 1,770 engagements with customers across the broad spectrum of public and private sector organisations, geographically disbursed across all regions.

CRU also facilitates security information exchanges (SIEs) where participants can share information in a confidential and trusted environment. The GCSB currently supports the operation of sector-based security information exchanges covering the energy, finance, government, network, transport and logistics, and university sectors. The SIEs generally take place quarterly to share information on cyber security risk management and resilience building. SIEs are organised on a sector-by-sector basis, and membership is restricted to NSOs.

In the current reporting period, the CRU facilitated 20 SIEs, which enhanced collaboration on cyber security challenges and opportunities across all sectors.

The CRU also published 24 reports for general customers identifying specific cyber security vulnerabilities, providing cyber threat mitigation advice and reinforcing cyber security best practice to raise overall cyber security resilience.

Guidance material

In 2017/18, the NCSC gathered data from 250 NSOs and produced the NCSC Cyber Security Resilience Assessment, which identified four areas of good practice where organisations can focus their efforts for the greatest effect. The identified key areas were governance, incident management, investment and supply chain.

In 2019/20, the first of a series of resources to help organisations address these focus areas was published. The NCSC's "Charting your Course" guidance provides practical advice to assist organisations enhance their cyber security governance. The steps outlined in "Charting your Course" define the principles of a cyber security programme and help to focus engagement between senior leadership and security practitioners.

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 infrastructure. It also protects the Government's most sensitive information.

GOVERNMENT CHIEF INFORMATION SECURITY OFFICER

Through the Director-General's role as Government Chief Information Security Officer (GCISO), the GCSB takes a strategic approach to identifying security risk and working across agencies to help enable effective responses. This includes identifying technical responses and making sure we have effective policy settings across government.

The GCISO continues to support ongoing work led by the Government Chief Digital Officer around system settings and leadership needed to improve how the public service operates in the digital environment.

The value of the GCISO role was reinforced when the GCSB assisted the government's rapid shift to working remotely, at the onset of COVID-19 Alert Level 4. Advice was required to support agencies adopting alternative communications technologies during lockdown. The GCISO and NCSC produced advice to government agencies on recommended mitigations to securely use Zoom to conduct government business up to and including RESTRICTED information. This enabled agencies to conduct remote meetings over lockdown, with increased understanding of the security risks and how to mitigate them.

INFORMATION SECURITY POLICY AND RESEARCH UNIT

In 2018/19, the GCSB established the Information Security Policy and Research Unit. This unit supports the GCISO. The unit produces information security guidance and policy for government agencies as part of government Protective Security Requirements.

In 2019/20, the unit has taken an increasingly strategic focus, working closely with other core government agencies to develop and circulate new security guidance. A key feature of this was the development of numerous pieces of guidance to support agencies' efforts to maintain a high level of information security resilience and awareness during the initial stages of the national response to the COVID-19 pandemic. Guidance included advice regarding remote working, securing cloud services, and securing video conferencing platforms.

The unit also supported the multi-agency response to the August 2019 data breach experienced by the Ministry for Culture and Heritage. A joint Cabinet paper on lifting ICT capability across Government was completed and provided to Ministers.

The Policy and Research Unit continues to work closely with the All-of-Government Cloud Programme, producing New Zealand Government Cloud Blueprints to be used by cloud vendors to support the migration of Government ICT environments to cloud platforms.

Ongoing work by GCSB continues in support of information security across the system as a whole. This included release of significant updates to the New Zealand Information Security Manual (version 3.3).

HIGH ASSURANCE SERVICES

The GCSB High Assurance Services unit (HAS) helps ensure the Government's most sensitive communications are not intercepted or compromised.

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 on the accreditation of sensitive compartmented information (SCI) sites and systems. The Director-General 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 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.

REGULATORY FUNCTIONS

The GCSB has assumed a number of regulatory functions relating to the identification and mitigation of national security risks.

Telecommunications (Interception Capability and Security) Act 2013

New Zealand's telecommunications networks are a core part of New Zealand's critical national infrastructure, and are integral to the daily lives and wellbeing of New Zealanders, as well as being a major economic driver. New Zealand networks are undergoing a number of changes, many of which are being accelerated in light of new demand for remote working and the growth in the Internet-of-Things devices. Changes include transition to 5G services (to support greater usage of mobile services by users and connected devices), the transition to cloud-based network management tools and services, and new flexible network architectures such as network virtualisation, and increasing the roll-out and capacity of fibre services.

The Telecommunications (Interception Capability and Security) Act 2013 (TICSA) provides a regulatory framework to prevent, mitigate, or remove security risks arising from the design, build, and operation of public telecommunications networks, or from the interconnection of public telecommunications networks to networks in New Zealand or overseas.

Under Part 3 of TICSA, the GCSB assesses proposed network changes for security risks. Such assessments are made on a case-by-case basis, and independent of any outside influence. All notifications received for assessment are held on a commercial-in-confidence basis.

In the 2019/20 reporting period, the GCSB received 145 notifications, comparable to the 158 notifications in 2018/19. Many of these involved changes related to the roll-out of 5G or full-fibre networks.

Outer Space and High-Altitude Activities Act 2017

New Zealand provides a uniquely beneficial environment for space-related activities. Our uncluttered air space, and the open expanse of unpopulated ocean along typical launch trajectories, gives us long and safe launch windows

for high-altitude vehicle flights and space launch activity. New Zealand's growing space industry provides significant economic opportunities for New Zealand.

