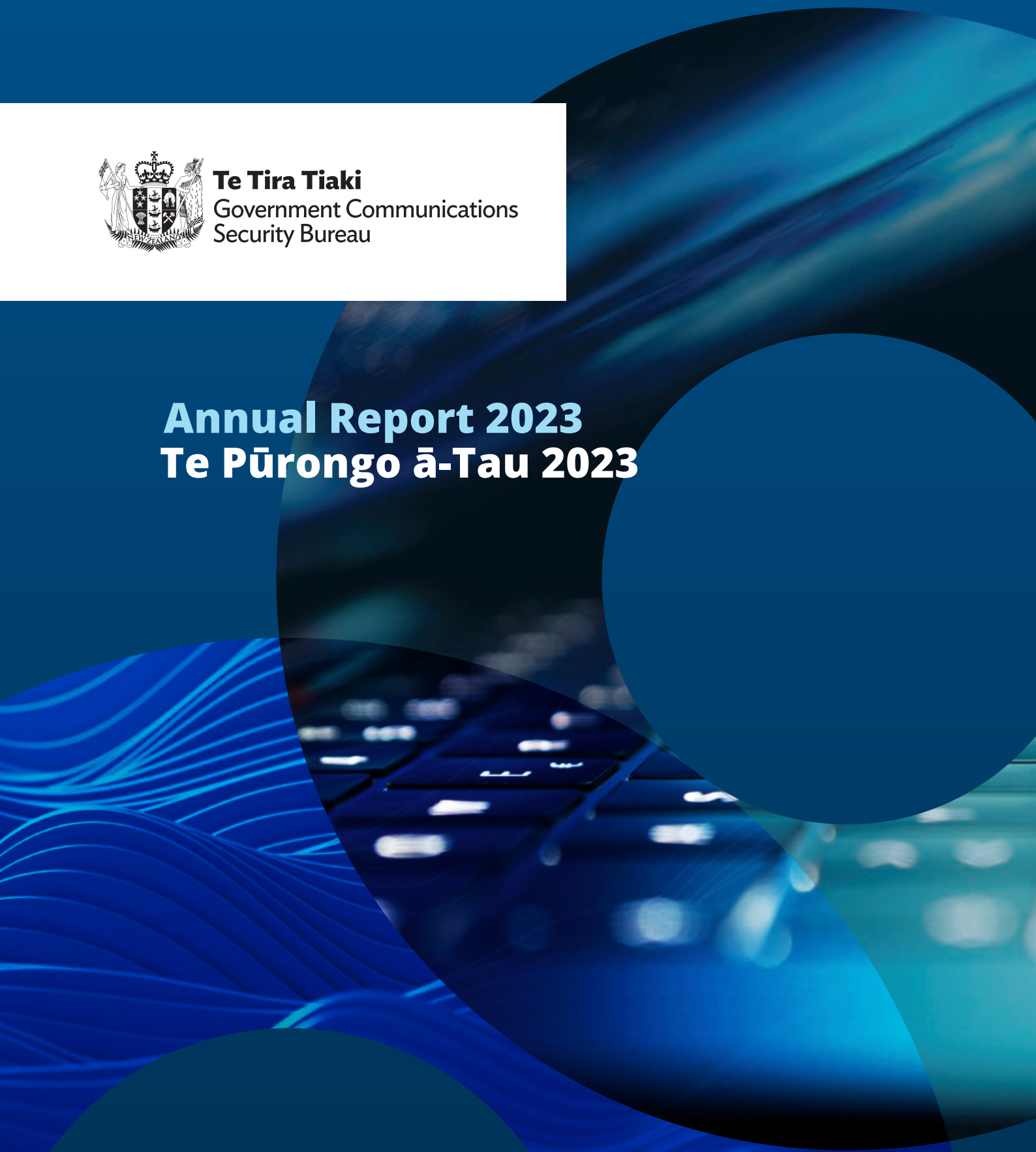
G.56 (2023)

Te Tira Tiaki
Government Communications Security Bureau

Annual Report 2023
Te Pūrongo ā-Tau 2023



GCSB.GOVT.NZ

Preface

This is the annual report of the Government Communications Security Bureau (GCSB) for the year ended 30 June 2023, 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
NGĀ IHIRANGI

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

The publication of this annual report is again set against a turbulent international backdrop. As the global community begins to move beyond the disruptions of the Covid-19 pandemic, we continue to operate in a complex and challenging threat environment. Russia's illegal and unprovoked invasion of Ukraine is ongoing, while global geopolitical tensions continue to intensify, including in our Pacific region.

These pressures are placing extraordinary and unprecedented pressure on the international rules-based architecture that Aotearoa New Zealand, as a small trading nation, relies upon to maintain order, peace and stability.

The Government Communications Security Bureau (GCSB) is New Zealand's lead for signals intelligence (SIGINT) and provides intelligence to government customer agencies. It is also the lead, through the National Cyber Security Centre (NCSC), for cyber security for organisations of national significance. Our mission is to provide our customers with intelligence advantage and cyber resilience to successfully navigate an unpredictable world.

Given the current geopolitical environment, it is no surprise both our SIGINT and cyber security missions have responded to high operational demand in the past year.

Peace and stability in the Pacific has been an enduring intelligence focus for the GCSB, and our Pacific mahi is more important now than ever as the region becomes more contested. Our Pacific intelligence and security advice is helping shape policy decisions and we will continue to inform our government customers on the shifting geopolitical tides in our region.

Beyond the Pacific, our SIGINT contributes towards global counter-terrorism efforts, and we continue to actively contribute more towards domestic counter-terrorism measures led by partner agencies, the New Zealand Security Intelligence Service (NZSIS) and New Zealand Police.

In the cyber security domain, the number of incidents we see affecting organisations of national significance remains consistent with previous years, as the malicious cyber activity we face continues to be more sophisticated and more impactful. Malicious cyber actors seek new ways to infiltrate weak supply chains, and severely impact service delivery and information security, at a time when there is increasing global reliance on complex shared delivery systems.

Both state-sponsored and financially motivated cyber criminals continue to target New Zealand's national digital infrastructure. In May 2023, we joined our international partners to highlight two incidents of malicious cyber activity, attributed to Russian Federal Security Service and People's Republic of China state-sponsored actors respectively. We published advisories on each occasion, outlining steps cyber defenders could take to mitigate the activity.

The positive impact our Malware Free Networks® (MFN®) service has had on New Zealand's cyber threatscape received acclaim this year, winning the 2023 Te Hāpai Hapori Spirit of Service Award for Service Excellence, as well as winning the overall Prime Minister's Award. MFN also received industry recognition as winner of "Best Security Product or Service" at the annual iSANZ cyber security industry awards in November 2022.

Building on the success that collaboration brings, we provided advice to Cabinet around the integration of CERT NZ with our NCSC to create a single operational lead for the Government's cyber security capability.

Sharing strengths in partnerships to protect New Zealand's national security, including the safety and security of New Zealanders, is particularly important in our current geostrategic context. The GCSB, along with the NZSIS hosted a Five Eyes conference in September 2022, which included high-level discussions on a range of matters critical to New Zealand's national security and that of our wider region.

