G.56 (2022)

Te Tira Tiaki
Government Communications
Security Bureau

TE PŪRONGO Ā-TAU 2022
ANNUAL REPORT 2022

Protecting and Enhancing New Zealand's Security and Wellbeing.

Te tiaki me te whakapiki i te haumarutanga me te oranga o Aotearoa.

Preface

This is the annual report of the Government Communications Security Bureau (GCSB) for the year ended 30 June 2022, 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.

CONTENTS

01

OVERVIEW OF THE YEAR
TE TIRO WHĀNUI KI TE TAU

DIRECTOR-GENERAL'S OVERVIEW
TE TIRO WHĀNUI A TE TUMUAKI AHUREI

Throughout the 2021/22 year the Government Communications Security Bureau's (GCSB) cybersecurity and signals intelligence missions have responded to significant and at times unprecedented challenges from the increasingly contested world that we live in.

It has been a year punctuated by Russia's illegal and unprovoked invasion of Ukraine, the ongoing escalation of global geostrategic competition, including within our Pacific region, and serious malicious cyber incidents impacting Aotearoa New Zealand.

The GCSB has continued to provide signals intelligence insights to 19 government agencies and their Ministers on a range of topics that has helped shape government policy, as well as deliver our unique cybersecurity services to organisations of national significance through our National Cyber Security Centre (NCSC). It has also been a year in which we have launched new information security services and continued to evolve our technical capabilities and strengthen our workforce.

Russia's ongoing invasion of Ukraine is one of the largest armed conflicts in Europe since the conclusion of World War II. Its knock-on effects continue to reverberate in global economic, food and energy markets, as well as recalibrate many states' foreign policies and test the global rules-based order.

With the battlefield invasion came the heightened risk of an escalating cyber conflict that directly or indirectly threatened Aotearoa New Zealand's digital infrastructure. Although the Russian cyber offensive was of a lesser scale than expected, we have remained alert to the possibility of domestic networks being impacted by malicious activity spanning from this conflict, the most likely of which would be an indirect attack on our digital supply chains.

Peace and stability in the Pacific has been an enduring signals intelligence focus for successive Governments in Aotearoa New Zealand, especially in recent years given the region is experiencing heightened geostrategic competition and transnational organised crime. This enduring focus includes understanding the range of current and emerging threats to the stability, security, resilience and governance of the Pacific region, including resource exploitation, maritime issues, and more recently COVID-19.

The GCSB continues to make unique and valuable contributions in countering terrorism and violent extremism internationally, and is working more proactively with New Zealand Police and New Zealand Security Intelligence Service (NZSIS) domestically.

The cybersecurity threats Aotearoa New Zealand faces are becoming more sophisticated and more impactful, and the past year is no different as ransomware and supply chain exploitation continue to be the focus of malicious cyber actors. In this reporting year Aotearoa New Zealand has attributed two malicious state cyber campaigns – one to the People's Republic of China and one to the Russian Federation – at a time where the line between state and criminal motivated cyber activity is becoming less and less distinct.

Staying ahead of the cyber threat and strengthening the national defensive posture is a significant task, and a critically important one. Working in partnership with the public sector to help build cyber resilience has been a key priority. We have worked with Microsoft and Amazon Web Services to incorporate baseline government security templates into cloud services, and we have launched our Malware Free Networks service, which makes our cyber threat intelligence available to commercial cyber security providers to help defend customer networks.

Looking ahead at our future capability, Budget 22 delivered $45.9 million of extra funding over the next four years which the GCSB's will focus on growing national cybersecurity, responding to increased geostrategic competition in our region, and our domestic counter-terrorism effort. This represents ongoing additional funding from Government in each Budget since 2016.

The year also saw the retirement and removal of the GCSB's most publicly recognisable structures – the two radomes and dishes at Waihopai Station. The first of the two satellite interception dishes and its protective radome covering were installed in 1989, during the age of fax machines and VHS recorders. In the intervening 33 years evolving technology and changes in global communications rendered them virtually obsolete.

Technological acceleration represents a constant challenge, and as new communications tools and platforms emerge, the intelligence community must be able to morph capability quickly and seamlessly. In response, this year has seen the GCSB develop and deploy new technical capability.

Against a backdrop of ongoing COVID-19-related disruptions our workforce has continued to grow and change. A strong focus for me personally and for the organisation as a whole, is ensuring we have a workforce that reflects the community we serve, and a workplace that is inclusive, and which truly values the different perspectives that comes with this diversity. With the NZSIS, we have appointed our first Chief Advisor – Māori, with our Māori cultural capability plan set out in this Annual Report for the first time.

While we continue our diversity journey, staff recruitment and retention remain a constant challenge with our workforce of highly skilled specialists who are extremely sought-after in a very competitive market. In response we are implementing a new performance management and remuneration framework.

Undoubtedly, this year has presented its fair share of challenges, but the professional people of the GCSB have risen to meet them. I am proud to lead a team that is so dedicated in fulfilling the mission to protect and enhance Aotearoa New Zealand's security and wellbeing.

Andrew Hampton

Te Tumu Whakarae mō Te Tira Tiaki
Director-General of the GCSB
Government Communications Security Bureau

YEAR IN REVIEW

Russian invasion of Ukraine

Russia's illegal and unprovoked invasion of Ukraine is the largest armed conflict in Europe in the 77 years since the conclusion of World War II. As well as the conflict on the land, air and sea, there is also a battle in the cyber and information domains.

In the lead-up to and following the invasion, the GCSB has been the New Zealand government's conduit of signals intelligence from our international partners. This intelligence has played an important role in assisting decision makers to lead Aotearoa New Zealand's ongoing response to the conflict.

The GCSB, through the National Cyber Security Centre (NCSC), stood up a dedicated cybersecurity effort in response to the cyber threats arising from the invasion. This response has been focussed on three key areas; sharing our cyber threat intelligence, providing advice and guidance to our most significant national organisations to build continued resilience, and using our technical cybersecurity capabilities to monitor New Zealand's networks for malicious activity. This effort has leveraged our recently launched Malware Free Network capability as well as other defensive capabilities.

Malicious Russian cyber activity has been a feature of the invasion but not at a scale some expected. While we have not seen any evidence of Russia directly targeting Aotearoa New Zealand, Russia is known to be unpredictable and we remain alert this may change as the conflict descends into a prolonged battle of attrition. The most significant threat to domestic digital infrastructure is an indirect attack on global digital supply chains, and we remain vigilant to the possibility of attacks emanating from sympathetic proxies or malicious criminal groups taking advantage of the unsettled global situation.

Geostrategic competition and counter-terrorism

The last year has seen a continued increase in geostrategic competition and ongoing changes in the global and domestic terrorism and violent extremist threatscape.

We are living in an increasingly complex and polarised world. Beyond the Russian invasion of Ukraine we are witnessing a rise in geopolitical competition, including in our region, that has been made more acute by the global impacts of the ongoing COVID-19 pandemic and the economic downturn that has ensued. We are seeing states acting more assertively and willing to challenge the international rules-based order and norms that underpin global peace and security.

Successive governments have had an enduring intelligence interest in the Pacific region and the GCSB makes a significant intelligence contribution in helping inform our decision makers and shape our national response. This enduring focus includes understanding the range of current and emerging threats to the stability, security, resilience and governance of the region. In the last year the GCSB has produced significant lines of reporting regarding New Zealand's interest in our region and geostrategic competition more broadly, in line with the National Security Intelligence Priorities.

The global terrorism threatscape continues to evolve notwithstanding the end of the so called Islamic State caliphate. Faith-based violent extremist networks continue to be active in parts of the Middle East, Africa and Asia. At the same time, the spread of extremist material online continues to engage identity and ideological-based extremists around the world, including white identity extremists.

The GCSB continues to make a unique highly valued and ongoing contribution to global counter-terrorism efforts, including helping to disrupt attack planning. Domestically, the GCSB is proactively providing more assistance to Police and the NZSIS in their counter-terrorism efforts, in line with observations from the the Commission of Inquiry into the terrorist attack on Christchurch Masjidain. All of our counter-terrorism contributions are carried out in accordance to the National Security Intelligence Priorities, and Aotearoa New Zealand's legislation and human rights obligations.

More broadly, the GCSB continues to provide signals intelligence on globally significant matters that has informed decision makers in 19 government departments and their Ministers. This has been across all 13 National Security Intelligence Priorities from COVID-19, to transnational crime.

Evolving cyber threatscape

The GCSB's role as a signals intelligence agency gives it access to technical capabilities, legal authorities and international relationships not available to other cyber security providers in Aotearoa New Zealand. For some years the Bureau's NCSC has stated the cybersecurity threats we face are becoming more sophisticated and more impactful – and in this reporting year it is no different.

This year the NCSC recorded 350 malicious cyber incidents affecting nationally significant organisations, which is down on last year. This likely reflects a range of factors including the impact of the Russian invasion of Ukraine on the behaviour of malicious actors and improved cyber defence and resilience. Nonetheless, we have been involved in the response to a range of cyber incidents that have not been reported publicly.

We have seen continued changes in tactics, techniques and procedures by malicious actors, who take advantage of rapidly evolving technology and its global use. This includes increasingly sophisticated ransomware attacks, the mass exploitation of recently disclosed vulnerabilities, and attacks on supply chains to compromise customers. We have also seen a shift in the strategic priorities of state-sponsored actors and the pursuit of new revenue streams by sophisticated criminally motivated actors. The line between these two continue to blur as criminal groups increasingly use capability once only used by state actors, and a small number of states continuing to provide safe harbour to criminal groups.

This year Aotearoa New Zealand publicly attributed two state-sponsored cyber campaigns informed by GCSB technical analysis. One to the Russian Federation for its malicious cyber campaign against Ukraine, and the other to the People's Republic of China for the activities of state-sponsored actors known as Advanced Persistent Threat 40, including its exploitation of Microsoft Exchange vulnerabilities.

Cyber defence and resilience

Cybersecurity has to be a team effort. Working in partnership with private sector organisations to help build cyber resilience has been one of our key priorities this reporting year.

We have worked with Microsoft and Amazon Web Services to deploy our government information security standards into cloud services baseline security templates. This means that organisations who use the templates automatically have the government's security controls built into their cloud infrastructure. The significant value of this work was acknowledged by Aotearoa New Zealand's cyber security industry when it was awarded 'Best Security Project' for 2021 at the annual iSANZ awards.

In November 2021, the NCSC formally launched Malware Free Networks – a scaling up of cyber defence capabilities, which makes our cyber threat intelligence available to commercial cyber security providers to help defend their customers' networks. It has already disrupted 120,000 threats, as at 30 June 2022.

Staying abreast of the evolving cyber threatscape and adjusting the national defensive posture is a significant task. This year we have engaged with hundreds of organisations to ensure they have effective cyber security governance, understand their critical systems and risks – particularly across their supply chain – and have a plan for how they would respond to a cyber-security incident.

This has been a busy year for our information security function. The GCSB is the security regulator for the telecommunications sector, and we, along with the NZSIS, have security regulatory functions for space launches from Aotearoa New Zealand

and foreign investment in key areas. All have seen marked increases in workload in the reporting year.

We also provide technology services to the 15 government agencies that operate at the Top Secret classification level, and this year we completed the replacement of the cryptographic management system, which encrypts Aotearoa New Zealand's most sensitive information.

The Director-General of the GCSB's role as the Government Chief Information Security Officer provides leadership and set standards around cybersecurity resilience for the broader public service. Funding was provided in Budget 21 to strengthen this role, and in 2022 it was formally designated as a system leader under the Public Service Act.

Evolving our capabilities

A significant moment for the GCSB was the decision to retire and remove the two satellite interception antennae and their protective radomes at Waihopai Station. The two dishes represented near-redundant technology. They were no longer operationally important and were contributing less and less intelligence reporting in comparison with other collection capabilities.