The Outer Space and High-altitude Activities Act 2017 (OSHAA) provides a regulatory framework for managing any risks to New Zealand's national security from outer space and high-altitude activities originating in New Zealand.

The Space Activities Risk Assessment Group (SARAG), consisting of members of the GCSB and NZSIS (with advisors from other parts of the NZIC, including NZDF) jointly assess space activities regulated under OSHAA for any national security risks. Those assessments inform advice to the Minister Responsible for the GCSB (and Minister Responsible for NZSIS), who must be consulted by the Minister responsible for OSHAA (the Minister for Economic Trade and Development).

During the 2019/20 reporting period, the GCSB conducted 31 assessments of regulated space activities, up from 29 in the last reporting period.

Overseas Investment (Urgent Measures) Amendment Act 2020

The Overseas Investment (Urgent Measures) Amendment Act 2020, which came into force on 16 June 2020, made changes to the Overseas Investment Act 2005.

The amended Overseas Investment Act includes a national interest test and a new emergency notification regime to manage risks associated with overseas investments that are contrary to New Zealand's national interest (including national security). The emergency notification regime is a temporary measure to address risks associated with overseas investment while the New Zealand economy is affected by and recovering from COVID-19.

The Overseas Investment Office (the regulator) provides advice to the responsible Minister regarding transactions. The GCSB supports NZSIS in providing advice to the regulator regarding any national security risks associated with proposed overseas investments.

As the amendment only came into force on 16 June 2020, there were no transactions forwarded for national security risk assessment within the 2019/20 reporting period.

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.

The GCSB has several significant projects underway in this area, including:

- The Cryptographic Products Management Infrastructure project; and
- The New Zealand Top Secret Network.

HIGH-GRADE CRYPTOGRAPHIC INFRASTRUCTURE

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

Due to the complexity and security involved, CPMI has been a multi-year project. Work on this project has progressed in 2019/20, although COVID-19 has resulted in a delay in completion of the project.

Indispensable Intelligence

Intelligence Collection

The GCSB is the New Zealand Government's signals intelligence agency. It uses 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 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.

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 DPMC, 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 2017 (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 after they are issued.

Throughout 2019/20 the GCSB continued to supply intelligence to 22 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.

In the 2019/20 period, the GCSB has provided a significant amount of intelligence to New Zealand Government customers in relation to the COVID-19 pandemic. The GCSB continued to provide this intelligence, and intelligence on other matters related to national security, during the COVID-19 lockdown in addition to maintaining its 24/7 watch and warn service.

Counter-terrorism

The GCSB's primary focus in counter-terrorism is external, including contributing to global efforts to counter violent extremism in its various forms.

The GCSB contributes to global efforts to counter all forms of violent extremism that pose a threat to New Zealand's national security and international security. The GCSB also plays a role in domestic counter-terrorism through assisting agencies such as the NZISIS and New Zealand Police in their investigations. This assistance is primarily the provision of technical capabilities and intelligence.

Since the implementation of the ISA, the GCSB has taken a series of deliberate steps to enable it to respond effectively to requests for assistance on domestic counter-terrorism, within 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 ISA. As a result, GCSB teams can be deployed across a range of intelligence priorities and agency requirements.

In response to the 15 March terrorist attacks, the GCSB provided support to the NZSIS and New Zealand Police investigations into the alleged perpetrator, politically and ideologically motivated violent extremism in New Zealand, and the risk of any copycat or retaliatory attacks.

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 interests in the South Pacific. This work focuses on providing support to other government agencies whose responsibilities include responding to security issues in our region.

Working with Government Agencies

Contributing to the protection of New Zealand's national security and wellbeing and supporting the safety and security of New Zealanders at home and abroad, are key objectives of the GCSB. One way of achieving these objectives is by supporting other government agencies through provision of relevant intelligence, so they can carry out their work.

WORKING WITH POLICE

The GCSB responds to requests for intelligence from, and provides technical assistance to, the NZSIS and New Zealand Police on request. Further, the GCSB has contributed to development of the Police-led Transnational Organised Crime Strategy.

WORKING WITH NEW ZEALAND CUSTOMS SERVICE

The GCSB has worked closely with Customs throughout 2019/20 to contribute to the prevention and detection of transnational organised crime. Our focus is on providing intelligence leads that will assist Customs to prevent large scale drug importation.

Using GCSB signals intelligence capabilities, we are supporting Customs to better target drug networks with the aim of disrupting their efforts before they reach our shores. Our collection and analysis activity has helped to enhance Customs' understanding of drug networks that seek to smuggle drugs to New Zealand.

SUPPORTING NEW ZEALAND DEFENCE FORCE

In 2019/20 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.

Customer Engagement

The GCSB continues to work with NZSIS and DPMC to better understand our customers and to improve intelligence services to meet their needs.

In 2019/20, the GCSB has continued a joint programme of work with NZSIS and DPMC to improve our approach to provision of intelligence and assessments to support our customers. Following detailed planning and consultation across the three agencies, NZIC leaders agreed in November 2019 to establish a joint business unit that will deliver intelligence products and services on behalf of the three agencies. Implementation of the joint customer services team will be phased over four years commencing in the 2020/21 financial year.