On the topic of working together, we have partnered with the New Zealand Defence Force to construct an all-of-government data centre at Royal New Zealand Air Force Base Auckland (Whenuapai) to house New Zealand's sensitive official information. As the government's information security lead, we will operate the data centre on behalf of a range of government agencies. The data centre is expected to be operational by 2025, and will provide data storage for agencies for at least 25 years. Construction on the facility began in 2022, and was publicly announced in April 2023 by the Minister Responsible for the GCSB, Hon Andrew Little, after security milestones had been achieved.

As the head of the GCSB, I hold the statutory role of the Government Chief Information Security Officer (GCISO), which is responsible for the strategic direction of the Government's approach to information security. This reporting year we have seen public discussion around the availability of mobile phone apps on government devices and the security of technology in government infrastructure.

The advice we provide is country and vendor agnostic, but includes a prerequisite for agencies to carry out due diligence and mitigate any risk identified when considering the use of any new platforms, services or apps. The GCSB received funding from Budget 2023 to enhance the GCISO function to deliver strengthened cyber resilience of critical national infrastructure through the NCSC.

The seismic strengthening remedial work at Pipitea House on Pipitea in Wellington has been completed, with the building now back to full occupancy. The last few years presented their share of challenges for business continuity, with the building disruptions a significant one. I do want to acknowledge our people, who showed enormous resilience throughout to fulfil the GCSB's core missions. Our capability indeed relies on the combination of GCSB's highly skilled workforce, as well as our technological ascendency, unique legal mandates, and our international and domestic partnerships.

Our greatest asset is indeed our people. The GCSB have for some years been on a journey to attract and retain the very best, and grow our diversity and inclusion. We recognise diversity and inclusion is essential for better decision making and a key contributor to improving public trust and confidence in the work we do.

This work is being recognised. In November 2022, together with the NZSIS, we won the Diversity Works Leadership award in the medium to large-sized organisation category. This is an achievement we are proud of, and builds on our New Zealand Supreme Rainbow Excellence Award, which we also won with the NZSIS in 2020.

We are also proud to have introduced Te Tiriti o Waitangi into our organisational strategy this year. This is a step towards recognising how Māori values should apply to the GCSB's work, and becoming a member of a culturally responsive community.

You will see we have included nine puzzles throughout our report this year. The skills involved in solving puzzles apply to many of our roles, and we actively look for these skills through our recruitment. Puzzling is also a form of problem solving. Our people are finding solutions to difficult problems every day, regardless of whether they are a good puzzler or not. We hope you have as much fun contemplating these as we did crafting them.

Following the end of this reporting period, we welcomed Andrew Clark to the role of Director-General of the GCSB in October 2023. We are very pleased to have Andrew with us.

Finally, I would like to acknowledge the enormous contribution former Director-General Andrew Hampton made to the GCSB in his seven years leading the organisation.

Andrew, who in April 2023 took up the role of Director-General of the NZSIS, steered the GCSB through a period of great change – including a scaling up of the organisation and driving greater public transparency.

Bridget White
Te Tumu Whakarae Rangitahi mō Te Tira Tiaki

Acting Director-General of the Government Communications Security Bureau

#2

														1				
												1		1				
												1		1				
												1	1	1				
				1					1			1	1	1	1			
		1	1	1			1	1	1			3	3	1	3			
		1	1	1	1		1	1	1	1		1	1	1	1			
		3	1	2	3		3	1	2	3		1	1	1	1			
		1	1	2	3		1	1	2	3		1	2	1	1			
		1	1	1	1		1	1	1	1		1	3	1	3			
		1	1	1	1		1	1	1	1		1	1	2	1			
		1	3	1	1		1	3	1	1		1	2	1	1			
		1	2	1	3		1	2	1	3		3	1	1	1			
		1	1	1	1		1	1	1	1		1	1	1	3			
	1	3	1	1	1	1	3	1	1	1	1	1	3	1	1	1		
36	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	36	

18							
1	1						
1	1	1					
1	4	1					
1	1	1					
1	1	1	1				
1	4	4	3	1			
1	1	1	1	1	1		
1	3	1					
1	1	1	1	1	1		
1	4	4	4	1			
1	1	1	1	1	1	1	
1	4	1					
1	4	4	1				
1	1	1	4	1			
1	1	1	1	1	1		
1	1	1	1	2	1		
1	4	4	1				
1	3	1					
1	3	3	1	1	1		
1	1	1	1	1	3	1	
1	3	3	1				
1	4	1					
1	4	4	1	1			
1	1	1	1	1	1	1	
1	1	2	1	2	4	1	
1	1						
1	4	4	4	1			
1	1	1	1	1	1		
1	4	4	2	1	1		
1	1						
1	3	1					
1	1	1	1				
1	3	1					
1	1						
18							

Who We Are and What We Do

Ko wai mātou, ā, he aha hoki ā mātou mahi

OVERVIEW
TIROHANGA WHĀNUI

Mission

The GCSB is Aotearoa New Zealand's lead organisation for signals intelligence (SIGINT), cyber security, and cyber resilience. Our mission is to equip our customers with the intelligence and cyber resilience necessary to forecast and successfully navigate New Zealand's changing strategic environment. The GCSB is a crucial part of how New Zealand makes sense of the world and manages national security threats.

The GCSB has two primary objectives: intelligence advantage and cyber resilience.

Whakapapa

Over many years, we have built GCSB's whakapapa based on respect for what has come before, pride in the unique things only we can do for New Zealand, and the diversity that each GCSB staff member brings to our mission.

The GCSB was established in 1977 as an agency under the Ministry of Defence, becoming a stand-alone government agency in 1989, and a statutory agency in April 2003. As a SIGINT agency, whose intelligence is derived from electronic communications, our work evolves alongside technological developments. The evolution of technology has led to our role in New Zealand's cyber security. This evolution also led to the removal of our two satellite interception antennas at Waihopai Station in 2022.

We continually assess and update our capabilities to ensure they fully contribute to the New Zealand Government's priorities. We respond to rapidly evolving technology and the security threats New Zealand faces.

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.

WHO WE ARE
KO WAI MĀTOU

Functions

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) leads the resilience of New Zealand's communication networks through information assurance, cyber threat detection, deterrence, disruption and advice.

Under the Intelligence and Security Act 2017 (ISA), 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.

Our people come from across New Zealand's society and work in a variety of roles. As at 30 June 2023, the GCSB has 539.8 full-time equivalent staff, made up from 546 staff.

Funding

We are funded through Vote Communications Security and Intelligence. The Minister Responsible for the GCSB is responsible for the single appropriation within this Vote.

The GCSB's Statement of Expenses and Capital Expenditure Against Appropriation is on page 59. Unlike other departments, we only provide a total in our annual reports. This is because the ISA provides for intelligence and security agencies to protect certain information, in order to discharge their national security responsibilities effectively.

In Budget 2023, the GCSB received $13.188 million of new funding over the next four years for the NCSC to deliver on two related government priorities:

- operationalising the mandate for the GCISO
- technical advice and engagement to improve the cyber resilience of critical national infrastructure.