There have been huge technological advancements since the first dish was installed at Waihopai Station in 1989. The world is cabled up, there is ubiquitous encryption, and we have seen the advent of the internet, which has transformed almost every aspect of how society goes about their lives within half a generation. Technological acceleration represents a constant challenge, and as new communications technologies emerge, our intelligence community must be able to evolve capability quickly and seamlessly.

The GCSB's legislation allows us to intercept communications, seek assistance from telecommunications network operators, and receive intelligence from our international partners. It also allows us to access information infrastructures, which enables us to retrieve digital information directly from where it is stored or processed.

With the exception of high frequency radio interception, the GCSB's capabilities have well and truly moved on since the first dish and radome was installed 33 years ago. This year saw the development and deployment of new intelligence collection and analysis capabilities in line with investment in previous Budgets.

In Budget 22, the GCSB received $45.9 million of additional funding over four years, which follows $139 million of investment over four years in Budgets 19 and 20. This year's funding allocation is focussed on boosting public sector cyber security, work on dealing with increased geostrategic competition in our region, and counter-terrorism.

Strengthening our workforce

The success of the GCSB doesn't just depend on our technical capacities, our relationships including with international partners, or our legislation and the social license under which we operate. The most important part of the GCSB remains our dedicated and professional staff.

Against a backdrop of a range of disruptions, including those COVID-19-related, the GCSB continued to grow and evolve as a community.

The GCSB is strongly focussed on ensuring we have a diverse workforce that reflects the community we serve, and a workplace that is inclusive, and which truly values the different perspectives that comes with this diversity.

It is fundamental that we not only bring to bear the broad range of perspectives to the problems we are seeking to solve, but that we can attract the best people from all parts of society to come and work for us. Diversity and Inclusion is also vital to public trust and confidence by providing assurance that, while we often operate in secret, our people reflect the values and perspectives of contemporary Aotearoa New Zealand.

We launched with the NZSIS our first Diversity and Inclusion Strategy about five years ago, and while we are still on our journey of change, today over half our senior leaders are women. Since 2017 we have eliminated gender pay gaps for like-for-like roles and reduced the overall gender pay gap by two-thirds, and ethnic diversity has doubled.

Another significant development this year has been the appointment, with the NZSIS, of a Chief Adviser Māori to assist our agencies build our Te Aō Māori capability and better understand and fulfil our obligations as part of the Crown under the Treaty of Waitangi.

Dealing with disruption

The year has posed a range of challenges that have placed extraordinary pressure on our people, including the continued reverberations of COVID-19, a rise in demand for our highly skilled staff from other sectors, and the disruptions from the four-week illegal Parliamentary occupation.

While the challenges associated with the COVID-19 pandemic and associated health mitigations have been felt by all New Zealanders, we are exceptional in that the vast majority of staff cannot readily work outside of a secure environment, which has placed additional considerations around coming to the office safely.

The Parliamentary occupation caused some disruption for most government agencies, including ourselves. Two of our offices, Pipitea House and the NCSC's location at Defence House, bordered the occupation cordons, which created difficulties in moving around the area.

Retention has been a significant issue of the GCSB over the past reporting year, with 19.3% turnover, more than double last year's turnover and up from 13.7% recorded in the 2019/20 year. We are an agency that undertakes highly specialised and unique work and our staff possess skills not commonly matched elsewhere. Unsurprisingly, the GCSB loses a steady stream of staff to more lucrative sectors, but this flow has intensified in the reporting year as the employment market has become even more competitive.

In response to these workforce pressures we, with the NZSIS, began implementing a new remuneration and performance management framework to ensure we remain a competitive employer.

In February 2022 the GCSB and NZSIS received the findings of a detailed seismic assessment undertaken ahead of the lease for our headquarters, Pipitea House, coming due for renewal. The detailed seismic assessment found one element of Pipitea House was problematic and meant the building overall was at seismic risk. was considered earthquake prone.

The GCSB and NZSIS sought further advice on specific risks related to continued use of the building. On the basis of that advice, we cordoned off certain areas of Pipitea House which has necessitated reducing staff numbers in the building to remain compliant with fire regulations.

The response to the detailed seismic assessment has been shared with the property owner and an agreed plan is in place to have the work completed in the first half of 2023.

Alongside COVID-19 related impacts, the detailed seismic assessment required GCSB and NZSIS to find ways to manage impacts to the agencies' outputs. Managing these impacts has been a key priority for the agencies, and has also been undertaken in cooperation with the wider national security sector.

02

OUR WORK IN DETAIL
HE TIROHANGA HŌMIROMIRO KI Ā MĀTAU MAHI

THE ROLE OF THE GCSB

The GCSB is New Zealand's lead organisation for signals intelligence (SIGINT) and cyber security and resilience for organisations of national significance. Our mission is to protect and enhance New Zealand's security and wellbeing. The GCSB is a crucial part of how New Zealand makes sense of the world and manages national security threats.

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. Our National Cyber Security Centre (NCSC) provides information assurance, cyber threat detection, disruption and advice to organisations of national significance and respond to cyber incidents that have the potential to have a national impact. The GCSB also has regulatory functions and the Director-General is the Government Chief Information Security Officer.

Under the Intelligence and Security Act 2017, the purpose of which is to protect New Zealand as a free, open, and democratic society, the GCSB has four core functions:

- Intelligence collection and analysis;
- Protective security advice and assistance, including information assurance and cyber security activities;
- Co-operation with other public authorities to facilitate their function, and
- Co-operation with other entities to respond to imminent threat.

Locations

The GCSB has facilities in three locations, Wellington, Auckland, and Waihopai, near Blenheim. We also have a high frequency radio interception and direction-finding station, Tangimoana, near Palmerston North.

THE NEW ZEALAND INTELLIGENCE COMMUNITY

The GCSB, along with the New Zealand Security Intelligence Service (NZSIS) and the National Assessments Bureau within the Department of the Prime Minister and Cabinet (DPMC) form the core national intelligence, assessment and protective security functions within the New Zealand Intelligence Community (NZIC).

These agencies work with the specialist intelligence functions of other agencies such as the New Zealand Police, the New Zealand Customs Service, the New Zealand Defence Force, and Immigration New Zealand.

The NZIC exists to protect New Zealand as a free, open, and democratic society. The intelligence-based insights and advice provided by the NZIC contribute to decisions that sustain and enhance New Zealand's security and wellbeing.

The NZIC has a crucial role to play in understanding the threats New Zealand faces and how to guard against those threats. By providing unique intelligence insights to policy and decision makers, the NZIC contributes to building a safer and more prosperous New Zealand.

The NZIC strives to advance New Zealand's international reputation and interests. By working with international partners the NZIC articulates New Zealand's national security priorities and interests on a global stage.

Te Rōpū Pārongo Tārehu o Aotearoa
Intelligence Community

The core NZIC agencies are:

Government Communications Security Bureau

The GCSB collects intelligence, in accordance with New Zealand's national security priorities, and provides that intelligence to relevant parties to support informed decision making. The GCSB also ensures the integrity and confidentiality of government information, provides cyber security services to organisations of national significance, and assists other New Zealand government agencies to discharge their legislative mandate.

New Zealand Security Intelligence Service

The NZSIS identifies, investigates, assesses and mitigates threats to New Zealand's national security, and provides a range of protective security advice and services to the New Zealand Government. The NZSIS also provides cooperation and assistance to other New Zealand government agencies.

Department of the Prime Minister and Cabinet: National Assessments Bureau

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

NATIONAL SECURITY INTELLIGENCE PRIORITIES (NSIPS)

The Government's National Security Intelligence Priorities (NSIPs) – Whakaarotau Marumaru Aotearoa - outline key areas of interest and define where intelligence can support government to make informed decisions about national security.

The priorities cover a large range of risks to New Zealand's security and wellbeing. This is because New Zealand takes an 'all hazards, all-risks' approach to national security. This approach allows coordination between government agencies, seeking to provide a joined-up response to national security risks.

The NSIPs are coordinated by DPMC and a range of agencies, including the GCSB, respond to them.

The current priorities were approved in December 2021. They are listed below in alphabetical order:

01. Biosecurity and human health	**02.** Climate change and environmental issues	**03.** Emerging, critical and sensitive technology	**04.** Foreign interference and espionage
05. Global economic security	**06.** Global governance and strategic competition	**07.** Malicious cyber activity	**08.** Maritime, border security and Antarctica
09. New Zealand's strategic interests in the Asia region	**10.** New Zealand's strategic interests in the Pacific region	**11.** Terrorism and violent extremism	**12.** Threats to New Zealanders overseas
13. Transnational serious and organised crime			

A full description of the NSIPs is available on the DPMC's website.

INTERNATIONAL PARTNERSHIPS

The GCSB's engagement with international partners aligns with the New Zealand Government priorities, including the 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, and to the laws of partner countries that share information or other support with us.

Five Eyes

New Zealand, Australia, Canada, the United Kingdom and the United States of America, make up an international intelligence and security partnership known as the Five Eyes. Working within this partnership provides New Zealand with support, technology, and information that it wouldn't otherwise have.

While New Zealand receives great benefit from the Five Eyes partnership, it also makes a unique and valued contribution to global efforts.

The Five Eyes partnership is fundamental to the GCSB's work to support New Zealand's national security 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.

INVESTING IN CAPABILITIES

The way in which the GCSB works has evolved, and will continue to evolve, alongside changes in technology. The GCSB needs to continuously assess and update its capabilities to ensure they contribute to the fullest extent possible to the Government's priorities, as well as respond to rapidly evolving technology, and to the security threats New Zealand faces.

Budget 22

Investment helps us equip and evolve our capabilities in the face of accelerating technology and growing geostrategic pressures, including in our region.

As a technology-based organisation, successive investment to enable new and upgraded technology is central to the continued success of our mission.

In Budget 22 the GCSB received $45.927 million of new funding, over four years. This included funding for initiatives related to cyber security within the public sector and for nationally significant organisations, responses to geostrategic competition in our region and counter-terrorism.

Of the total funding, $18.986 million is being allocated over four years to improving services to continue to protect New Zealand's most significant information. The increasing frequency of cyber attacks means we need to adapt to stay resilient to threats to enhance New Zealand's economic wellbeing.

Our strategic capabilities and activities received $26.941 million over four years, and approximately $12.636 million over four years of this funding will be invested in GCSB counter-terrorism activities, responding in part to commentary within the report of the Royal Commission of Inquiry into the Terrorist Attack on Christchurch Masjidain.

Waihopai

We announced in November 2021 that the GCSB had decided to decommission and remove the radomes and dishes at Waihopai Station after more than 30 years of service. This decision is an example of the way the GCSB has evolved as an agency alongside technological changes.

This decision was primarily grounded in the fact that changes in global telecommunications and information technology mean the interception of satellite communications from Waihopai had declined over the years to the point where dish use is now virtually obsolete.

THE INTELLIGENCE AND SECURITY ACT 2017

The Intelligence and Security Act 2017 (ISA) provides the legal framework for GCSB and the New Zealand Security Intelligence Service (NZSIS)'s 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.

Review of the Act

The periodic statutory review of the ISA commenced on 2 March 2022. The purpose of the review is to understand what improvements could be made to the ISA to ensure it continues to be clear, effective and fit for purpose, as well as considering the issues and recommendations related to the Act that were raised in the Royal Commission of Inquiry into the Terrorist Attack on Christchurch Masjidain report.

Alongside the NZSIS, the GCSB is engaging fully with the review which is scheduled to be concluded no later than 20 December 2022.

Statement of Warrants

19	Type 1 Warrants issued
16	Type 2 Warrants issued
0	Warrants declined
2	Business directions applied and issued

Under the 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 35 intelligence warrants were approved in 2021/22, of which 19 were Type 1 intelligence warrants and 16 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.

No very urgent authorisations were made this year by the Director-General under section 78. Very urgent authorisations are authorised by the Director-General where the delay in making an urgent application to a Commissioner of Intelligence Warrants and the Minister would defeat the purpose of obtaining the warrant. It is automatically revoked 24 hours after the authorisation is given.