The decision to take a joint approach with NZSIS and DPMC recognised that through collaboration, the agencies would be able to eliminate duplication of effort in service delivery and be able to provide more specialised engagement with customers. The joint team will know our customers and what matters to them, sharing a common understanding of their business needs and how to best provide high impact, tailored intelligence that will shape their decision-making.

In December 2019, the Customer Engagement programme team commenced recruitment and planning for phase one. This phase was designed to establish an initial capability while ensuring continued delivery of vital intelligence during the change process.

International Partnerships

The GCSB's engagement with international partners aligns with New Zealand's national security priorities, including the National Strategic Intelligence Priorities (NSIPs), and operates within the context of New Zealand's independent foreign policy.

Any cooperation and intelligence sharing with international partners is subject to New Zealand's laws, including human rights obligations.

FIVE EYES

New Zealand, along with Australia, Canada, the United Kingdom and the United States of America, makes 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.

This partnership is fundamental to the 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 an instrumental part of New Zealand's intelligence and security activities since World War Two. The partnership began as 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.

OTHER INTERNATIONAL PARTNERS

In addition to our Five Eyes partnership, the GCSB collaborates with a range of other nations. 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.

COVID-19 IMPACT ON INTERNATIONAL PARTNERSHIPS

Travel restrictions and local lockdowns around the world due to COVID-19 have resulted in the cancellation of international conferences and bilateral engagements that GCSB would normally attend or host. Many of these engagements have been able to proceed via secure video conferencing facilities, allowing us to maintain our international partnerships.

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 GCSB in April 2016 and has been reappointed to 2024.

Beyond the specific responsibilities set out in the Intelligence and Security Act 2017 (ISA), the Director-General has the following 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

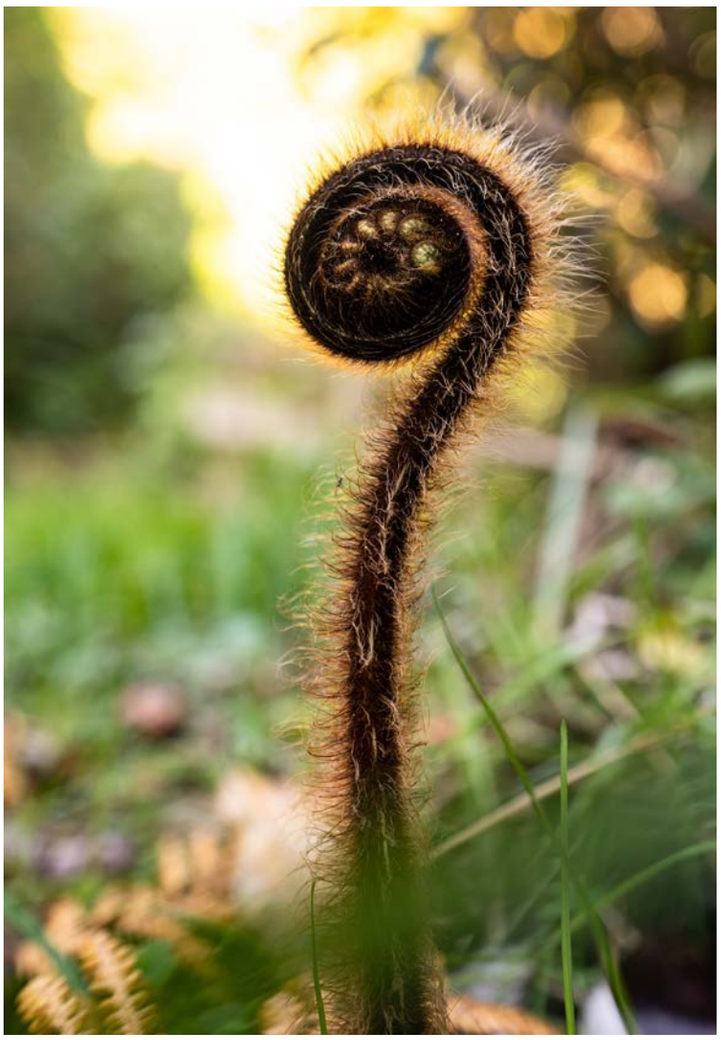
The Director-General is supported by an internal Senior Leadership Team (SLT).

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 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 Public Service 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. However in order to ensure all managers receive this training in a timely manner a new online module has been created and rolled out for all remaining and future managers to complete. Managers and staff have also had the opportunity to attend courses on neuro-diversity, Crown and Māori Relations and Te Reo. Following the successful launch of the LGBT+ network sessions will be available to all managers and staff from July 2020.

Work to develop a new Leadership Development programme, Te Ara o Tātāriki – The Path of Kākā/Leadership, began in February 2020. This programme is aimed at tiers 4 and 5 and is designed to shape leaders who can act on the demands of an evolving environment, who are strategic, innovative, agile, adaptable and authentic. The programme will cover leadership, strategic execution, leading change and resilience, teamwork and collaboration, decision making in complexity and ambiguity. The first two cohorts are set to begin at the end of July 2020.

Retain, Develop and Recruit the Best People

The GCSB is a Public Service Department with 488.23 full-time equivalent staff, as at 30 June 2020.