We also received $10.372 million of new funding over the next four years to help us continue delivering our services in the face of inflation pressures.

National Security Intelligence Priorities Whakaarotau Marumaru Aotearoa

We work to the New Zealand Government's National Security Intelligence Priorities – Whakaarotau Marumaru Aotearoa (NSIPs).

These define key areas of national security interest, assisting agencies with related roles to make informed, joined-up decisions. A description of the 2023 NSIPs is available on the Department of the Prime Minister and Cabinet (DPMC)'s website.[1]

Our work contributed to all of the 13 NSIPs in effect during the reporting period. Those NSIPs are outlined below:

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

[1] The 2023 NSIPs were approved in June 2023, replacing the 2021 NSIPs which were in effect for most of this reporting period. As such, references to NSIPs in this document are to the 2021 NSIPs.

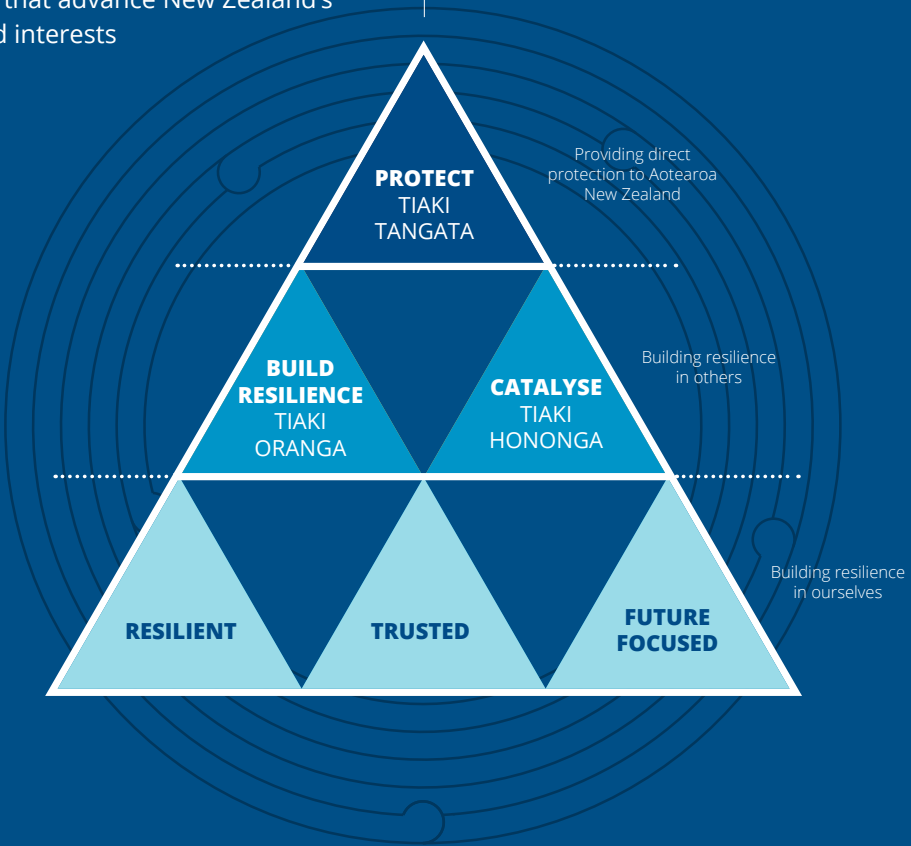
ORGANISATIONAL STRATEGY
TE RAUTAKI WHAKAHAERE

We developed a new organisational strategy for the GCSB this year, with effect from 1 July 2023. Our strategy sets out the contribution GCSB can make to New Zealand's national security and economic wellbeing over the next four years, guiding our activities between now and 2027. We look forward to this strategy shaping our mahi around intelligence collection and cyber resilience over the coming year.

Our organisational strategy is formed around six outcomes. Three focus on our mahi to protect New Zealand; three focus on ensuring that we are a strong and resilient agency.

- **Protect Tiaki Tangata** – We protect New Zealand; our people, infrastructure and information
- **Build Resilience Tiaki Oranga** – We build resilience in others so that New Zealand can confidently navigate future security challenges
- **Catalyse Tiaki Hononga** – Our products and services are based on customer partnerships and enable real-world outcomes that advance New Zealand's values and interests
- **Resilient** – We invest in GCSB's resilience so that we can better serve New Zealand
- **Trusted** – We are a trusted and confident organisation. We make a positive impact, and the value we bring to New Zealand is well understood, and
- **Future focused** – We will ensure we have the right relationships, co-ordination, and tradecraft to respond to and counter both existing and emerging threats.

Our Strategy's outcomes are underpinned by more detailed initiatives, which are developed and advanced through the annual planning process.



OUR PARTNERSHIPS
Ō MĀTAU RANGAPŪTANGA

Domestic partnerships

As part of New Zealand's National Security Sector, the GCSB works together with a range of agencies and organisations to help enhance New Zealand's national security.

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

The GCSB works closely with the NZSIS. The two agencies are co-located and share a number of enablement functions including People and Capability, Technology Directorate, Corporate and Commercial Services, as well as a Security Services Group. The majority of shared enablement staff are employed by the GCSB but work equally across both agencies.

The NZIC works alongside other agencies, such as New Zealand Police, New Zealand Customs Service, and Immigration New Zealand, to contribute to New Zealand's national security and the wellbeing of New Zealanders.

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.

To support the objective of enhancing national security, the NZIC also strives to advance New Zealand's international interests and reputation. By working with international partners the NZIC articulates New Zealand's national security priorities and interests on a global stage.

The NCSC engages with organisations of national significance in the public and private sector, to help them understand their cyber security risk and provide guidance. We also engage with the digital supply chain to increase their cyber resilience for New Zealand users. We partner with other system leaders such as the Government Chief Digital Officer and the Government Chief Data Steward to facilitate public service digital transformation.

As the government lead for information security, we partnered with the NZDF for the construction of a data centre at RNZAF Base Auckland (Whenuapai). This data centre will house protected information for a broad range of government agencies.

#3

JM JHNEMJHZ AGPQW EJAEXQJNF LEDLQW NLHJ H "FEDJEKEAHJN EJAEXQJN".

GP-XWSXVWSXEUF ETP WQGWFUQEA PH IDVWGWPNA GZJUM DGEWYWEZ TWEX WQEUMQDEWPQDV RDMEQUMA

WFT REKWM-ZKSGGMDMZSWMJU IJPX OPJCPSRRT OMKJWTA UTI ISVG JD IJPXMUC.

BCAGEXHDCL CM OXDOADB OHSXLJHIXLDLJ SXAXRDPE FCST PH CKS IXPR CMMDBX YKDERDLJ.

TOMGNF KPPWOPFJUJPB WV LKBK FJPBEJ KB EPDKV MKXJ KOFCGKPL (QYJPOKTKN).

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.

Our international partnerships include the international intelligence and security partnership known as the Five Eyes. The Five Eyes is made up of New Zealand, Australia, Canada, the United Kingdom and the United States of America.