The GCSB did not provide any advice and assistance to the New Zealand Defence Force or the New Zealand Police for the purpose of exercising those agencies' functions 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.

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

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

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

OFFICIAL INFORMATION AND PRIVACY ACT REQUESTS

The GCSB is subject to the Official Information Act 1982 (OIA) and the Privacy Act 2020. 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 2021 to 30 June 2022, the GCSB:

- Completed 70 OIA requests, with five requests completed outside the legislated timeframe; and
- Completed 16 Privacy Act requests, all within the legislated timeframe.

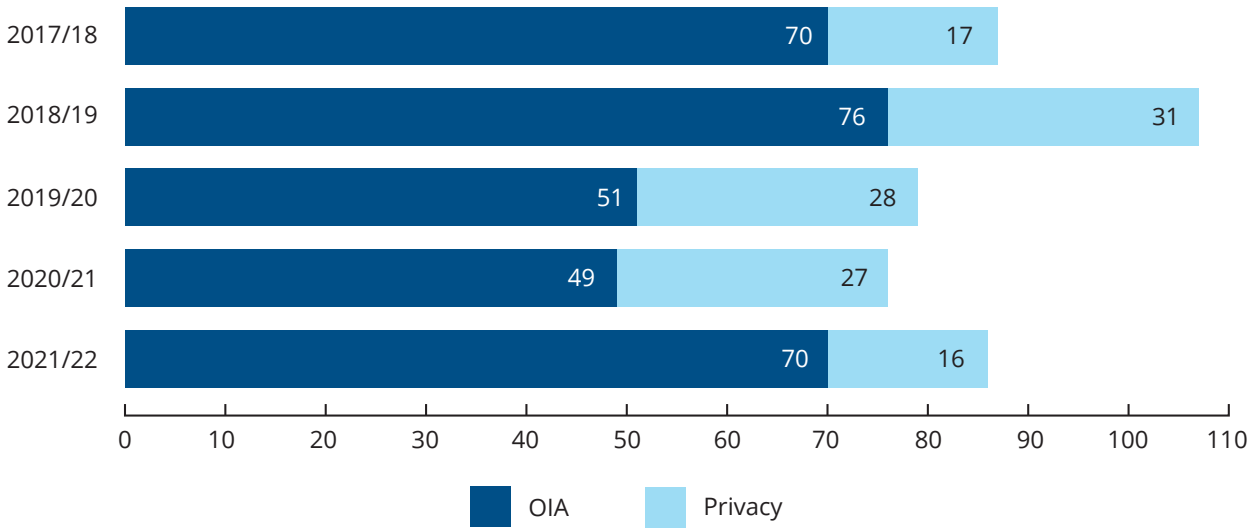
The GCSB aims to complete all information requests within the legislated timeframe. A range of factors including COVID-19, staff turnover and accommodation issues impacted the GCSB's ability to respond to information requests within the legislated timeframe during this year. This situation is regrettable and we expect to return to full legislative compliance as soon as the significant disruption caused by COVID-19 and building issues is over.

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

The GCSB was notified of two complaints by the Office of the Ombudsman during the 1 July 2021 – 30 June 2022 period. One complaint was resolved in the GCSB's favour, while the other is still being considered. In addition, the Ombudsman formed a final opinion against the GCSB, in respect of a complaint which was notified in the previous year.

The GCSB was notified of two complaints by the Privacy Commissioner during this period. These complaints, plus another from the previous year, were all resolved during this time period. In each instance the Privacy Commissioner was satisfied with the decision-making on the original request and the complaints were resolved in the GCSB's favour.

THE GCSB'S OFFICIAL INFORMATION ACT AND PRIVACY ACT COMPLETED REQUESTS



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.

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.

In 2021/22, the GCSB appeared before the ISC on several occasions often with other agencies, in addition to the Estimates of Appropriation Reviews and the Financial Review of the agency. We participated on briefings on specific topics including the cyber threatscape and our response, and our intelligence continuation on geostrategic competition and counter-terrorism.

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.

No new reports or investigations were published in the 2021/22 financial year.

OUR SUSTAINABILITY REPORTING

We are committed to meeting the requirements of the Carbon Neutral Government Programme (CNGP) and operating in an emissions and energy friendly manner. We have chosen the 2018/19 financial year as our base year as this represents a typical 12-month period before COVID-19 impacted on our operations.

Independent Verification

The GCSB is planning to have its emissions independently verified against ISO14064-1:2018. The emissions reported in this annual report have not been independently verified.

The greenhouse gas emissions measurement (emissions data and calculations) reported in this annual report have been calculated based on an extrapolation of a sample of underlying financial records.

In 2021/22 (based on our sampled data and extrapolation) we emitted 1,760 Tonnes CO2-e. Most of our emissions came from electricity, as well as from passenger transport and motor vehicles.

Total Annual Emissions and their sources (Unverified)

CATEGORY	2018/19 TONNES CO2-E	2021/22 TONNES CO2-E
TOTAL GROSS EMISSIONS	**2,707**	**1,760**
Change in gross emissions (all Categories) since base year		-35%

Our Reduction Targets

The Government has set the following emission reduction targets for Government departments, as required by the CNGP.

- **2025 target:** Gross emissions (all Categories) to be no more than 2,138 Tonnes CO2-e, or a 21% reduction in gross emissions (all Categories) compared to the base year FY 18/19.
- **2030 target:** Gross emissions (all Categories) to be no more than 1,570 Tonnes CO2-e, or a 42% reduction in gross emissions (all Categories) compared to base year FY 18/19.

Our Initiatives

We are still undertaking work, including undertaking consultation with staff, to complete and approve our emission reduction plans.

Further research and analysis is required to understand the impact that reduction emission plans would have on the GCSB before they are approved. The final plan will focus on the areas of greatest emissions, and the potential of programmes to achieve emission reductions.

Improving our data

The GCSB is in the early stages of the CNGP. The GCSB has identified that it needs to make improvements to its emission data collection methods, and is planning on making these improvements over the next year.

3.0
IMPENETRABLE INFRASTRUCTURE
HE HANGAROTO PĪTONGATONGA

The GCSB's National Cyber Security Centre (NCSC) protects Aotearoa New Zealand's wellbeing and prosperity by providing trusted cyber security services to government and New Zealand's most significant organisations.

NATIONAL CYBER SECURITY CENTRE STRATEGIC FOCUS

The National Cyber Security Centre (NCSC) protects Aotearoa New Zealand and its interests through its delivery across four key information assurance and cyber security strategic focus areas: Detect, Disrupt, Advise and Deter.

We detect indications of malicious activity or vulnerabilities, and provide timely and evidence-based advice to our customers on best-practice techniques to mitigate potential risks to their operating environments.

We disrupt threats from harming our customers' environments by providing best-practice mitigation advice.

We provide trusted, independent advice that helps reduce the cost across the system by providing assurance, mitigating risk, enabling innovation, and supporting our customers through security issues.

Our advice guides and equips our customers to protect their valuable information and manage risks.

We deter our adversaries by raising the cost of targeting Aotearoa New Zealand by providing best practice and world-leading information security services.

When required to support response to potentially high-impact events, we assist victims and their commercial suppliers to remove and dispose these harmful threats.

Detect

We detect indications of malicious activity or vulnerabilities, and provide timely and evidence-based advice to our customers on best-practice techniques to mitigate potential risks to their operating environments.

We protect Aotearoa New Zealand's information networks by deploying our cyber security technologies to detect and discover cyber security threats.

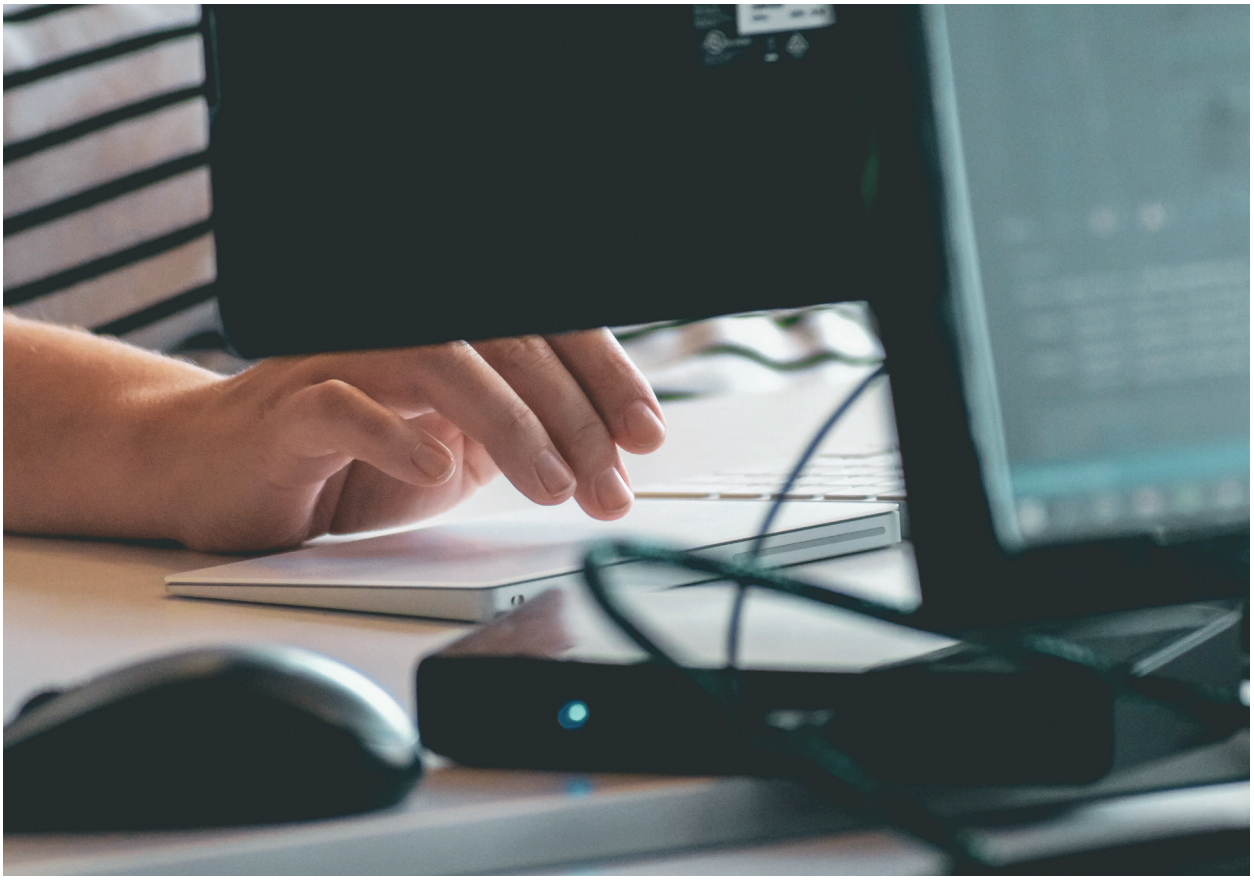
We ensure the New Zealand Government's classified systems are free from compromise by providing assurance to secure systems and sites, and diplomatic posts.

We drive evidence-based decisions by providing cyber threat and intelligence reporting and advice to key public and private sector customers.

Disrupt

We prevent threats from harming our customers' environments by providing best-practice mitigation advice and, when required, we intervene to remove and dispose these harmful threats. We do this through the following activities:

- We provide protection for our customers by blocking harmful activities through our active disruption capabilities.
- We support our customers' incident response activities by isolating and removing potential threats or vulnerabilities from our customers' environments.
- We support our customers to protect themselves by providing advice around potential threats within their landscape and provide advice on how to mitigate these.



Advise

We guide and equip our customers to protect their valuable information and manage risks. We act as trusted, independent advisors, reducing the cost across the system by providing assurance, mitigating risk, enabling innovation, and supporting our customers through security issues.