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 2019/20 the GCSB has focussed on retaining the existing workforce and providing opportunities for growth and development.

Recruiting the best people has continued to be a priority for the GCSB throughout 2019/20. The GCSB employs people from a wide range of disciplines, including foreign language experts, communications and cryptography specialists, engineers, technicians, and support staff. Over the past year efforts have been focussed on ensuring that recruitment resources reflect that we want a more diverse workforce.

In 2019, an external research firm conducted research into the perceptions of the GCSB held by Māori, Pacific Island, Muslim, Asian and female audiences in New Zealand. The purpose of this was to gain a deeper understanding of what matters to these audiences, in order to drive recruitment and retention initiatives. This research showed that if we want to attract and retain ethnically diverse staff, we need to have a culture that is collaborative, respectful and focussed on helping others. A sense of "giving back" in relation to protecting New Zealand is strongly routed in duties associated with Kaitiakitanga, whanau and cultural identity. Aligning our employer proposition to this, and implementing the recommendations from this research will be a focus area over the next 12 months.

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 people.

In the past the GCSB has benefited from relatively low rates of staff turnover. In 2019/20 the turnover rate has increased by 1.7%, which is slightly higher than the public sector average from 2018/19. A contributing factor for this is that we operate in an increasingly competitive environment where the skills we use (particularly in technology and cyber security) are highly sought after in the wider public sector and 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 development and progression. This has also been highlighted as a priority within the new Learning and Development (L&D) Strategy.

To improve retention, over the past couple of years we have worked with our staff, staff associations, and network groups to gain a more comprehensive understanding of the key reasons people leave. This information has informed a joint Retention Strategy with the NZSIS that is due for release in August 2020. The strategy sets out the actions the agencies will focus on at an organisation-wide level in the next four years to improve staff retention. Directorates within the agency will also support our retention strategy through the development of their own retention initiatives focussed on addressing any retention issues specific to their Directorate.

Table 1: GCSB core unplanned staff turnover (2015 to 2020)

	2015/16	2016/17	2017/18	2018/19	2019/20
Staff Turnover	9.3%	6.9%	7.1%	12.0%	13.7%
Public Service	11.1%	11.5%	12.1%	11.8%	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. This commitment has now been captured in a new L&D Strategy which was launched at the end of June 2020.

The L&D Strategy aims to "enable a workforce with beyond ordinary capabilities, engagement and adaptability to deliver on the mission of the NZIC", and will do so through the comprehensive four year action plan. The action plan focuses on six key principles:

- Developing a relevant learning programme;
- Ensuring consistent learning and outcomes;
- Fostering workforce inclusion;
- Enabling all learning styles;
- Growing trusted leaders; and
- Creating informed agencies.

Throughout 2019/20 we have increased the number of face-to-face internal and external professional development courses. Unfortunately due to COVID-19, some of this training was disrupted.

During New Zealand's COVID-19 Alert Level 4, the GCSB implemented a number of additional health and safety protocols to help keep our staff safe while operating as an essential service, including reducing the number of staff present in the office at any one time. The L&D team quickly set about providing support to enable staff to learn from home. This involved creating and collating new unclassified content for staff and adapting face-to-face training into online sessions with external providers.

Proving that online virtual conference sessions can work for our staff and some of the content we provide, has unlocked a new norm and provided our L&D team, providers and staff with new possibilities for learning within the NZIC. Consideration is being given to how this could work for L&D programmes going forward, taking all staff feedback into consideration.

CAREER PATHWAYS

The Career Pathways and Career Board system was introduced within the GCSB and NZSIS 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.

In 2018, the GCSB reviewed the Career Board system to ensure it is still meeting the agency's needs, with a number of changes implemented in 2019. Significant work was undertaken to provide staff and managers with an iterative, electronic solution to complete their applications. This resulted in customisation of iLearn (our in-house learning management system) to enable staff to complete their applications online. Between 1 July 2019 and 30 June 2020, the GCSB had 26 staff progressing to a higher level of technical competence through the Career Boards. Due to COVID-19, this does not include applicants who were invited to the May 2020 board, which was postponed to July 2020.

WORKFORCE PLANNING

The NZIC continues to identify current and future workforce requirements. This programme of work 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. Throughout 2019/20, 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 graduate programme is designed to ensure graduates get a wide range of experiences within the GCSB before they are appointed to a permanent role. The focus for the graduate programme is now technical graduates as that is where the need is for the future of the GCSB.

For the 2019/20 graduate recruitment intake of technical graduates, the GCSB received a total of 71 applications, of which 22 (31%) were female. Of the successful applicants, 43% were female. The low numbers of female science, technology, engineering and mathematics (STEM) students continues to be of concern, which is why GCSB sponsors and participates in events aimed at women who study STEM subjects.

The GCSB has retained 91% of staff who have come though the graduate programme since the first intake in 2016.

SUPPORTING WOMEN IN STEM

The GCSB undertook a 'Women in STEM' (science, technology, engineering and mathematics) scholarship programme for a third year in 2019/20. 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.

In 2019/20 we received a total of 72 applications for the scholarship. Applications came from all of our universities, with the highest number from University of Auckland (21). Massey University (10) was closely followed by University of Canterbury (9), University of Otago (8), and University of Waikato (8) and Victoria University of Wellington (6). Ten applications were from polytechnics throughout New Zealand.