The Five Eyes partnership has been an instrumental part of New Zealand's intelligence and security activities since World War II. The partnership began as a cryptologic venture to share efforts and results in code breaking (and code making) during the war. The Five Eyes partnership remains 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.

While New Zealand receives great benefit from the Five Eyes intelligence partnership, it also makes a unique and valued contribution to global efforts. In September 2022, we hosted the annual conference of Five Eyes partners. This conference brought together the leaders of the Five Eyes intelligence and security agencies, and covered a range of matters critical to New Zealand's national security, and that of our wider region.

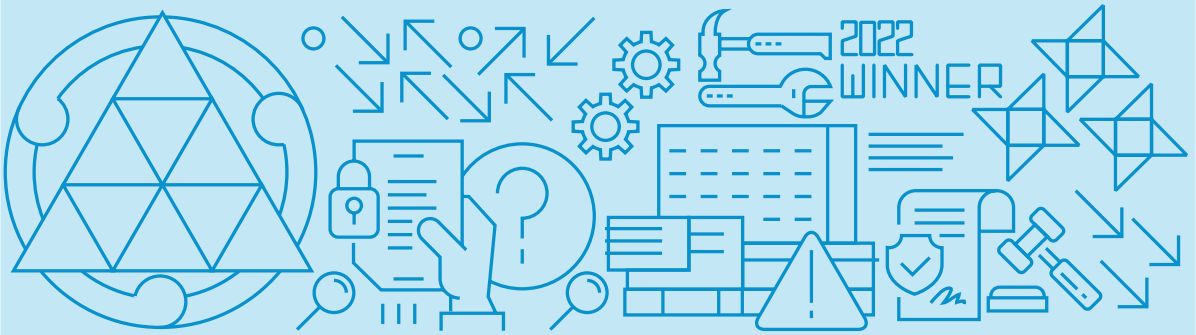
We also value the partnerships we have with many other states.

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.

#4

https://www.gcsb.govt.nz/puzzle-04.html

YEAR AT A GLANCE
TE RARAPA I TE TAU



WHO WE ARE AND WHAT WE DO

- Development of new organisational strategy, with effect from 1 July 2023.
- Completion of seismic strengthening remedial work at our head office building.
- Public announcement of data centre at RNZAF Base Auckland (Whenuapai).
- Co-hosted Five Eyes conference in September 2022.

ORGANISATIONAL CAPABILITY

- Along with the NZSIS, we won the Leadership Award at the 2022 Diversity Works Awards, recognising our efforts to drive diversity and inclusion and create a welcoming and inclusive environment.
- Introduced Te Tiriti o Waitangi into our organisational strategy and held Māori capability workshops to ensure all staff are informed and engaged on our efforts to improve our Māori cultural capability.
- Our gender pay gap decreased 2.8 percentage points.
- Our staff turnover decreased by 3.7 percentage points, from 19.3 percent to 15.6 percent.
- The Multi-Classification Work programme piloted new ways of working.

INDISPENSABLE INTELLIGENCE

- Provided a significant amount of intelligence reports to customer agencies across all NSIPs.
- The highest priority topics for intelligence delivered to customers included matters of most significance to the National Security of New Zealand and New Zealanders.
- We contributed to NZDF efforts to detect and counter threats to New Zealand military personnel deployed overseas.
- We provided intelligence to customers on a range of key issues affecting our region.
- Provided SIGINT to New Zealand Customs Service and New Zealand Police to stop drugs entering New Zealand.

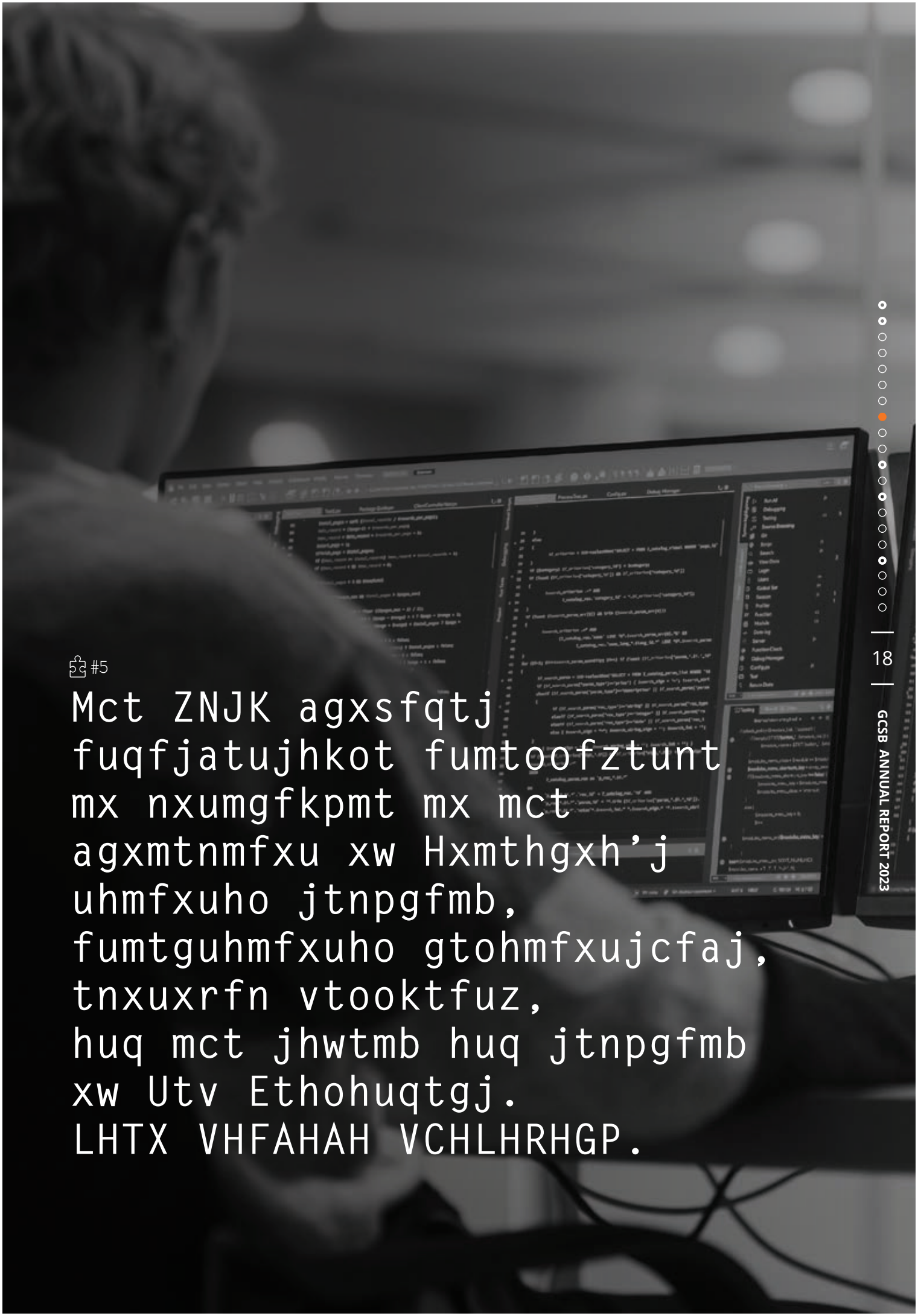
ACCOUNTABILITY AND TRANSPARENCY

- Fifteen Type 1 intelligence warrants and 12 Type 2 intelligence warrants approved.
- Completed 59 OIA requests and 23 Privacy Act requests.