We improve Aotearoa New Zealand's information security maturity by developing, managing and promulgating policies, standards and guidance.

We improve Aotearoa New Zealand's security resilience by upskilling government agencies and nationally significant organisations.

We support decision-making advantage by informing national security determinations with fit-for-purpose reports and briefings.

Deter

We raise the cost for our adversaries in targeting Aotearoa New Zealand by providing best-practice and world-leading information security services. We do this through the following activities:

- We ensure the confidentiality and integrity of the New Zealand Government's classified information and communications by providing high-grade encryption capabilities.
- We ensure the safety and security of the New Zealand's Government's most sensitive information through regular inspections and accreditation of classified sites and systems.
- We support robust technology investment within Aotearoa New Zealand's critical systems by upholding the independence and rigor of our regulatory frameworks.
- We are Aotearoa New Zealand's first line of cyber defence by detecting, disrupting, analysing and publicly identifying threats from across the cyber landscape.

CYBER THREATSCAPE

The cyber threats that Aotearoa New Zealand faces continue to evolve, becoming more persistent, more sophisticated, and more capable of causing severe impact to service delivery and information security.

This is happening against a background of rapid change in the way technology is being used. Increased use of cloud services, changing work patterns driven in part by response to the pandemic, and a generally increasing reliance on digital platforms for delivery of services are creating a greater attack surface for malicious actors.

We are seeing an increase in the speed and scale of scanning and mass-exploitation of recently disclosed vulnerabilities.

Malicious actors are quickly taking advantage of newly discovered vulnerabilities by targeting every device and organisation that is potentially vulnerable to exploitation, establishing footholds in networks, and selectively picking their targets for further compromise.

They are also shifting to establish more strategic access, for example through the compromise of critical supply chains. Examples of this include exploitation of vulnerabilities in widely used products such as Microsoft Exchange, and the compromise of the Solar Winds Orion server management platform, in recent years.

Another development we are seeing is in the nature of threat actors' in particular, the blurring of lines between state and non-state actors.

Financially motivated criminal groups have access to sophisticated tools that were once in the exclusive control of nation states. These groups are provided safe havens to operate by states who do not abide by the international norms of acceptable behaviours in cyber space. Issue-motivated actors, including those aligning with state interests, currently feature on the international threatscape.

Conversely, state actors can masquerade as criminal groups to cause disruption, as we saw in 2017 with NotPetya, where Russian state actors developed and deployed malware intended to disrupt Ukrainian financial systems. Their indiscriminate deployment of NotPetya resulted in a widespread global impact including here in Aotearoa New Zealand.

RUSSIAN INVASION OF UKRAINE

This year we saw Russia use its cyber capabilities in the context of its invasion of Ukraine.

Malicious cyber activity in Aotearoa New Zealand reflects international trends, and alongside Russia's invasion of Ukraine and the ongoing conflict, there has been increased potential for cyber attacks that cause widespread disruption. Such attacks can have serious impact, even for countries and organisations not directly targeted.

The NCSC has contributed to the Aotearoa New Zealand Government's condemnation of the widespread disruption resulting from indiscriminate cyber campaigns conducted by Russia.

As part of the international response to the increased cyber threat as a consequence of Russia's invasion of Ukraine, the NCSC stood up a dedicated effort which focused on three areas:

- Sharing cyber threat intelligence with Aotearoa New Zealand organisations;
- Using our technical cyber security capabilities to monitor New Zealand networks for malicious activity, and
- Providing advice and guidance to our most important organisations to build continued resilience.

In February 2022, we advised operators of Aotearoa New Zealand's critical infrastructure to prepare for potential cyber threats – including destructive malware, ransomware, distributed denial-of-service (DDoS), and cyber espionage – amidst increasing geopolitical tensions in Europe.

In April 2022, the NCSC released a joint cyber security advisory (CSA) with the cyber security authorities of the United States, Australia, Canada, and the United Kingdom. The joint CSA, titled Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, warned organisations that Russia's invasion of Ukraine could expose organisations both within and beyond the region to increased malicious cyber activity.

Of equal concern to direct targeting of Aotearoa New Zealand by Russian state-sponsored actors is indirect targeting that affects a critical supply chain, or an opportunistic malicious campaign by a criminal group, such as ransomware. These actors may be either sympathetic to Russia or simply motivated by financial gain and are taking advantage of the global disruption.

Along with our partners in the Five Eyes we issued an advisory warning organisations that Russian state-sponsored cyber actors have demonstrated capabilities to compromise IT networks; develop mechanisms to maintain long-term, persistent access to IT networks; exfiltrate sensitive data from IT and operational technology networks; and disrupt critical industrial control systems by deploying destructive malware.

On the domestic front, the NCSC has not seen a significant change in the cyber threat landscape that can be associated with Russia's invasion of Ukraine. The NCSC is alert to the fact the situation could change with no advance warning, as both pro-Russia and pro-Ukraine cyber activity continued to impact systems around the world. The NCSC assesses the most significant threat to Aotearoa New Zealand networks from Russia's invasion of Ukraine is indirect malicious cyber activity that affects a critical supply chain, including opportunistic activity by cyber criminal groups.

CYBER SECURITY INCIDENT RESPONSE

The GCSB's NCSC continues to provide an incident response capability to assist organisations in their response to potentially high-impact cyber security incidents.

In 2021/22, the NCSC recorded 350 cyber incidents, compared to 404 in 2020/21. Of those recorded incidents 118, or 34%, indicated links to suspected state-sponsored actors, compared to 28% in the 2020/21 year, 81 incidents, or 23%, were likely criminal or financially motivated.

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

Major event support

The NCSC contributes cyber security support to multi-agency efforts on major national events. Planning for major events involves preparing for the possibility that a cyber security incident could cause disruption and/or reputational harm.

We assisted agencies involved to ensure the virtual hosting platforms used to facilitate online meetings were secure, and that risk assessment and mitigation processes were in place to protect participants. By successfully adapting to hosting the Asia Pacific Economic Cooperation forum (APEC) virtually, Aotearoa New Zealand played a leadership role in championing the APEC goal of building an open, dynamic, resilient, and peaceful Asia-Pacific community.

The NCSC also supported the Electoral Commission's delivery of a by-election in the Tauranga electorate. This included the provision of cyber resilience advice, and engagement with the Electoral Commission to ensure that appropriate incident response processes were in place.

As at 30 June 2022, the NCSC is supporting key organisations involved in the delivery of the 2022 local government elections. This includes working with organisations in the lead-up to the event to help protect their systems from cyber interference, as well as the provision of cyber resilience advice and cyber threat assessments.

The NCSC's support to Census 2023 is also in the planning stages.

Cyber Defence Capabilities

The NCSC's CORTEX cyber defence service continues to play a significant role in the GCSB's work to support organisations of national significance to protect their networks from malicious, advanced, persistent, and sophisticated cyber security threats.

The NCSC provides its advanced cyber threat disruption and detection capabilities to a range of nationally significant organisations. Our CORTEX customers are spread across the central and local government, critical infrastructure providers, key economic generators, and key research institutes.

For security and confidentiality reasons, we don't disclose CORTEX customers publicly.

Malware Free Networks

In November 2021, we publically launched our Malware Free Networks (MFN) capability. This cyber defence tool provides a cyber threat intelligence feed that contains indicators of malicious activity, generated from a range of sources. MFN is a malware detection and disruption service that enables us to significantly scale our cyber defence effort across a large range of Aotearoa New Zealand organisations.

The NCSC delivers MFN in partnership with internet service providers and managed services providers. MFN partners use our automated threat feed to detect and disrupt threats before they impact their customers' systems. They provide telemetry back to us so we understand the effectiveness of the feed, and gain greater understanding of the domestic environment.

As of 30 June 2022, MFN has now disrupted more than 120,000 threats. That figure reflects disruptions of potentially malicious activity that has the potential to cause significant harm to Aotearoa New Zealand's organisations.

Cyber security capability development

The dynamic nature of the cyber threat environment and the increasingly rapid evolution of technology platforms means the NCSC needs to be constantly thinking ahead to ensure our capabilities continue to be fit for purpose to respond to the changing environment.

This includes developing roadmaps to enable business planning and identify future strategic investment opportunities.

We have also commenced work on an improved data acquisition capability leveraging cloud provider relationships, and our network ingestion and processing systems have received a significant lifecycle refresh.

A continuous improvement focus has been implemented across a range of cyber security analytic tools to support our existing cyber security mission and delivery of Malware Free Networks.

Cyber attributions

The Aotearoa New Zealand Government continues to work closely with international partners to "call out" malicious cyber activity counter to the internationally accepted norms of behaviour in cyberspace.

The GCSB, through the NCSC, frequently conducts internal, technical attributions of malicious cyber activity and shares these, usually at a classified level, with the Aotearoa New Zealand Government and international partners.

When it is in our national interest to do so, the Aotearoa New Zealand Government may decide to publicly reveal the conclusions of our technical attribution process to call out a malicious cyber actor.

In April 2021, the Minister Responsible for the GCSB, added New Zealand's voice to international condemnation of the compromise and exploitation of the Solar Winds Orion platform by Russian State Actors.

The NCSC's technical assessment contributed to public attribution of a range of malicious cyber activity to Chinese state actors. In July 2021 the Minister condemned a range of activity undertaken by the Chinese Ministry of State Security both in Aotearoa New Zealand and globally. At the same time he also confirmed that NCSC analysis indicated Chinese state-sponsored actors were responsible for the exploitation of Microsoft Exchange vulnerabilities in Aotearoa New Zealand in early 2021.

The NCSC often becomes aware of malicious cyber activity without knowing the identity of the actor responsible, and it is not always possible to attribute activity to a particular state or malicious cyber actor.

RESILIENCE RAISING

The NCSC works to increase cyber resilience of Aotearoa New Zealand's organisations of national significance to help protect the economic wellbeing of New Zealanders.

Cyber Security Policy

Throughout 2021/22, the NCSC continued to develop its cyber security policy capability as part of our support for the Director-General of the GCSB's Government Chief Information Security Officer (GCISO) functional leadership.

The GCISO provides system-level information, security policy, strategic advice, and support across government agencies. This includes establishing the Aotearoa New Zealand Government information security standards and guidance, as set out in the New Zealand Information Security Manual (NZISM). Through the GCISO function, we support the Government's digital transformation programme.

As part of our engagement with industry partners in this area, we have collaborated with major cloud service providers Microsoft and Amazon Web Services to develop templates for the implementation of their cloud products. These templates, which have had wide uptake across the public and private sector, help increase the baseline security of those products by building core New Zealand Government information security standards into their basic implementation.

The significant value of this work was acknowledged by Aotearoa New Zealand's cyber security industry when the development of the cloud templates was awarded 'Best Security Project' for 2021 at the annual iSANZ awards.

Advisories and alerts

During the 2021/22 financial year, the NCSC continued to alert and advise organisations across Aotearoa New Zealand. We sent out a total of 35 advisories or alerts:

- 16 NCSC Cyber/General Security Advisories
- 7 NCSC Vulnerability Alerts
- 7 Partner Security Advisories
- 5 Joint Security Advisories.

We also distributed 25 NCSC Cyber Security Highlights documents, providing high-level summaries of relevant cyber security news and current events.

Security Information Exchanges

We continued our trust-based collaborations with specific sectors, hosting 27 meetings across our six security information exchanges. These are forums that support peer-to-peer sharing between members of sector-specific experiences, best practice and cyber security threats.

Exercises

In 2021/22, the NCSC conducted a national cyber security exercise and in early November 2021 we participated in an industry-led exercise named GridEx. GridEx was a table-top exercise including participants from Aotearoa New Zealand energy companies. The participants engaged remotely in a fictional scenario and responded in real time to events as they happened.

This exercise provided an opportunity for organisations to test their incident response processes and ensure that these aligned with their businesses requirements. The exercise also gave the sector the opportunity to engage with government to understand what resources were available, and to gain a clearer understanding of the Government's expectations for them.