The calibre of applicants was extraordinary, resulting in four scholarships being awarded. Two of our winners identify as New Zealand European, one identifies as New Zealand European and Pasifika, and the other identifies as New Zealand European and Māori.

Two of the 2019/20 scholarship winners and a further top applicant from a previous year have applied for the 2019/20 graduate programme and have successfully made it to the last stage of the recruitment process.

Moving forward we will provide a clearer pathway for our top Women in STEM Scholarship applicants to enter our graduate programme.

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 (D&I) Strategy for the GCSB and the NZSIS 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. Our initial focus areas have related to increasing the number of women and ethnically diverse people across all levels of our workforce. These will continue to be priority areas for us. As part of our D&I Strategy refresh in 2020/21 we will also have an increased focus on wellbeing, flexibility and making our organisation a supportive environment for people with disabilities.

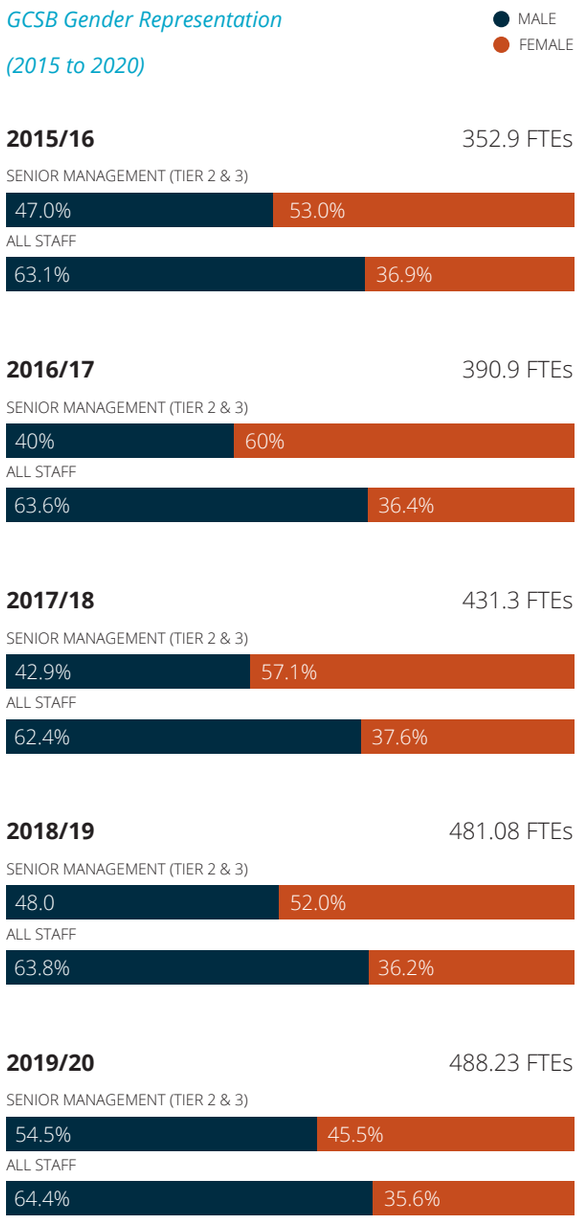
The GCSB aims to be recognised as an inclusive, diverse and progressive organisation which maximises capability through its workforce. Further to this we want to embrace, promote and encourage diversity in our workforce and our thinking.

GENDER DIVERSITY

At 30 June 2020, women made up just under half of the GCSB's senior management group. This has dropped below our diversity and inclusion aspiration of not less than 50%, due to temporary parental leave absence.

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 all layers of the organisation. Initiatives such as the scholarship supporting women in STEM subjects, and the introduction of a Poutamatia (a women's self-development programme – referred to overleaf) are a part of our efforts to improve this representation.

GCSB Gender Representation (2015 to 2020)



CLOSING THE GENDER PAY GAP

Closing the gender pay gap has been a focus for the GCSB with a target of reducing the average gap to a maximum of 5% by 2021. At the end of the 2019/20 financial year, the gender pay gap in the GCSB was 4.9%. This is a decrease of 0.5% from 5.4% in 2018/19, and puts us ahead of our goal to have a gender pay gap of no higher than 5% by 2021.

The gender pay gap is calculated as a comparison of the average salary of all males and all females within the GCSB, and is not indicative of a pay gap within the same or similar positions ('like-for-like'). The GCSB has addressed its like-for-like gender pay gap through successive remuneration rounds. This means men and women who have been in the same roles for the same amount of time and who are performing at the same level are paid equally. We will continue to monitor the like-for-like gender pay gap to ensure staff remuneration remains equitable.

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 Public Service Commission seeking to resolve the gender pay gap across the public service.