THE HEART OF AOTEAROA NEW ZEALAND'S CYBER DEFENCE

- GCISO function strengthened.
- 316 cyber incidents recorded by NCSC (350 in 2021/22).
- No national cyber incidents higher than a "significant incident".
- 105 vulnerabilities triaged, leading to 20 critical vulnerability alerts.
- Co-highlighted two incidents of malicious cyber activity with international partners.
- MFN® awarded "Best Security Product or Service" at the 2022 annual iSANZ cyber security industry awards, as well as the 2023 Te Hāpai Hapori Spirit of Service Award for Service Excellence and overall Prime Minister's Award.
- 7 cyber security advisories published (5 co-authored with domestic and international cyber security partners).
- Cyber security support to events including the Local Government elections and Census 2023.
- New Zealand Information Security Manual version 3.6 published in September 2022.
- Co-chaired 22 Security Information Exchanges across six sectors.

- Conducted 20 national security risk assessments of applications under the Outer Space and High-altitude Activities Act 2017 with the NZSIS.
- Conducted 45 assessments of satellite licensing requests made under the Radiocommunications Act 1989 with the NZSIS.
- Provided advice to the Overseas Investment Office on 42 proposals with the NZSIS.
- Delivered annual Telecommunications (Interception Capability and Security) Act 2013 (TICSA) roadshow.
- Received 159 notifications for assessment of network changes.



#5

Mct ZNJK agxsfqtj fuqfjatujhkot fumtoofztunt mx nxumgfkpmt mx mct agxmtnmfxu xw Hxmthgxh’j uhmfxuho jtnpgfmb, fumtguhmfxuho gtohmfxujcfaj, tnxuxrfn vtooktfuz, huq mct jhwtmb huq jtnpgfmb xw Utv Ethohuqtgj. LHTX VHFAHAH VCHLHRHGP.

Our Work in Detail

He Tirohanga Hōmiromiro ki ā mātau Mahi

INDISPENSABLE INTELLIGENCE
HE MŌHIOHIO WAIWAI

Introduction – Intelligence Collection

The GCSB is a signals intelligence (SIGINT) agency, meaning we collect and analyse electronic communications to produce intelligence. We provide a range of intelligence products across all NSIPs under our function to contribute to the protection of New Zealand's national security, international relationships, economic wellbeing, and the safety and security of New Zealanders. In 2022/23 we provided intelligence reports to 18 government agencies across the 13 NSIPs.

The intelligence we provided included intelligence sourced through our international partnerships as well as intelligence collected and analysed by GCSB. In 2022/23, the main areas of focus for GCSB intelligence collection and analysis under the NSIPs included:

- Foreign interference and espionage
- Global economic security
- Global governance and strategic competition
- Malicious cyber activity
- Maritime and border security and Antarctica
- New Zealand's strategic interests in the Asia region
- New Zealand's strategic interests in the Pacific region
- Terrorism and violent extremism
- Threats to New Zealanders overseas
- Transnational serious and organised crime.

Our legislation enables us to seek authorisation to intercept communications, seek assistance from telecommunications network operators and service providers, and receive intelligence from our international partners. Our legislation also permits us to access information infrastructures when authorised, allowing us to retrieve digital information directly from where it is stored or processed. We are subject to robust oversight, including from the Inspector-General of Intelligence and Security and the Parliament's Intelligence and Security Committee.

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 an area of strategic competition for various great powers seeking to project influence into the region. This competition could have a detrimental effect on regional security. Transnational organised crime also impacts the security of the region.

The GCSB provides SIGINT in relation to New Zealand's interests in the South Pacific. This focuses on providing support to other government agencies whose responsibilities include responding to security issues in the Pacific region.

Countering Foreign Interference

We work closely with the NZSIS to understand how New Zealand's people and sovereign structures are at risk from the foreign interference activities of other states.

Counter-terrorism

Our counter-terrorism effort has both a foreign and a domestic focus, and is aimed at ensuring New Zealand, New Zealanders, and our interests overseas are protected from extremism at home and abroad. Internationally, we continue to make a unique and highly valued contribution to global counter-terrorism efforts. This includes helping disrupt attack planning. Our work has focussed on UN-designated terrorist entities and identity-motivated violent extremists.

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

Transnational organised crime

We are a participant in the New Zealand Police-led New Zealand Transnational Organised Crime (TNOC) Strategy. We provide intelligence and technical assistance to the New Zealand Customs Service (Customs) and Police to help counter TNOC.

The TNOC strategy strongly aligns with the 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.

Supporting NZDF

We contribute to NZDF efforts to detect and counter threats to New Zealand military personnel deployed overseas.

Customer Engagement

The Intelligence Customer Centre (ICC) leads the provision of intelligence products to customers on behalf of Intelligence Community agencies. By having a combination of GCSB, NZSIS and DPMC staff, our customers have a single point of contact and get the right information at the right time in a coordinated way. This is done through a range of activities, including in-person read services and digital read folders.

Our delivery and coordination improved this year, both internally and between agencies, leading to excellent feedback from customers. This demonstrates a positive impact on the New Zealand Government's ability to understand and respond to global developments.

During 2022/23 the ICC supported customers with classified intelligence relating to a number of significant events. We continue to run Introduction to Intelligence courses for attendees across 18 different government agencies. We ran five of these courses in the past year supporting the staff in these agencies to understand how we can help them and what we can provide to assist New Zealand's decision makers.

THE HEART OF AOTEAROA NEW ZEALAND'S CYBER DEFENCE
TE PŪMANAWA O NGĀ MAHI WHAKAHAUMARU Ā-IPURANGI O AOTEAROA

The GCSB's National Cyber Security Centre (NCSC) works to protect New Zealand's wellbeing and prosperity through trusted cyber security services. The NCSC responds to national-level cyber harm and supports New Zealand's nationally significant organisations to improve their cyber security posture.

The NCSC's key objectives are to:

- defend New Zealand's national security
- raise New Zealand's cyber resilience
- facilitate New Zealand's digital transformation.

We operate in a complex, challenging, and uncertain environment. Networks around the world remain vulnerable to malicious cyber activity. With mounting global reliance on complex shared systems for the delivery of services, malicious cyber actors seek new ways to infiltrate weak supply chain access points, and severely impact service delivery and information security.

Information security threats continue to evolve rapidly with advancing technologies. Defending New Zealand's national security ensures our values and way of life are protected. We play a crucial role in upholding New Zealand's national security and global standing by maintaining trusted and effective information security protections at a national level. We continue to work closely with international partners to reinforce important global norms of acceptable behaviour in cyberspace.

Raising cyber resilience helps our digital environment withstand adversity. To achieve this, we assist nationally significant organisations to actively protect themselves, reducing cyber security risk, and ensuring their systems and information are safe and secure. We also role-model good practice across the wider economy.