In late November, following GridEx, the NCSC hosted the National Cyber Security Exercise 2021 (INTENSITY). Led by the NCSC, INTENSITY included an inter-agency steering group, and participants were from government agencies.

INTENSITY was a facilitated discussion exercise, and our focus was on testing the New Zealand's Cyber Security Emergency Response Plan.

Data breach notification service

In 2021/22, the NCSC launched a government partnership with the global data breach notification service Have I been Pwned (HIBP).

HIBP is an independent service that collates data about reported website breaches and makes the information available for consumption. The NCSC has been mandated to extract breach information linked to government domains on behalf of New Zealand. The domains captured include .govt.nz, .mil.nz , and .cri.nz

To date, the NCSC has provided historical breach reporting to a group of 15 trial customers, including two face-to-face consultations in which we provided them with a customised data trend analytics report.

Customers have advised us that the HIBP services helped their chief information officers gain better visibility over the use of shadow IT in their organisations, and that the delivery of historical breach information also prompted reviews of password and authentication policies, as well as security awareness communication to their employees.

We are preparing to release the services to the next group of customers, and will continue to collate feedback.

REGULATORY FUNCTIONS

The GCSB carries out 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 Aotearoa 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. Over the reporting period New Zealand networks have undergone a number of changes, include the continued rollout of new 5G services related to extending national 5G coverage, continued support for 4G networks, an ongoing number of hardware lifecycle updates for most operators, an increase in international capacity and carrier diversity, and the introduction of new-to-market service offerings including Fixed Wireless Access and Mobile Virtual Network Operators.

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 2021/22 reporting period, the GCSB received 179 notifications, comparable to the 141 notifications in 2020/21. Many of these involved changes related to the continued maintenance and hardware lifecycle updates and newly introduced market services.

Outer Space and High-altitude Activities Act 2017

The Outer Space and High-altitude Activities Act 2017 (OSHAA) provides a regulatory framework for managing any risks to Aotearoa 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 the New Zealand Security Intelligence Service (NZSIS), with advisors from other parts of the New Zealand Intelligence Community (NZIC), including the New Zealand Defence Force jointly assesses 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 2021/22 reporting period, the GCSB conducted 19 assessments of regulated space activities, down from 29 in the last reporting period. This is largely due to impacts of the COVID-19 pandemic on the New Zealand launch provider's activities.

Radiocommunications Act 1989

The Radiocommunications Act 1989 is administered by the Radio Spectrum Management (RSM) team at the Ministry for Business, Innovation and Employment. The risk assessment of radio communications applications was introduced into the SARAG's activities this year to bolster the assessment for ground infrastructure that is associated with on-orbit space activities.

During the reporting period, the GCSB conducted 55 assessments of regulated radio communications activities.

Overseas Investment Act 2005

In June 2021, the Overseas Investment Act (Urgent Measures) amendment was retired and the Overseas Investment Act (National Security and Public Order regime) came into effect. The amended Act includes a national interest test and changed the notification conditions for certain transaction types. However, the primary function of the Act remains largely unchanged – namely, to manage risks associated with overseas investments that are contrary to New Zealand's national interest (including national security).

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

During the 2021/22 reporting period, the GCSB conducted 42 assessments under the national security and public order regime.

The NCSC also responded to a number of ad-hoc requests for technical security assessments throughout the 2021/22 year.

INFORMATION ASSURANCE

Technical Counter-Surveillance Unit

The NCSC's Technical Counter-Surveillance Unit (TCU) (formerly called High Assurance Services) helps ensure the Government's most sensitive communications are not intercepted or compromised.

The TCU provides technical security and emanations security services. Technical security services are focused on countering technical surveillance techniques used by hostile actors, including eavesdropping and video surveillance. Emanations security services are focused on countering the threat posed by spread of unintentional signals from ICT equipment that could be intercepted and interpreted by malicious actors.

In addition to technical and emanations security, the TCU also provides recommendations to the Director-General of the GCSB on the accreditation of sensitive compartmented information (SCI) sites and systems. The Director-General is the Aotearoa New Zealand Government's accreditation authority for highly classified information systems and sites.

TCU 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. The GCSB provides technical inspection services and advice, and seeks to ensure that these facilities are free from vulnerabilities that would allow unauthorised access to information. The TCU also has a mobile capability to inspect existing facilities for signs of technological efforts to compromise security.

High-Grade Cryptographic Infrastructure

The Cryptographic Products Management Infrastructure (CPMI) project was formally closed in March 2021.The project underwent its final Cabinet mandated project review, the Treasury-led Operations and Benefit Realisation Review, in November 2021, resulting in an overall rating of Amber-Green. This acknowledges the immediate benefits of delivering the CPMI systems for Aotearoa New Zealand, and recognises the challenges we have in fully supporting and optimising the systems.

The importance of getting a good result from this review cannot be understated. The total cost of ownership of CPMI is estimated to be approximately $412 million by the end of the 2031/32 financial year. The review highlighted the immediate benefits that the government is receiving and the prospect of a positive return on investment. A good result in this review adds to the confidence that Cabinet and Treasury has in the GCSB as a whole to deliver high risk / high value projects in the future.

Secure Mobility

A recent five eyes Secure Mobility Working Group conference identified the delineation of responsibilities between the GCSB and our customers who would implement a Secure Mobility solution connected to their own classified infrastructure.

4.0

INDISPENSABLE INTELLIGENCE
HE MŌHIOHIO WAIWAI

INTELLIGENCE COLLECTION

The GCSB is a signals intelligence (SIGINT) agency, meaning 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 Department of Prime Minister and Cabinet (DPMC), and any person or class of person the Minister authorises to receive it. This includes other government agencies and international partners.

In 2021/22 GCSB provided intelligence to 19 government agencies across all 13 National Security Intelligence Priorities (NSIPs) on topics including COVID-19, counter terrorism and transnational crime.

The GCSB undertakes its activities in accordance with the Government's NSIPs, legislation, and New Zealand's human rights laws. We are also subject to robust oversight, including from the Inspector-General of Intelligence and Security and the Parliament's Intelligence and Security Committee.

As technologies continue to change, we constantly review and develop our capabilities. This year has seen the decommissioning of the satellite interception capability provided by 'the domes' at Waihopai. Changes in global telecommunications meant that the interception of satellite communications was no longer productive. In response, we have continued to develop and implement new intelligence collection and analysis capabilities in line with investment by government in recent budgets.

The Bureau's legislation enables us to intercept communications, seek assistance from telecommunications network operators and service providers, and of course receive intelligence from our international partners. Our legislation also allows us to access information infrastructures, which is more than just interception; "accessing information infrastructures" also allows us to retrieve digital information directly from where it is stored or processed.

OUR OPERATING CONTEXT

Russia's invasion of the Ukraine

GCSB has leveraged its international intelligence sharing arrangements to source a significant body of intelligence in relation to the Russia-Ukraine conflict. This intelligence is being provided to New Zealand government agencies to enable decision-making in response to the conflict.

The Russia-Ukraine crisis was in many respects business as usual for the Intelligence Customer Centre (ICC), in that surging in response to crises is a core part of the ICC's business. Specifically, the ICC worked very closely with Department of Prime Minister and Cabinet (DPMC), New Zealand Defence Intelligence and the Ministry of Foreign Affairs and Trade to ensure that relevant secret intelligence was moved quickly and reliably to customers, working to fill information gaps and promote a common understanding of a complex and rapidly unfolding situation.

The ICC was able to maintain information flows and ensure front-line analytic staff had rapid access to intelligence in support of advice to senior officials, whilst sustaining information flows to other customers. In response to an initiative suggested by DPMC, the ICC ran an intelligence digest for time-pressed senior officials supplying intelligence or other governmental information judged to be amongst the most useful items they should see.

Regional security and geostrategic competition

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, 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.

Counter-terrorism

The GCSB counter-terrorism effort provides both a foreign and a domestic focus. In respect of the foreign effort, GCSB has continued to make a unique and highly valued contribution to global counter-terrorism efforts, including contributing to the disruption of attack planning. As well as UN-designated terrorist entities, this work has also focussed on identity-motivated extremists.

The spread of extremist content and ideologies online remains a threat to New Zealand's safety and security.

Domestically, the GCSB has continued to respond to recommendations made by the Royal Commission of Inquiry into the terrorist attacks on Christchurch Masjidain and has worked closely with both the New Zealand Security Intelligence Service (NZSIS) and Police partners on a number of domestic terrorism related investigations.

In-line with the commentary from the Royal Commission into the abhorrent Christchurch terror attacks, the GCSB has been increasingly proactive in support for domestic counter-terrorism investigations.

Foreign Interference

All states engage in foreign influence activity in that they seek to shape perceptions and decision making in other countries. This activity becomes foreign interference when it is purposely misleading, deceptive, covert or clandestine.

GCSB works closely with the NZSIS to better understand the extent to which New Zealand's sovereign structures are at risk from foreign interference.

Transnational organised crime

GCSB is a participant in the Police-led New Zealand Transnational Organised Crime Strategy. This strategy strongly aligns with GCSB's key objectives, which include 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. One way we achieve these objectives is by supporting other government agencies, through provision of relevant intelligence.

In respect of Transnational Organised Crime (TNOC), GCSB provides intelligence and technical assistance to the New Zealand Customs Service (Customs) and New Zealand Police. The GCSB has contributed to implementation of the TNOC Strategy and has worked closely with Customs throughout 2021/22 to contribute to the prevention and detection of transnational organised crime. Our focus is on providing intelligence leads that assist Police and Customs to prevent large-scale drug importation.

GCSB's collection and analysis activity has contributed to the understanding of suspected illicit drug trafficking networks affecting New Zealand and the Pacific.

SUPPORTING NEW ZEALAND DEFENCE FORCE (NZDF)

The GCSB continued to provide support to the 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. In August 2021, GCSB provided assistance to NZDF's non-combatant evacuation mission in response to the deteriorating situation in Afghanistan, including providing threat warning for deploying NZDF elements.

CUSTOMER ENGAGEMENT

Following its establishment in 2020/21, the joint Intelligence Customer Centre (ICC) continued to build towards a single team, the purpose of which is to engage and lead the provision of products and services to customers on behalf of the GCSB, Department of Prime Minister and Cabinet's National Assessments Bureau and the NZSIS. The ICC creates an integrated team responsible for intelligence products and services from our three agencies. This means more coordination between the agencies and more capacity for us to tailor to customer needs.

The ICC augmented its presence with a key customer ministry, increasing the frequency and range of in-person intelligence read services, meeting with a very favourable reaction from senior managers. The ICC also undertook a programme of work to simplify and streamline the way our customers receive intelligence reporting, improving the efficiency of disseminating intelligence to customers. The ICC welcomed readers from a number of new customers across government agencies.

On the customer education front, despite impacts of COVID-19 and building occupancy constraints, the ICC improved the Introduction to Intelligence course that it delivers to consumers across government. The improvements resulted in increased collaboration with NZ Defence Intelligence and the Office of the Inspector-General of Intelligence and Security and new sections to the course. Reviews of customer feedback showed that the course is continuing to improve in quality and appeal.

5.0
OUR PEOPLE
Ō MĀTAU TĀNGATA

OUR VALUES

Respect

We respect the role that each individual plays in the organisation. We value diversity in all its forms. 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 and 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.

Beyond the specific responsibilities set out in the Intelligence and Security Act 2017, the Director-General has the following responsibilities (set out in the Public Sector Act 2020):

- Stewardship of the GCSB, including its medium and long-term sustainability, organisational health and capability, and capacity to offer free and frank advice to successive governments;
- Ensuring the performance of the functions and duties and the exercise of the powers of the Director-General of the GCSB;
- The tendering of free and frank advice to Ministers, as well as the integrity and conduct of the employees for whom the Director-General is responsible; and
- The efficient and economical delivery of the GCSB's 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 the GCSB's strategic direction, risk, opportunities, overall work programme, significant organisation-wide policies, major projects, departmental budget and workforce capability and capacity.