ETHNIC DIVERSITY

The GCSB is working to improve the ethnic representation of its workforce, and has achieved modest improvement in some areas. In 2019/20 the GCSB continued to implement the Diversity and Inclusion strategy. The strategy ensures we have diverse talents, views and thinking, which are 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

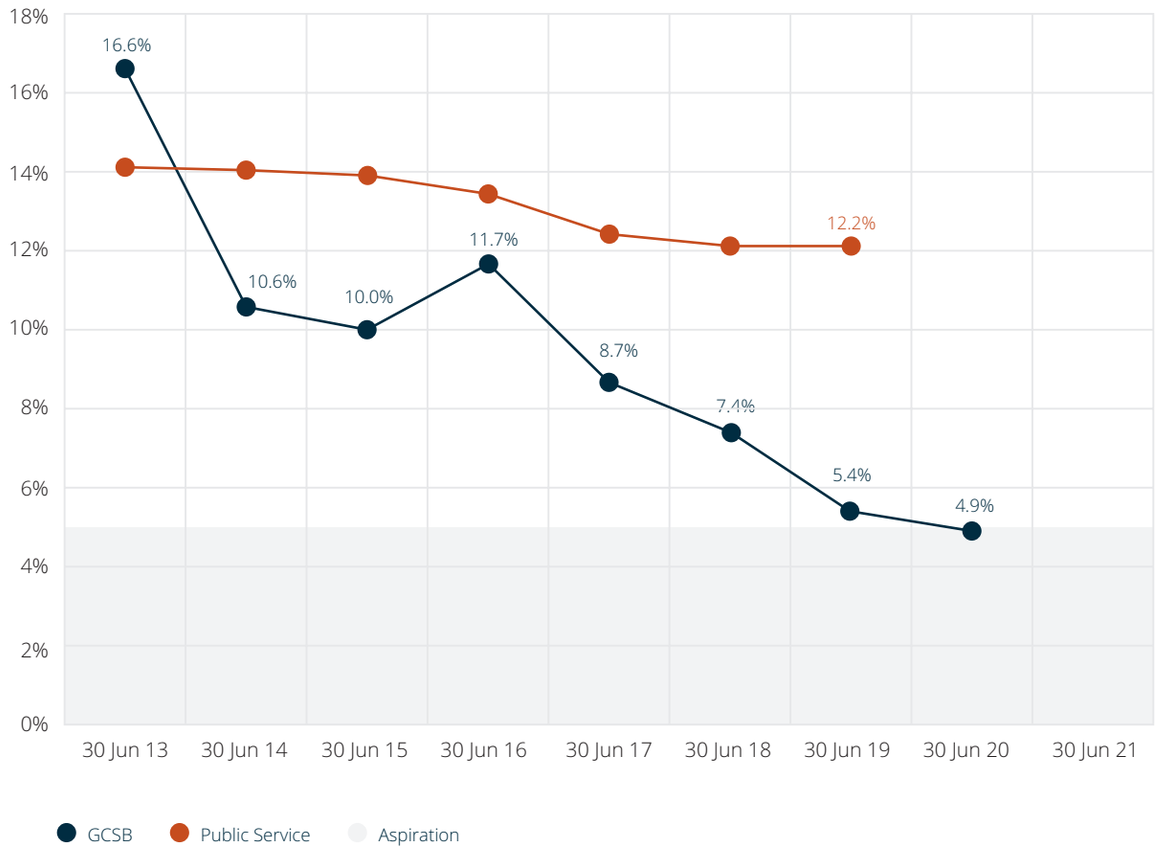


Table 2: GCSB Staff Ethnicity (2015 to 2020)

	2015/16	2016/17	2017/18	2018/19	2019/20
New Zealand European & European	69%	68.7%	67.6%	67.8%	71.2%
New Zealander	N/A	N/A	27.5%	29.4%	26.8%
New Zealand Māori	6.5%	7.2%	7.8%	7.2%	7.3%
Asian	5.8%	5.4%	4.9%	5.4%	5.5%
Pacific Peoples	1.6%	1.8%	2.8%	2.3%	1.6%
Middle Eastern, Latin American, and African (MELAA)	0.3%	0.3%	0.3%	0.9%	1.1%

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.

WOMEN'S SELF-DEVELOPMENT PROGRAMME

In August 2019, the NZIC implemented a new women's development programme, Poutamatia – Reach for the highest. The Poutamatia programme was developed to support women with their personal and professional career development and self-confidence. The programme is now preparing for its third cohort and the feedback from the first two cohorts has been extremely positive with many of the attendees showing a notable improvement in their confidence both at work and personally.

SUPPORTING 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 a number of internal networks, including the Women of the New Zealand Intelligence Community (WNZIC) network, Standing Out (our LGBTQI+ network), Parents Group, Kahikatea (our ethnicity network), and our Health and Wellbeing network.

These networks meet bi-monthly with both Directors-General to discuss strategic initiatives. They are actively involved in organising events, providing speakers and supporting staff. We have celebrated and acknowledged a number of special days and events, including International Women's Day, Māori Language Week, and Mental Health Awareness Week.

ENGAGEMENT WITH OUR PEOPLE

We place a strong emphasis on engaging with staff to understand what matters most to them. We do this through a range of channels – employee surveys, staff network groups, internal research and workshops.

Over the last 18 months we have conducted research into those who have taken parental leave and the experiences of women in the NZIC. The parental leave research resulted in key enhancements to our Parental Leave and Childcare Policies which came into effect in February 2020.

Research into the experiences of women has provided useful insights into how we can further improve to be a more inclusive workforce. We have held workshops with staff to co-create solutions and will be implementing actions over the next 12 months.

Through seeking suggestions from staff we have re-named a number of meeting rooms across all locations to ensure the names reflect who we are as an intelligence community, our commitment to diversity and inclusion, and showcase the rich culture of New Zealand.