While technology brings many benefits, it comes with its own risks. With sharpening geostrategic tensions, it is possible the cyber threats New Zealand faces will increase. We have pre-emptively focused on potential implications for New Zealand, and deliver timely, relevant guidance and services to nationally significant organisations to support their cyber resilience.

Digital transformation provides the foundation for organisations in New Zealand to flourish in the digital age. We facilitate organisations in New Zealand to embrace technology responsibly and securely. As organisations expand their digital footprints, information security risks increase in parallel. It is important to embed security solutions and processes into business to secure vital assets and mitigate any risks.

Through our Director-General's role as Government Chief Information Security Officer (GCISO), we are able to provide a single source of information security leadership and investment advice about information security risks across the public sector.

The role of the Government Chief Information Security Officer

The GCISO draws on the unique insights and observations from the NCSC to help inform the public sector about current and emerging cyber security risks. This mahi is supported by the Deputy GCISO, who engages across the public sector on information security matters, and ensures guidance and advice drives change in the public sector.

The GCISO focuses on setting and lifting information security controls and standards across government, and supporting digital investment by protecting the security and integrity of information and associated infrastructures of importance to the New Zealand Government.

The GCISO works closely with the Data and Digital System Leads – the Government Chief Data Steward (GCDS) and Government Chief Digital Officer (GCDO) – to support the public sector to deliver better outcomes for New Zealand. The System Leads have committed to collectively focus their efforts to achieve this shared vision. These three System Leads collect information from agencies under their mandates to ensure that the system and its individual parts are working as intended.

The three System Leads also work together to support the Government's investment in data, digital and cyber security in a more coordinated and strategic manner. The GCISO, GCDS and GCDO support system leadership advice to the Minister of Finance regarding relevant budget bids.

In April 2023, Cabinet reaffirmed the GCISO's mandate, leadership role and responsibilities, and clarified expectations on agencies that fall within the scope of the mandate.

The 2022 – 2023 year

This was a year of progression for the NCSC. We released the NCSC strategy publicly for the first time, which involved acknowledging the need to make our work more accessible, and that we can have impact at scale when we collaborate with others. Domestically, we continued to partner with New Zealand industry to deliver Malware Free Networks® (MFN®), and to drive system-wide improvements alongside the Data and Digital system leaders. Internationally, we worked to release joint products regarding the latest threats and best practice advice.

State-sponsored cyber actors remain the most significant espionage and security threat to New Zealand's organisations. These actors continue to demonstrate intent and capability to target New Zealand for information of intelligence value.

The sophistication and persistence of malicious cyber actors, both state-sponsored and financially motivated criminals, continues to cause significant impacts to New Zealand and global organisations. Service providers are increasingly targeted by cyber criminals seeking ransom payments.

Cyber security is a rapidly evolving domain. There has been significant work across government to ensure the right settings are in place for us to have impact at scale. These decisions reflect the confidence that New Zealand Government has in the mahi we do.

These decisions included expanding the GCISO mandate to a broader customer set, moving beyond the core public service to crown entities. Government also invested in the NCSC to act as a technical authority in support of cross-government work, improving the cyber resilience of critical national infrastructure.

In addition, we supported planning around the integration of CERT NZ with the NCSC to establish the GCSB as the government's lead operational cyber security agency. This integration will ensure there is a single agency with the expertise and relationships to help increase New Zealand's cyber resilience across the spectrum of harm.

To achieve the NCSC's three objectives, we provide services in four key categories.

- **Detect:** We alert our customers to malicious activity, threats and vulnerabilities.
- **Disrupt:** We prevent threats from harming our customers.
- **Advise:** We guide and equip our customers to protect their valuable information and manage risk.
- **Deter:** We raise the cost for our adversaries in targeting New Zealand.

Budget 2023

We received $13.188 million in Budget 2023 to fund initiatives building critical cyber resilience. This includes providing technical expertise and engagement to improve the cyber resilience of New Zealand's critical national infrastructure, and to operationalise the mandate for the GCISO.

This funding was additional to the $18.986 million received in Budget 2022 for initiatives improving services to protect New Zealand's most significant information.

These are long-term initiatives that will help establish systems and foundations for the New Zealand Government to continuously improve cyber resilience.

DETECT

The NCSC detects indications of malicious activity or vulnerabilities on consenting customer networks, and provides advice to customers on best-practice techniques to mitigate potential risks to their operating environments.

The NCSC ensures the New Zealand Government's classified systems are free from compromise by providing assurance to sensitive compartmented information systems and sites, and diplomatic posts.

Information security threats continue to evolve rapidly with advancing technologies. The increasing sophistication and persistence of malicious cyber actors, both state-sponsored and financially motivated criminals, continues to cause significant impacts to New Zealand and global organisations. Service providers are increasingly targeted by cyber criminals seeking ransom payments.

In response to this cyber security threatscape, we continuously develop and refine our detection and disruption capabilities to better protect New Zealand and its people. During 2022/23 we continued to stabilise and improve our capabilities, services, disruption and collection. This included streamlining existing capabilities, and investigating and developing new methods to enhance our detection suite.

Cyber Defence Capabilities

Our cyber defence capabilities continue to play a significant and valuable role to support organisations of national significance by protecting their networks from malicious cyber activity. We provide advanced cyber defence capabilities, including CORTEX and MFN®, to a range of nationally significant organisations with their express consent. This enables us to identify and protect organisations that are vulnerable to specific threats, or are at risk of targeting by malicious cyber actors.

Our cyber defensive capabilities are designed to supplement commercial service offerings, and are tailored to the specific threats New Zealand faces. Our customers are spread across critical infrastructure providers, central and local government, key research institutes and key economic generators. For security and confidentiality reasons, we do not routinely disclose specific customers.

During 2022/23 we continued to stabilise and improve our capabilities, services, disruption and collection. This included streamlining existing capabilities, and investigating and developing new methods to enhance our detection suite.

Have I Been Pwned

In early 2022, the NCSC announced its partnership with Have I Been Pwned (HIBP). HIBP is an online resource that compiles open-source information about data breaches into a searchable database. The service is being used to understand potential vulnerabilities within public sector organisations and to enable better protection against incidents that leverage credential-based targeting.

During 2022/23 the NCSC successfully completed historical breach reporting to 151 New Zealand Government organisations and provided insights into their existing cyber security practices through data analytics, trend reporting, and tailored guidance. Insights from this are also being used to improve our approach to public sector cyber resilience.

Technical Counter-Surveillance Unit

The NCSC's Technical Counter-Surveillance Unit (TCU) helps ensure New Zealand's most sensitive communications are not intercepted or compromised.

The TCU provides technical security, emanations security and accreditation services. Technical security services focus on countering technical surveillance techniques by hostile actors, such as eavesdropping and video surveillance. The TCU has a mobile capability to inspect facilities for signs of technological efforts to compromise security. Emanations security services are focused on countering the threat posed by the 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 sites and systems. The Director-General is the New Zealand Government's accreditation authority for highly classified information systems and sites.