In addition to the Director-General, the SLT includes the following roles:

- Deputy Director-General, **Strategy, Governance and Performance;**
- Deputy Director-General, Intelligence;
- Deputy Director-General, **National Cyber Security Centre;**
- **Chief Legal Adviser;**
- Deputy Director-General, **Technology;**
- Deputy Director-General, **Financial Commercial & Support Services**; and
- Chief People Officer, **Intelligence Community Shared Services**.

The roles of Deputy Directors-General Technology, Financial Commercial & Support Services, and the Chief People Officer lead functions that are shared with the New Zealand Security Intelligence Service (NZSIS).

Leadership Development

Equipping and developing leaders as the organisation grows and evolves remains a priority. The New Zealand Intelligence Community (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.

In total our leaders have access to over 15 centrally managed, leadership development opportunities. As at 30 June 2022 more than 58 per cent of our leaders have completed one or more of these core programmes.

RETAIN, DEVELOP AND RECRUIT THE BEST PEOPLE

The GCSB is a public service department with 527.6[1] full-time equivalent staff, as at 30 June 2022.

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.

Throughout 2021/22 the GCSB has continued its focus on retaining the existing workforce and providing opportunities for growth and development.

Recruiting the best people remained a priority throughout 2021/22. The GCSB employs people to fill a wide range of roles, including investigators, case officers, analysts, linguists, technology experts, and other professional and support staff. Over the past year efforts have been focused on ensuring that recruitment resources and processes will result in a more diverse and inclusive workforce.

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.

The GCSB has experienced staff turnover at an unprecedented level over the past year, which reflects the high demand for the expertise and experience our staff have from both the public and private sector. With turnover up to 19.3%, this year we have refreshed our remuneration strategy to respond to unplanned attrition and we have implemented a fresh approach to performance development.

TABLE 1: THE GCSB'S CORE UNPLANNED STAFF TURNOVER (2016 TO 2022)

	2016/17	2017/18	2018/19	2019/20	2020/21	2021/22
Staff Turnover	6.9%	7.1%	12.0%	13.7%	8.1%	19.3%
Public Service	11.5%	12.1%	11.8%	10.1%	10.5%	17.3%

The GCSB supports staff retention through providing significant investment in learning and development and offering career pathways where appropriate. We continue to work with external providers to offer unique and engaging learning experiences for staff.

Another way we recognise, reward, and retain our talented staff is through our Long Service Recognition programme and the Exceptional Achievement Awards.

The awards are aimed at recognising our highest achievers, those that have performed or achieved at an exceptional level, accomplishing outstanding results for our agency, the NZIC, or beyond.

[1] As per the Public Service Commission Full Time Equivalent count

A fresh approach to performance and remuneration

Our 2021 *Kōrero Mai | Tell Us staff survey* results highlighted staff dissatisfaction with our performance management and remuneration frameworks. In line with these findings, and the unprecedented recent levels of turnover, the GCSB and NZSIS jointly commenced a review of our Performance and Remuneration Frameworks.

The review identified market alignment to Central Government median is not appropriate for our agencies. This is because we compete for people with the Public and Private sector. Additionally, bands were behind the market, and are based on 2019 market data, and there was no clear pathway for staff to progress through the bands to a fully competent level once on board.

The review also identified that the performance process needed to mature in order to better support the development of our people and inform remuneration outcomes.

The agencies jointly implemented a new remuneration framework in June 2022. An interim performance system has been implemented for FY22/23 to support the new remuneration framework and pilot concepts to inform the design of our future performance development framework. A long term solution will be designed in collaboration with staff from both agencies over the coming year.

DIVERSITY IN THE WORKFORCE

To achieve our mission, we need people who can think differently, people with different skills and experiences, and people who embrace diversity of thought to solve the problems we face.

This means we need people from a wide range of backgrounds. Diversity and Inclusion (D&I) is essential for better decision making and a key contributor to improving public trust and confidence in the work we do.

In July 2021 the GCSB and NZSIS launched our refreshed D&I Strategy 2021-2025. Increasing representation of women and ethnic diversity at all levels continues to remain a priority for us.

Our refreshed strategy builds on the great work we've done, and aspires to take it to the next level. Our first strategy was focused heavily on increasing our diversity. We learnt that recruiting a diverse workforce is not enough – an inclusive environment is essential to retain that diverse talent. That's why our refreshed strategy places a stronger emphasis on inclusion.

Gender Diversity

As at 30 June 2022 women made up 63.2% of the GCSB's senior management. We have continued to successfully meet our diversity and inclusion aspiration of women forming no less than 50% of our senior management group.

TABLE 2: THE GCSB'S GENDER REPRESENTATION (2016 TO 2022)[2]

	2016/17	2017/18	2018/19	2019/20	2020/2021	2021/22
Senior Management (Tier 2 and 3)						
Men	40.0%	42.9%	48.0%	54.5%	47.8%	36.8%
Women	60.0%	57.1%	52.0%	45.5%	52.2%	63.2%
All Staff						
Men	63.6%	62.4%	63.8%	64.4%	64.5%	61.1%
Women	36.4%	37.6%	36.2%	35.6%	34.9%	37.9%
Another Gender	-	-	-	-	0.2%	0.2%
Undisclosed	-	-	-	-	0.4%	0.8%

One of the key goals in our *2021–2025 D&I Strategy* is to increase our representation of women by 1 percentage point a year (4 percentage points by 2025). We have successfully achieved our yearly goal, increasing our representation of women significantly by 3 percentage points (34.9% to 37.9%) compared to last year.

The GCSB has a range of initiatives in place to recruit women and is actively fostering external connections to support the development of technical capabilities our agency, and New Zealand, needs for the future. This includes initiatives such as our Women in STEM scholarship graduate programme, which are all key to our efforts in improving the representation of women

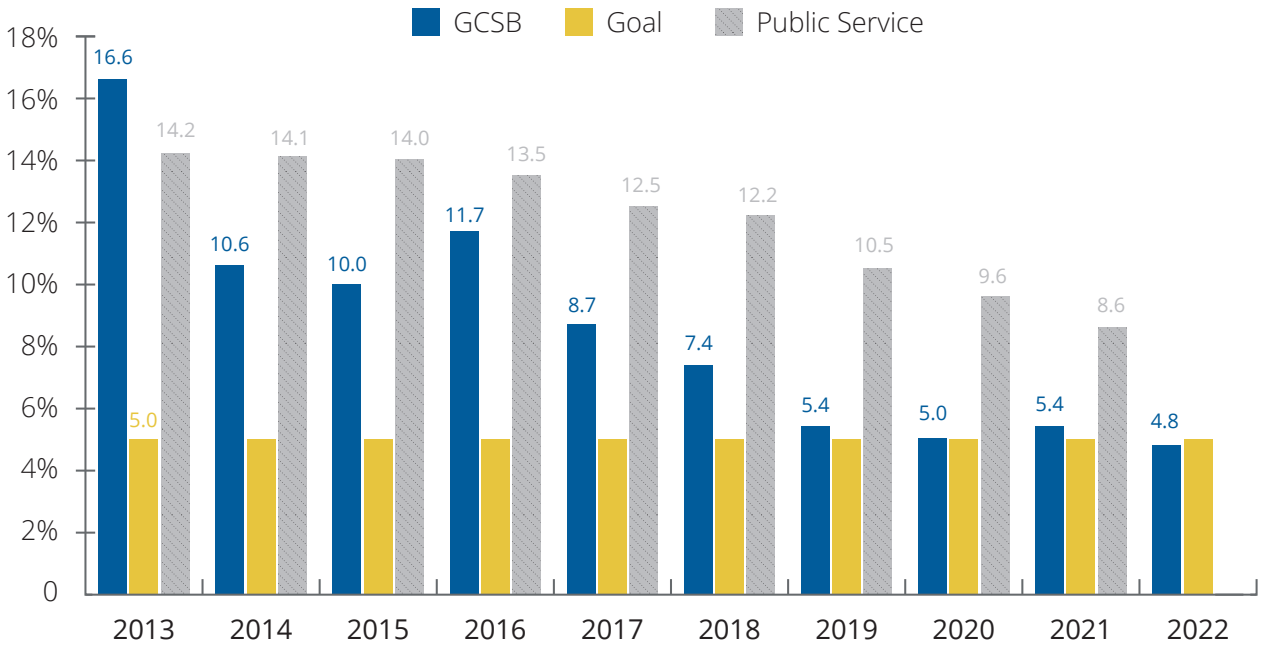
[2] This year we have aligned ourselves with Te Kawa Mataaho's definition of Senior Management. This means all Tier 2 and 3 people managers will now be included as "Senior Management" in workforce data metrics.

in the GCSB. More information on these initiatives can be found further below.

We have eliminated the gender pay gap for like for like roles and met our current goal of an average gender pay gap of 5% with the pay gap down to 4.8%. This is a 0.6% decrease from last year and a 6.9 percentage point decrease since 2016. We continue to have a significantly lower gender pay gap when compared to the Public Service average (8.6%).

Our median gender pay gap (6.8%) is 2.3 percentage points lower than New Zealand's (9.1%)[3].

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.



Our Gender Pay Gap Action Plan incorporates four core milestones:

- Equal pay
- Flexible work by default
- There is no bias or discrimination in remuneration systems and human resource practices
- Gender balanced leadership.

Actions underpinning these core areas align with our *D&I Strategy 2021-2025*. We have made, and continue to make, steady progress towards these goals. The GCSB has established a new Flexible Working Policy (and associated online training), and we continue to work on identifying and mitigating bias and discrimination in all practices.

[3] As per Stats NZ Labour market statistics (income): June 2021 quarter

We will be developing our first annual pay gap action plan under Kia Toipoto – the Public Service Gender, Māori, Pacific and Ethnic Pay Gap Action Plan. This action plan will build on our previous published gender pay gap action plans, focussing strongly on gender/ethnicity data and union/employee participation. This action plan will be released in November 2022.

Ethnic Diversity

Increasing the ethnic diversity across the GCSB is another key focus of our *D&I Strategy 2021-2025*. We aim to increase the ethnic diversity of our workforce by 1 percentage point every year (4 percentage points by 2025). We have surpassed our yearly target, increasing our ethnic diversity by 3 percentage points. Our two largest increases were in Māori representation (1.9 percentage point increase) and Pacific Peoples representation (0.8 percentage point increase).

92.7% of our workforce have disclosed at least one ethnicity which exceeds our 90% targeted disclosure rate for robustness of analysis. One of the focus areas in our upcoming 2022 Pay Gap Action will be improving the disclosure rate of staff who identify with multiple ethnicities and providing clear communication to staff on the purpose and importance of collecting this information.

We will continue to implement our D&I Strategy which will ensure we have diverse talents, views and thinking, which is critical to achieve our mission.

TABLE 3: THE GCSB'S STAFF ETHNICITY (2016 TO 2022)[4]

	2016/17	2017/18	2018/19	2019/20	2020/21	2021/22
NZ European & European	68.7%	67.6%	67.8%	71.2%	76.0%	74.6%
New Zealander	N/A	27.5%	29.4%	26.8%	22.8%	18.5%
New Zealand Māori	7.2%	7.8%	7.2%	7.3%	7.2%	9.1%
Asian	5.4%	4.9%	5.4%	5.5%	7.2%	7.3%
Pacific Peoples	1.8%	2.8%	2.3%	1.6%	2.6%	3.2%
MELAA	0.3%	0.3%	0.9%	1.1%	1.2%	1.6%
Other[5]	-	-	-	-	0.2%	0.2%

We are in the early stages of analysing and understanding our ethnic pay gaps. This will be another focus area of our 2022 Pay Gap Action Plan under Kia Toipoto.