By engaging with our staff and understanding their lived experiences we are able to co-create improvements that contribute to a better workplace culture and help ensure that we focus our attention on improving the things that matter most.

RAINBOW INCLUSION

Following our Rainbow Tick Accreditation in July 2019, we have continued to implement initiatives to ensure rainbow inclusion in the workplace. We have developed Transitioning Guidelines, which provide helpful information and practical advice for managers and staff who are in transition (or considering it). We have also developed and delivered our own rainbow-inclusion training, specifically for vetting staff. Our entire senior leadership team has also attended rainbow-inclusion training and education, and this training is now available to all staff.

RAINBOW TICK CERTIFIED
www.rainbowtick.co.nz

MENTAL HEALTH AND WELLBEING

We take the mental health and wellbeing of our staff very seriously. We have an in-house Psychological service and also 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.

During COVID-19, we developed a specific Wellbeing Plan for all staff. This plan focussed on five dimensions of wellbeing including physical, mental, career, social and financial wellbeing, where staff had access to advisory support, training and a range of wellbeing resources.

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.

Legal Compliance and Oversight

The Intelligence and Security Act 2017

The Intelligence and Security Act 2017 (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 provide guidance for the agencies on how certain lawful activities should be conducted.

COMPLIANCE SYSTEMS

An essential component of retaining the trust and confidence of the Government and the public is having robust internal processes in place to ensure the GCSB complies with New Zealand law and our international human rights obligations at all times. The GCSB has a responsibility to ensure that we use our intrusive powers and access to sensitive information in a manner that is legal, justifiable and proportionate.

To ensure this, the GCSB has a compliance framework in place and audits operational activities. This provides assurance that staff are compliant with New Zealand law and that our compliance training and operational policies are fit-for-purpose. Our policies are also reviewed in response to any relevant findings set out by Inquiries or the recommendations of any of our independent oversight bodies.

Independent Oversight

Aside from our own internal processes, the GCSB is subject to the oversight of several external bodies.

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.

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 INTELLIGENCE AND SECURITY COMMITTEE

The Intelligence and Security Committee (ISC) is the Parliamentary oversight committee for 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.

OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

The Inspector-General of Intelligence and Security (IGIS) provides independent external oversight and review of the GCSB and NZSIS. The IGIS provides assurance to the New Zealand public that the activities of the GCSB are lawful and proper, which includes identifying any areas of concern.

The IGIS also provides an avenue for public complaints about the agencies' conduct. The GCSB regularly engages with the Office of the IGIS to discuss issues and provide information and resources to support IGIS investigations and queries.

Independent Inquiries

In 2019/20, the GCSB participated in a number of major inquiries.

GOVERNMENT INQUIRY INTO OPERATION BURNHAM AND RELATED MATTERS

The GCSB worked closely with other Crown agencies to participate in the now-completed Government Inquiry into Operation Burnham and related matters. In addition to its substantive participation in the Inquiry, the GCSB supported the Inquiry's arrangements for the secure handling of classified material.

IGIS INQUIRY INTO THE ROLE OF THE GCSB AND NZSIS IN RELATION TO CERTAIN EVENTS IN AFGHANISTAN

The GCSB put significant time and effort into its engagement with this Inquiry. The IGIS's report, which was published in 2020, acknowledged that the GCSB and NZSIS provided valuable assistance to support the New Zealand Government's role in Afghanistan, including playing a key role in protecting New Zealand personnel stationed there.

The report notes that the GCSB appropriately shared information across the New Zealand Government with regard to the aftermath of Operation Burnham, including on likely civilian casualties, and also the allegation that an insurgent captured by New Zealand forced and subsequently held by the Afghanistan authorities was tortured. However, the IGIS also considered that the GCSB could have taken a broader role.

The IGIS's report makes recommendations around anticipating and managing human rights risks, and sharing intelligence with international parties. The GCSB has already made significant policy and process changes since the events examined in this report. The legal framework for co-operation between the New Zealand intelligence agencies and international partners has been updated as a result of the ISA coming into force.

ROYAL COMMISSION OF INQUIRY INTO THE ATTACK ON THE CHRISTCHURCH MOSQUES

The GCSB has continued to provide information to the Royal Commission of Inquiry into the Attack on Christchurch Mosques.

THE JUSTICE SELECT COMMITTEE INQUIRY INTO 2017 GENERAL ELECTION AND 2016 LOCAL ELECTIONS

In August 2019, the Directors-General of the 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 committee to answer questions pertaining to decision-making about security investigations into New Zealand citizens, and mechanisms to address foreign interference risks.