Russia-Ukraine conflict continues to impact cyber threat landscape

Shifts in the cyber threat landscape following Russia's invasion of Ukraine in February 2022 continue to be felt internationally. Russia-aligned cyber actors are likely emboldened by the invasion, and we continue to see concerning activity affecting Russia's neighbours and our Western partners. As the invasion persisted into 2023, malicious cyber activity continued to be observed in support of Russia and Ukraine, albeit not to the extent many suspected. The support Ukraine received to improve their cyber defences may have hampered the effectiveness of Russia's actions in cyberspace.

Russian malicious cyber activity has likely continued its pre-invasion trajectory, including targeting individuals of high espionage value with high-quality, highly sophisticated social engineering and malicious software (malware). This traditional cyber espionage has been punctuated by disruptive cyber campaigns directed at Ukraine and Russia's other neighbours.

A theme of the year's cyber landscape has been the rise of issue-motivated 'hacktivists' on both sides of the conflict. On the Russian side, these actors are likely emboldened by permissive attitudes to cyber-enabled crime within Russian borders. Issue-motivated cyber activity has usually followed the public commitment of support to Ukraine from Western democracies. Issue-motivated malicious cyber actors have widely targeted Western organisations with denial-of-service campaigns, including in the healthcare sector, with mixed success. We remain concerned about accidental escalation as a result of disruptive malicious cyber activity stemming from the Russia-Ukraine conflict.

The main cyber threat to New Zealand due to Russia's invasion of Ukraine is indirect cyber targeting, affecting our critical supply chains. State- and non-state cyber actors alike could disrupt key suppliers on which New Zealand's organisations depend.

DISRUPT

The NCSC disrupts malicious cyber activity from impacting its customers' environments by blocking harmful activities through our active disruption capabilities. We intervene to remove malicious cyber actors from victim networks, and support affected organisations through service restoration and recovery.

We help our customers to protect themselves by providing advice about relevant potential threats and how to mitigate these.

Malware Free Networks®

Our MFN® cyber defence capability, launched in November 2021, uses a range of NCSC-sourced intelligence to detect and disrupt malicious cyber activity targeting New Zealand. Our threat intelligence feed contains indicators of malicious activity generated using automation from a range of sources and is curated by our analysts.

As of 30 June 2023, MFN had disrupted more than 390,000 threats since its launch in 2021. This figure reflects disruptions of potentially malicious activity with the potential to cause harm to New Zealand's organisations and individuals.

The NCSC works closely with managed service providers, internet service providers and cyber security providers to deliver our MFN capability. These partners use our automated threat feed to detect and disrupt threats before the malicious activity can impact customers' systems. MFN partners provide sighting notifications back to us, so we can understand the effectiveness of MFN and gain a greater understanding of the cyber threat landscape in New Zealand.

In the 2022/23 year, MFN expanded to 14 private sector partners, with some partners also increasing who they offer services to. This expansion represents a meaningful increase in the span of New Zealanders that can be protected by the intelligence provided by MFN.

Our MFN capability has received industry recognition. In November 2022, MFN won the "Best Security Product or Service" at the annual iSANZ cyber security industry awards. The judges noted that MFN helps defend against an evolving range of cyber threats and has increased the cyber security resilience of many New Zealand's organisations. Additionally, the judges commented on the strength of MFN's design and implementation, and its ability to improve security across the country while also protecting the privacy of users.

MFN was also nominated as a finalist for the 2023 Te Hāpai Hapori, Spirit of Service awards for Service Excellence, later jointly winning both that award, and the overall Prime Minister's Award. The wins recognised the collaborative, leading-edge approach MFN uses to raise New Zealand's cyber defence. Judges acknowledged the NCSC's innovation and its commitment to continuous improvement of services and sharing data through world-leading sector partnerships.

Incident Response Services

Our Incident Coordination and Response function plays a vital role in safeguarding New Zealand's nationally significant organisations against cyber threats that could impact New Zealanders' national security and wellbeing. We triage incidents according to their potential national impact, engage with the victim to understand the scope of the activity, and support the victim throughout the incident's lifecycle. This involves performing analysis and providing recommendations to support malicious activity containment, remediation and recovery.

As significant incidents often require careful coordination of interagency, sector, and wider government actions, our responses often involve working closely with wider sector partners such as CERT NZ, Police, and the private sector.

Even with strong cyber defences, cyber security incidents still occur, and malicious cyber actors continue to discover weaknesses to gain access to systems. We continue to see rapid exploitation of vulnerabilities, highlighting the importance of timely patching regimes, adequate log retention, and ongoing investment in cyber security.

#6

)*$!)$!)!)&!)^&)*#)^^

)&*)(&!!^!)%!!!!!))(&!)*)^&!@!)
(*!)!!!$

)*#!)!)((!!&!!$!)%!!^!@!
)^&!)!!!)!!^!!$!)!

!)%!!% !!^!)$!)!

!)$!)!)(&!!$!!^ !!!!!)@

)^%!!!!!^!)!)(&!!$!!!)(&)#(!!%)((!@!)
(*!)!!!$

!))!)!!)@!)!!!))((!)!)$^
)*$)&#)&@)&()&#

)*&)^%)&#)&&)^%)*%)&%)*%
)*&)^()&^)&^)*#)&))&()*@)^*)$^

Cyber Incident Trends and Statistics

In 2022/23, the NCSC recorded 316 cyber incidents[2]. This is a reduction from 350 in 2021/22. The difference may reflect a number of contributing factors, including:

- recent disruptions to cyber criminal infrastructure
- changing state priorities or tactics
- organisational cyber resilience and maturity
- increased ability to disrupt activity before harm takes place.

This is the first year the NCSC recorded a higher percentage of cyber criminal-linked incidents than incidents linked to state-sponsored actors. However, the distinction between state-sponsored and cyber criminal activity continues to blur. This creates challenges for cyber investigators to understand the motives of malicious cyber actors. Of the 316 recorded incidents, 28 percent were likely criminal or financially motivated, while 23 percent indicated links to suspected state-sponsored actors. In 2021/22, 34 percent indicated links to suspected state-sponsored actors.

We categorise incidents based on the severity of the compromise, as well as the significance of the victim organisation. The scale ranges from C1 (national cyber emergency) to C6 (minor incident). This year's most severe incidents were rated C3 (significant incident) and were predominantly associated with extortion activity, such as ransomware. Some incidents had potential flow-on effects for other organisations, with the compromise of one posing risks to the privacy and security of others.

Our focus on high impact cyber incidents and organisations of national significance means the above figures represent a portion of the overall malicious cyber activity targeting New Zealand.

In 2022/23, we led the response to a number of significant incidents, including the targeting of a local government organisation by a sophisticated malicious cyber actor. Analysis revealed a vulnerability in a remote access solution was exploited to gain initial access to the victim's network.

The NCSC assisted the victim organisation and its managed service provider to understand the scope of the intrusion, remove the intruder and prevent further attempts to compromise their network. Prompt response efforts and work to identify the full path of the intrusion contained the compromise for both victims, and reduced its impact.

[2] A cyber security incident is an occurrence that appears to have degraded the confidentiality, integrity, or availability of a data system or network.

ADVISE

The NCSC advises and equips its customers to protect their valuable information and manage risks.