[4] These metrics cover the number of employees who identify themselves as having a certain ethnicity. They are calculated by taking the number of people who identify themselves as being in the ethnic group divided by the number of people who have provided an ethnicity. A person may identify with multiple ethnicities. This means the total of all percentages can add up to over 100%. Metrics are taken 'as at 30 June' of the relevant year.

[5] Staff who have self-identified their ethnicity as "New Zealander" have been excluded from "Other" and reported as their own group.

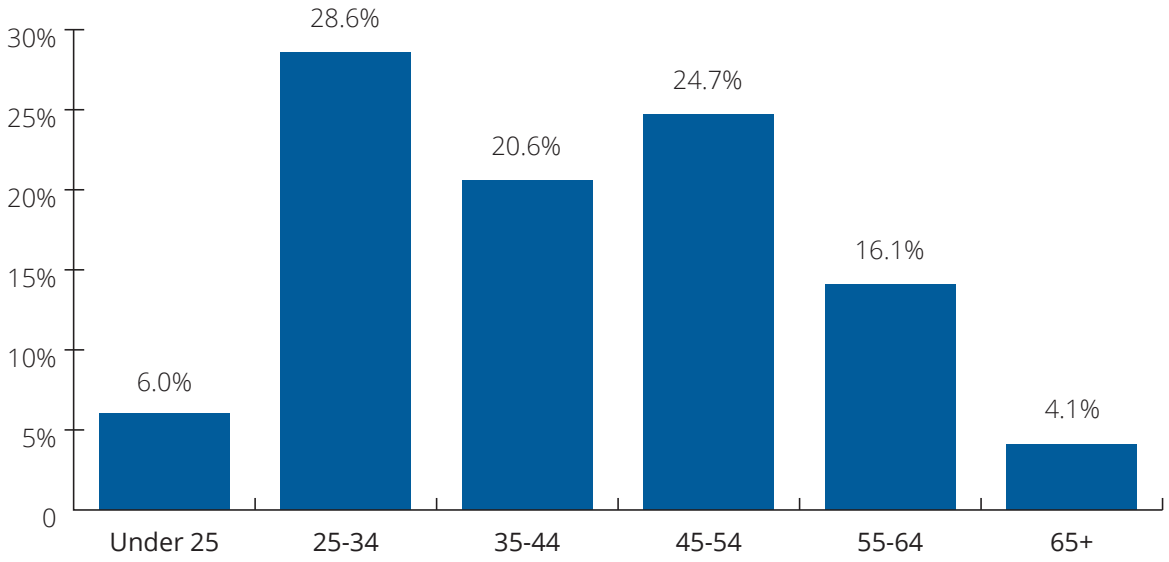
TABLE 4: THE GCSB'S ETHNIC PAY GAPS (30 JUNE 2022)[6]

ETHNIC GROUP	AVERAGE
European	-5.5%
New Zealand Māori	4.6%
Asian	6.2%

European is the only ethnicity with a negative average ethnic pay gap (in favour). This means on average non-Europeans are earning 5.5% less than Europeans. Of the three groups with sufficient numbers for statistical robustness, Asian has the highest average pay gap. On average non-Asians are earning 6.2% more than Asians. As we dig deeper into analysing our ethnic pay gaps to find causes and solutions, we will also look at median ethnic pay gaps and how gender and ethnicity intersect.

Age Demographics

The majority of our workforce are less than 45 years old (54.2%).This is reflective of our average tenure and age (6.5 years and 42.8 years). Our average age has decreased slightly by 0.2 years and our average tenure has increased by 0.1 years. Of our staff under 35, 75% have started in the last four years. 12 years is the average tenure for our staff who are 65 years and older.



[6] Pacific Peoples, MELAA and Other have been excluded as the number of staff identifying with this ethnicity is under the number needed for statistical robustness. An ethnic pay gap measures the difference between the average (or median) salary for an ethnic group and average (or median) salary of all those not in that ethnic group, expressed as a percentage of the average (or median) salary of those not in the ethnic group.

PROGRESS AGAINST PUBLIC SERVICE COMMISSION PAPA POUNAMU COMMITMENTS

In mid-2021 we reviewed our D&I learning pathway for leaders and staff across the NZIC. The purpose of this was to ensure our expectations for completing essential learning considered aspects such as pre-existing experience and operational workload of all staff.

As a result of this review we split out the learning into 'leadership' and 'essential'. Within 'essential' we now have specific D&I learning alongside other essential learning (e.g. compliance) that our people have to complete.

The four categories of learning within this pathway include; Health & Wellbeing, Inclusion, Language & Culture, and Values & Ethics. Key topics within these categories are outlined within the following sections.

Addressing bias

In our refreshed *D&I Strategy 2021-2025* we have specific objectives that relate to bias and discrimination. Over the next four years we have committed to:

- Review how we approach recruitment to identify ways we can eliminate bias and break down barriers to entry.
- Gender and ethnicity data analysis at different stages of the employment lifecycle.
- Review people policies to identify opportunities to make them more inclusive.
- Review forms, systems, and processes, and update where required to ensure D&I is incorporated.
- Incorporate D&I into our performance framework and organisational values.

Our *Understanding & Managing Unconscious Bias* eLearning module continues to be our primary learning resource to support staff knowledge around what bias is and how to manage it. 78.5 per cent of our leaders have either completed this learning in a former face-to-face workshop or online.

Additionally, in October 2021 our *Bias in the Selection Process* eLearning module was launched for all staff to complete before participating on recruitment panels. This is monitored by our Recruitment Advisors who have noted a 100 per cent completion rate for panel members.

Cultural competence

Developing a strategic approach to Māori cultural capability for the GCSB and NZSIS is critical to recognising the place of Māori as tangata whenua and to our role in supporting the strengthening of the Crown's relationship with Māori.

In collaboration with our new Chief Advisor Māori, Learning and Development have committed to a 12 month plan to design and develop learning resources within five key areas of Te Arawhiti's Māori Crown Relations Framework; New Zealand History and the Treaty of Waitangi, Worldview Knowledge: Te ao Māori, Te Reo Māori, Tikanga/Kawa, and Understanding Racial Equity and Institutional Racism.

These resources include developing new resources as well as redesigning existing materials.

Additional information on learning completion rates can be found in areas 2 and 3 of our Māori cultural capability section below.

Inclusive leadership

The GCSB offers a range of leadership development opportunities tailored specifically to the needs of leaders within the Public Service. These include in-house learning activities, the range of Leadership Development Centre programmes and other externally provided offerings.

In addition to specific leadership programmes, our D&I learning pathway helps leaders recognise and mitigate bias, value diversity and foster inclusivity in the workplace, through a range of learning opportunities which encourage inclusive leadership.

Employee-led networks

We have established staff networks to support the breadth of diversity across the workplace. At present we have seven networks:

- Women in the New Zealand Intelligence Community
- Women in Technology
- Standing Out
- Kahikatea
- Military Support Network
- Tagata Pasefika in Intelligence Network (TPIN)
- Neuro-divergence Support Group

Each network is assigned their own budget, giving them the autonomy to drive their own initiatives. Staff networks contribute to, and deliver many initiatives including policy development, D&I events, internal celebrations, guest speakers, D&I training, networking functions, and conferences.

Our newest networks include TPIN and our Neurodivergent Support Network. TPIN saw a real need for our Pasefika people and realised they were in a unique position to support our agencies' work. Our Neurodivergent Support Group established itself in May 2022 and provides a safe space for staff who identify as neuro-divergent, somewhere members can share their challenges and get support from peers.

Our staff networks are crucial to driving our D&I agenda, and play an important part in shifting culture from the ground up. While each of our staff networks has a specific focus, the actions and initiatives they implement benefit a wide range of people.

Building relationships

To support inclusivity across our workforce we have provided a number of tools, resources, and opportunities for our people. These include:

- access to an internal Psychology Services team who actively promote their services and are readily available to all staff;
- team profiling services so teams and leaders can better understand and embrace individual work preferences, styles, and motivations;
- active engagement with staff associations to inform policy development and implementation;
- a D&I Advocacy Group, chaired by both Directors-General, for staff networks to represent their D&I challenges and opportunities;
- development of a new psychosocial wellbeing framework for staff working in high-risk functions;
- open sharing of Kōrero Mai results with leaders and staff so they can collectively celebrate successes and address improvement areas; and
- a new interim performance development process for 2022/23 that's focused on regular, conversational style performance reporting.

DIVERSITY AND INCLUSION HIGHLIGHTS

Rainbow Tick re-accreditation

The GCSB, jointly with the NZSIS, embarked on our first Rainbow Tick accreditation process in 2019 and were re-accredited in August 2021. Results from the reaccreditation process showed we met the Rainbow Tick standards in five key areas – Strategy and Policy; Staff engagement and Organisational Support; External Engagement; Organisational Development; and Monitoring; and in some cases demonstrated significant improvement from our first accreditation.

2021 Rainbow Excellence Awards

In 2021 we nominated our own Chief People Officer, Shelly Thompson for the Leadership and Ambassador categories of the Rainbow Excellence Awards. Shelly's leadership, advocacy, commitment and drive shone through with her winning the Chorus Ambassador Award. This Award recognises internal heroes and role models in formal and informal leadership positions who are actively driving improvements with rainbow inclusion.

Shelly was also a finalist in the Newmarket Business Association Executive Leadership Award category. In addition to this, we were a finalist for the Westpac Supreme Award, which the GCSB and the NZSIS won in 2020.

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.

In 2021 we ran our own internal *Kōrero Mai | Tell Us staff survey*. Our Kōrero Mai findings showed strong results in the areas of psychological safety and inclusion. The statement 'I feel supported in the workplace when I am dealing with personal or family issues' rated 79% for the GCSB - the second highest scoring statement for our agency. 'I feel included in my team' was the third highest scoring statement (76%) for the GCSB. The fourth highest rated statement 'My line manager considers psychological wellbeing to be as important as productivity' rated 74% for the GCSB.

The GCSB also participated in the 2021 Te Kawa Mataaho | Public Service Commission Census. The results from this Census further support our progress. 92% of the GCSB's respondents believe the agency supports and actively promotes an inclusive workplace, 85% feel they can be themselves at work, and 86% feel accepted as a valued member of the team. The score in relation to 'agency supports and actively promotes an inclusive workplace' were significantly higher than the Public Service average of 78%.

2022 Diversity Works Awards

In June the GCSB alongside the NZSIS were named finalists for the Leadership category in the Diversity Works Awards. This award will be given to an organisation which demonstrates how they equip their leaders to create environments of inclusion for all employees.

Being a finalist is another acknowledgement of the progress we're making in building a diverse and inclusive community. Winners will be announced in August 2022.

The GCSB Graduate Programme

A key part of growing the pipeline of talent and ensuring the ongoing resilience of the GCSB workforce is the graduate programme. Throughout 2020/21, the GCSB has been working hard to attract more diverse candidates, including people from diverse communities, and more female candidates.

The graduate programme runs for 16 months and looks for people with strong skills and an interest in engineering (software, systems, network), computer science, data science, telecommunications, network analysis and/or cyber security. Graduates rotate through different parts of the GCSB, giving them more opportunity to learn and experience the wide range of work we do, before being appointed to a permanent role at the end of the programme.

For the 2022/23 graduate recruitment intake (Intake 9.0), the GCSB received 41 applications, of which 11 (27 per cent) were female and 22 (54 per cent) were ethnically diverse.

The lower proportion of female applicants applying for the graduate programme is reflective of women being underrepresented in science, technology, engineering, and mathematics (STEM) fields both domestically and internationally. To help encourage more women into STEM careers, the GCSB participates in external outreach opportunities to attract women studying STEM disciplines. The GCSB also has a Women in STEM scholarship.

The GCSB Women in Science, Technology, Engineering, and Mathematics scholarship

Our Women in STEM scholarship started in 2017. The scholarship programme is aimed at second-year and above tertiary students who are undertaking STEM disciplines at New Zealand tertiary institutions. We award up to three scholarships per year, with at least one being awarded to a Māori/Pasifika student.