The GCSB continues 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 2019 to 30 June 2020, the GCSB:

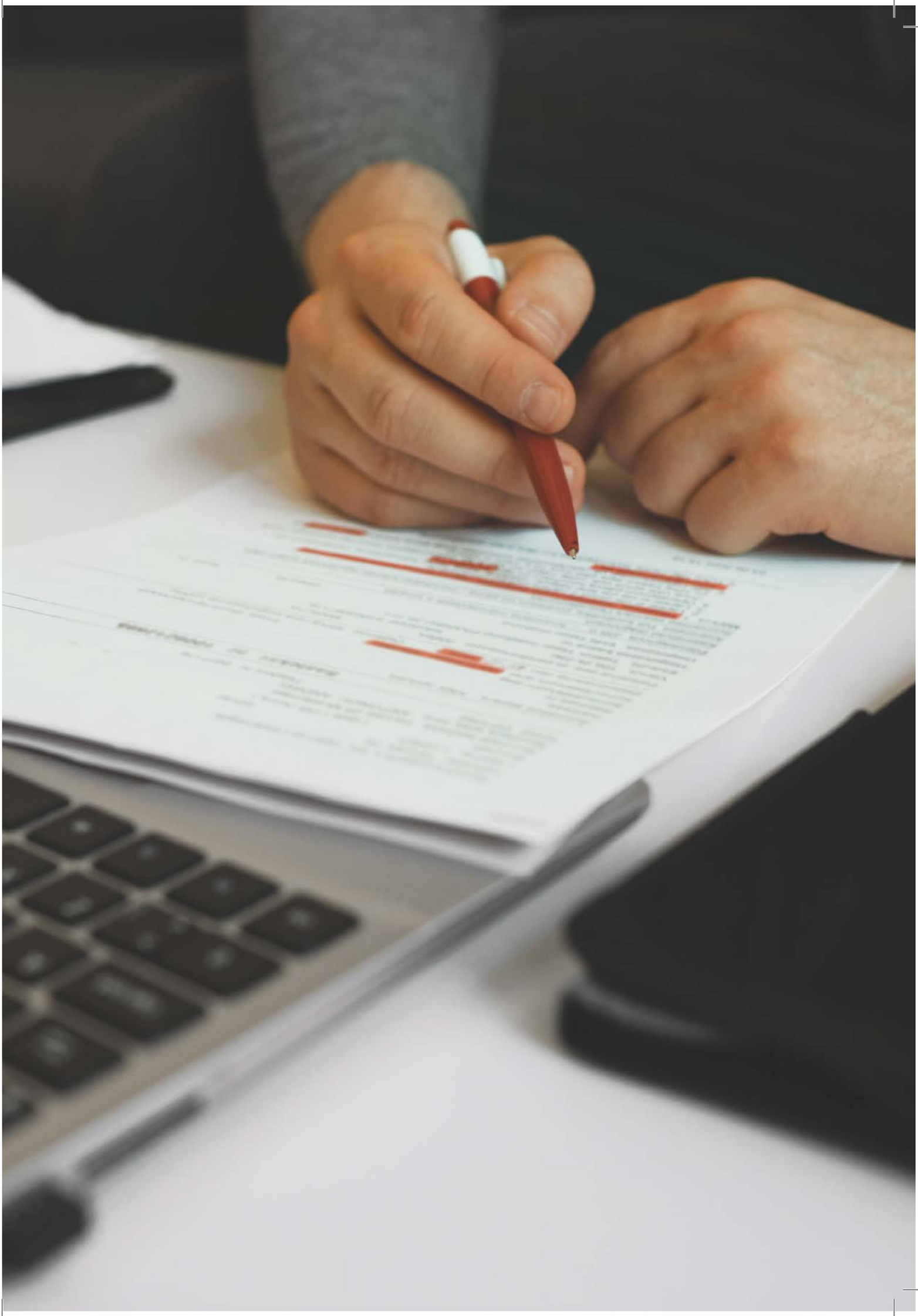
- Completed 51 OIA requests, with five requests not completed within the legislated timeframe; and
- Completed 28 Privacy Act requests within the legislated timeframe.

The GCSB aims to complete all information requests within the legislated timeframe. It is important to note that the necessary health and safety restrictions in place due to the COVID-19 pandemic did cause some OIA response time delays. Prior to New Zealand entering Alert Level 4, the GCSB was on track to have 100% of its requests completed within the legislated timeframe.

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

No complaints were raised with the Office of the Ombudsman during the 1 July 2019 – 30 June 2020 period.

Three complaints were raised with the Office of the Privacy Commissioner during the period. In all cases the GSCB worked with the Office of the Privacy Commissioner to achieve a resolution, and no final decisions were made against the agency.



Financial Statements

Independent Auditor's Report

To the readers of the Government Communications Security Bureau's statement of expenses and capital expenditure against appropriation for the year ended 30 June 2020

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 expenses and capital expenditure against appropriation of the GCSB for the year ended 30 June 2020 on page 55.

Opinion

In our opinion the statement of 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 November 2020. This is the date at which our opinion is expressed.

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

Basis for our opinion

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

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

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our 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 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, Supplementary Estimates and Addition to the Supplementary Estimates of Appropriations 2019/20 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 on pages 3 to 48 and 54, but does not include the information we audited, and our auditor's report thereon.

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. 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 report that fact. We have nothing to report in this regard.

Independence

We are independent of the GCSB in accordance with the independence requirements of the Auditor General's Auditing Standards, which incorporate the independence requirements of Professional and Ethical Standard 1: International 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

AUDIT NEW ZEALAND
Mana Arotake Aotearoa

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 2020 and its operations for the year ended on that date.

Andrew Hampton
Te Tumu Whakarae mō Te Tira Tiaki
Director-General, Government Communications Security Bureau

30 November 2020

Statement of Expenses and Capital Expenditure against Appropriation

For the year ended 30 June 2020

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

	$000
Total appropriation	$178,702
Actual expenditure	$134,286

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.

GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

New Zealand Government