Winners have come from a range of disciplines including cyber security, mathematics, physics, data science, computer science, and engineering. Since 2017 we have awarded 18 scholarships to women throughout New Zealand, and hosted five STEM Scholarship events in-house. The in-house event is an opportunity for the top scholarship finalists (10-12 students, including the winners) to learn more about the GCSB, and the wide range of STEM-related career opportunities we can offer.

This year we received a total of 57 applications from across all of New Zealand's universities. The calibre of applicants was extraordinary, and four scholarships were awarded. Our four winners represented a number of different ethnicities, two of whom were of Māori/Pasifika descent.

Between 2018 and 2021 we have awarded, on average, 50% (7/14) of our scholarships to people of Māori or Pasifika descent.

In the last three graduate programme intakes we've appointed a number of scholarship finalists and winners. It's now creating a clear pipeline of diverse talent into our graduate programme.

Health, Safety and Wellbeing

Providing a safe and healthy working environment is pivotal to the NZIC. We take a pragmatic approach to health and safety, while ensuring that we are complying with the Health and Safety at Work Act 2015.

Priorities during 2021/22 were the ongoing training and education provided to staff and managers on health and safety matters, improvements with our hazard management framework and working safely.

We continue to focus on wellbeing and supporting our people through COVID-19. Throughout the pandemic we have responded quickly and provided ongoing and frequent communication to our people to minimise the impact. The lessons we learnt during 2020 help us respond quickly and effectively with the deployment of incident response management as the pandemic continues to ensure not only the ongoing wellbeing of our staff but the continued delivery of critical functions.

During 2021/22 we continued to review our health, safety and wellbeing requirements and have redirected resources to further invest in the ongoing safety and capability of our people, including growth within the Health, Safety and Wellbeing team. Continuous growth of Health and Safety Representatives (HSR) has been prioritised. We have approximately 55 trained HSRs advocating for good health, safety and wellbeing outcomes across the NZIC.

We have also undertaken a review of our Health and Safety Policy ensuring we are incorporating the Health and Wellbeing components sufficiently to ensure the ongoing wellbeing of our workforce. A core element of work which commenced, and will rollover into 2022/23, is the development of a Psychosocial Framework for high risk roles.

During this 2022/23 period there were no lost time injuries reported and no notifiable incidents or events reported to WorkSafe New Zealand.

6.0
MĀORI CULTURAL CAPABILITY
TE WHANAKETANGA O TE AO MĀORI

Tirohia te pae tawhiti, whāia rawatia kia tata, whakamaua kia tīna.

Seek out distant horizons, draw them near, cherish and hold fast to those in which you attain.

Nau mai te mātahi o te tau me ōna tini hua

This year NZIC welcomed and embraced the goodness of Matariki, a signal of hope and the promise of good year. Matariki encouraged us to reflect on the year that was, and in doing so, reminded us of our cultural uplift journey which started in early 2021. Throughout our discovery phase we identified the need to develop a strategic approach to Māori cultural capability for the GCSB and NZSIS; acknowledging that it was critical to recognise the place of Māori as tangata whenua and our role in supporting the Government to fulfil its stewardship responsibility to strengthen the Crown's relationship with Māori.

THE BEGINNING OF OUR JOURNEY

During our discovery phase our agencies undertook a maturity assessment against Te Arawhiti's Māori Crown relations framework and as a result a combined agency maturity model was developed and implementation initiated with the appointment of a Chief Advisor Māori in February 2022.

Although we are at the infancy of our journey our community have enjoyed some wins along the way:

- the awareness of staff hearing leaders inter-weave kupu Māori within everyday business, helping normalise it;
- the inter-weaving of Te Reo Māori within our official documents, job descriptions, internal and external communications;
- significant uptake of staff aboard the Māori Crown relations training;
- significant uptake of staff in Te Reo Māori classes;
- participation of staff in waiata classes;
- development of interactive Pepeha tool;
- development of interactive Matariki tool.

With cultural expertise on-board we have set the direction and look ahead to seek out the horizons and pursue drawing them near. Our agencies will soon enter into an exploring phase that will help build solid foundations and enable us to set our narrative, articulate our roles and responsibilities under Te Tiriti o Waitangi, and develop our Te Ao Māori framework and strategy.

As we prepare for this exciting phase ahead, we reflect on our past year under three key areas:

- Te pae tawhiti
- Whāia kia tata
- Whakamaua kia tīna

TE PAE TAWHITI
DISTANT HORIZONS

Our hopes and aspirations in terms of our communities' journey to uplift our cultural capability.

The NZIC is committed to building greater understanding and incorporation of te ao Māori, te reo Māori, tikanga and te Tiriti throughout our day to day activities and interactions. Our intent for 2021/22 was to lay the foundations required to make this possible:

- securing Māori cultural expertise to guide and enable our journey
- communicating our intended path and role modelling the desired capability at all levels of leadership
- increasing learning experiences to develop Māori cultural competency development
- confirming the measures that will help us track our Māori cultural capability journey.

WHĀIA KIA TATA
PURSUE AND DRAW NEAR

How our progress tracks against the objectives set.

The initial maturity assessment identified the need to take time to lay the foundations for improved cultural capability. The first year has focused on sourcing the best possible Te Ao Māori expertise to guide the journey and to build on existing efforts. This included expanding our te reo and cultural capability offerings to support our people's development and adjusting our recruiting practices to be more inclusive of our commitment to Māori.

Two further positions have been established to support this work programme in order to expand the range of learning and development offerings available to our people and, broadening the use of te reo in position descriptions and recruitment advertising. The two new roles is another signal of NZIC's strong commitment to this journey.

The agencies had intended to confirm and communicate its cultural capability plan during the reporting period. This was not achieved but we are well position to begin these discussions this year.

The goal for 2022/23 is to finalise and communicate our direction, and to gather the resources we need to support our journey. In particular this will include:

- Recruiting two roles to form the NZIC Māori Cultural Advisory function (Te Ao Māori team)
- Defining and launching our Te Ao Māori framework and strategy which will provide a segway into the development of formal plans that will uplift our overall capability.

Our framework will be underpinned by Te Tiriti and seek to:

- Communicate our narrative and Treaty (maturity) journey clearly
- Declare our commitment to honouring Te Tiriti
- Align with Strategy, our people, the services we provide and the work we do
- Provide a reference point for stakeholders to understand and meaningfully engage
- Effectively communicate the NZIC's roles and responsibilities under Te Tiriti
- Provide a reference point for leaders and core business areas to align
- Acknowledge skills, capabilities and resources needed to ensure the NZIC is prepared for its roles and re responsibilities.

Whāinga Amorangi

Our organisational development plan for 2021/22 focused on moving our organisation from Unfamiliar to Comfortable as described by Te Arawhiti's Māori Crown Relations Capability Framework.

We focused on increasing capacity for our Crown Māori Relations programme and identifying a complementary online programme for non-leaders. Seven programmes were delivered this year providing 112 staff for our staff. An online version has been developed and is in the final stages of review.

65.3% of the GCSB's leaders have completed the Crown Māori Relations programme.

While we weren't able to complete all actions within our Māori language plan, we have made progress in promoting opportunities and engaging our staff in activities to develop their te reo Māori.

WHAKAMAUA KIA TĪNA
HOLD FAST TO THOSE OF WHICH WE HAVE ATTAINED

Objectives we have achieved and celebrate.

Matariki

Nau mai Matariki me ōna hua nui.

NZIC paused to recognize the significance of Te Kāhui o Matariki Public Holiday Bill by celebrating this auspicious occasion in style. Across the week leading up to the public holiday we provided daily informative learning that covered various aspects of Matariki, its significance, meaning and ways in which we can celebrate. We developed a Matariki interactive tool enabled staff to grow their understanding of Matariki, the meaning of each star, how to find the cluster and the appropriate terminology when greeting others to say happy Māori New year. We celebrated across our offices with traditional hāngī taking a moment to reflect and plan ahead for the future.

Māori Language Plan

The GCSB and NZSIS 2021/22 Māori Language plan identified a range of activities including providing all staff with opportunity to learn te re Māori, supporting te reo Māori events, and ensure leaders are learning te reo and drive success of reo initiatives.

Over the past three years the GCSB and NZSIS have prioritised providing all staff opportunity to learn te reo Māori and senior leaders role modelling the use of te reo day-to-day. This evidenced in the findings of the Te Tuanaki/Public Service Census 2021/22.

- 72% of the GCSB respondents hear leaders speaking te reo Māori
- 79% of the GCSB respondents recognise the support available to improve their own te reo Māori.

Te reo classes are provided jointly to the agencies and encompass Te Reo Levels 1-13. In 2021/22, 41 people completed one or more te reo programmes. 40% of Level 1 participants have gone on to join Level 2 classes, and 90% of Level 2 participants went on to join Level 3 classes.

There are currently 49 people waitlisted for te reo Level 1 in 2022/23.

In September we celebrated Te Wiki o Te Reo Māori with daily promotion of learning resources under the themes of listen, speak write and join. These included Waiata group performances, seminars where rangatahi Māori spoke about their journey with te reo Māori, a guide to learning your mihi, key board cheats for macrons and links to official Te Wiki o Te Reo Māori resources.

Te reo Māori coaching relationships have been established for a number of our Senior Leadership team members. Both the use of coaching for development and use of te reo day to day is openly role modelled by our Director-General.

Our agency's mission, vision and values were translated for use in our position descriptions and translations for common role titles identified.

Where we are heading

Whilst our community acknowledge we may be at the beginning of our journey, we are excited by what is ahead as we embark on shaping, shifting and strengthening our movements to seek out the distant horizons. We look forward to uplifting our collective cultural capability to increase our communities' understanding of and ability to apply te ao Māori, reo Māori, tikanga and mātauranga Māori to the way we work.

7.0
FINANCIAL STATEMENTS
NGĀ TAUĀKĪ PŪTEA

STATEMENT OF RESPONSIBILITY

I am responsible, as Director-General of the Government Communications Security Bureau (GCSB), for:

- the preparation of the GCSB's financial statements, and the statement of expenses and capital expenditure, and for the judgements expressed 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 annual report fairly reflects the operations, progress, and the organisational health and capability of the GCSB;
- the financial statements fairly reflect the financial position of the GCSB as at 30 June 2022 and its operations for the year ended on that date; and
- the forecast financial statements fairly reflect the forecast financial position of the GCSB as at 30 June 2023 and its operations for the year ended on that date.

Andrew Hampton
Te Tumu Whakarae mō Te Tira Tiaki
Director-General of the GCSB
Government Communications Security Bureau

30 September 2022

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 2022

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 2022 on page 70.

Opinion

In our opinion the statement of expenses and capital expenditure against appropriation of the GCSB for the year ended 30 June 2022 is presented fairly, in all material respects, in accordance with the requirements of section 221(4)(a) of the Intelligence and Security Act 2017.

Our audit was completed on 30 September 2022. 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 and Supplementary Estimates of Appropriations 2021/22 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.

AUDIT NEW ZEALAND
Mana Arotake Aotearoa

Other information

The Director-General of the GCSB is responsible for the other information. The other information comprises the information included on pages 5 to 66, but does not include the information we audited, and our auditor's report thereon.

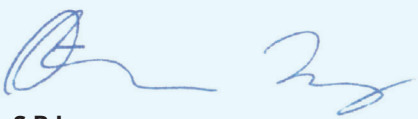
Our opinion on the information we audited does not cover the other information and we do not express any form of audit opinion or assurance conclusion thereon.

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

STATEMENT OF EXPENSES AND CAPITAL EXPENDITURE AGAINST APPROPRIATION

FOR THE YEAR ENDED 30 JUNE 2022

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

	$000
Total appropriation	248,483
Total expenditure	182,441

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.

Te Tira Tiaki
Government Communications
Security Bureau