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

We improve 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.

Advisories and Alerts

We assess and triage common vulnerabilities and exposures based on their perceived impact to New Zealand. We alert organisations of national significance when a vulnerability might impact New Zealand. While these alerts are not a replacement for organisations' internal vulnerability monitoring, they reinforce existing decisions and support out-of-cycle patching and changes. In the 2022/23 year, we triaged 105 vulnerabilities, leading to 20 critical vulnerability alerts.

The NCSC also supports New Zealand's organisations to respond to changes in the cyber and technology threat landscapes by publishing a range of security advisories and alerts about potential or current threats on the NCSC website. Security advisories share information about specific vulnerabilities or types of malicious cyber activity seen targeting local networks. Advisories may incorporate technical indicators of compromise and mitigation advice security teams can use to strengthen their defences.

During 2022/23 we published seven cyber security advisories, which highlighted a range of cyber security activity by Advanced Persistent Threat groups, and best-practice advice that organisations should follow to protect their computer networks from harm. Five of these advisories were co-authored with domestic and international cyber security partners.

Support to Major Events

The NCSC continues to provide cyber security support to major national events in coordination with cross-government efforts. Cyber security incidents could undermine the confidentiality, integrity or availability of data associated with an event, and events are likely of interest to both state-sponsored and criminal malicious cyber actors.

We provided cyber security support to several events in 2022/23, including the Local Government elections in October 2022. While a paper-based process lessened the cyber threat to the voting process itself, the NCSC provided a range of assistance to organisations associated with the local election. This included the provision of threat assessments, and proactive advice and guidance to organisations associated with the elections.

We also supported Census 2023, providing threat briefings, cyber resilience advice, advice around securing networks, and incident response planning and support.

We began proactively providing cyber security support ahead of the General Election scheduled for October 2023.

New Zealand Information Security Manual

The GCISO function includes establishing the New Zealand Government information security standards and guidance, as set out in the New Zealand Information Security Manual (NZISM). The NZISM version 3.6 was published in September 2022. This version includes a new chapter on public cloud security, supporting the refresh of the Government's Cloud First Policy Refresh.

Government Cloud Programme

We continue to support the all-of-government Cloud Programme, including contributing to the Cloud First Policy Refresh. This work is led by the Department of Internal Affairs, and is an all-of-government certification process for onshore data centres, established to support public sector agencies to securely transition to cloud-based technologies.

Cyber Security Framework

We published a cyber security framework in February 2023. The framework sets out how we, as cyber security leaders, think about, talk about and organise cyber security efforts. The framework has five functions which together represent the breadth of work needed to secure an organisation. The framework can be used by any organisation in New Zealand, and feedback from users will be incorporated as appropriate.

Engagements

Cyber threat information and best-practice guidance is generated by both public and private sector organisations. We facilitate information sharing, especially where sharing requires a high level of trust. This primarily takes place through Security Information Exchanges. In the 2022/23 year, we co-chaired 22 of these exchanges across six sectors: energy; finance, government; network-providers; tertiary; and transport & logistics.

We delivered a Telecommunications (Interception Capability and Security) Act 2013 (TICSA) roadshow, an annual opportunity to talk with operators on their obligations under the Act, and outline the NCSC assessment processes. Sessions were provided in Auckland, Wellington, and Christchurch. We also engage with network operators at the New Zealand Network Operators Group and on an ad-hoc basis.

DETER

We deter adversaries by providing world-leading information security services to customers. This, in turn, makes it more difficult for malicious cyber actors to target our customers.

Our deterrence work includes:

- securing our customers' sensitive information
- supporting robust technology investment across New Zealand's critical systems
- supporting the secure provision of telecommunications services
- public attribution of malicious cyber actors.

Calling out Malicious Cyber Activity

We continue to publicly attribute malicious cyber activity that contradicts the internationally accepted norms of behaviour in cyberspace. In collaboration with domestic and international partners, we aim to raise awareness of the cyber threat and provide information of value to cyber defenders to mitigate malicious cyber activity. Throughout the past year, we publicly released information with our partners on three separate occasions to expose previously unknown malware or tradecraft.

We continue to conduct technical attributions and analysis to identify those responsible for malicious cyber activity. These attributions are shared with domestic and foreign partners to inform understanding of cyber threats to New Zealand. While these attributions are usually classified, the New Zealand Government can choose to declassify and publicly release the conclusions when it is in New Zealand's interests to do so.

In early May 2023, we joined international partners to publish a technical advisory about a Russian malware named Snake. Snake was used by the Russian Federal Security Service almost certainly for sensitive intelligence collection. Combined with the tensions from Russia's invasion of Ukraine, we saw the potential for an increase in malicious cyber activity impacting New Zealand, including through the use of the Snake malware. The advisory enabled cyber defenders to mitigate the malware and associated FSB intelligence collection.

We also joined our international partners to highlight malicious cyber activity associated with PRC state-sponsored cyber actors in May 2023. Partners observed the targeting of critical infrastructure in the United States; the actors' techniques have the potential to impact other organisations and sectors within New Zealand. We published an advisory detailing the activity with technical information to assist cyber defenders identify it.

In collaboration with CERT NZ and cyber security partners from six other nations, in June 2023 we released an advisory detailing the tactics, techniques and procedures used by cyber criminal affiliates using LockBit ransomware. LockBit, a Ransomware-as-a-Service, is one of the most globally used and prolific ransomware. The ransomware has been used against organisations worldwide including critical infrastructure. The advisory helps organisations understand and defend against this global threat.

Cryptographic Solutions and Development

The GCSB is New Zealand's national authority for communications security (COMSEC). COMSEC is the technology and processes used to protect our most sensitive data through advanced, high-grade encryption. COMSEC is the primary means of maintaining the integrity of New Zealand's highly classified communications.

We provide High-Assurance Cryptographic Equipment (HACE), key material and COMSEC support to New Zealand Government agencies and selected commercial entities above the RESTRICTED classification level.

During 2022/23 we implemented new frameworks to support our mandate as the national authority for COMSEC. These include introducing a COMSEC Incident Board to triage and manage incidents. We actively engage with COMSEC compliance working groups in the Five Eyes community to share information and identify international trends. These findings inform initiatives for COMSEC users to help lower the overall rate of COMSEC incidents.

High-Assurance Cryptographic Equipment (HACE) Procurement and Delivery

The GCSB is responsible for assisting all New Zealand Government departments to procure HACE and mandating the policy, standards and procedures in order to achieve consistency and inter-operability with the international cryptologic community for HACE during its lifecycle.

Cryptographic Infrastructure

The GCSB continues to enable New Zealand Government agencies to protect their highly classified information through the operation of New Zealand's Cryptographic Products Management Infrastructure (CPMI). CPMI is a secure ordering, generation, and distribution capability for encryption keys and other cryptographic services which handles the majority of encryption products provided by the GCSB.

Supporting our Customers

The CPMI infrastructure operated by the GCSB provides protection for a range of highly classified New Zealand Government communications, including emails sent by diplomats posted overseas, to air, land and sea communications systems deployed by the NZDF.

Regulatory Functions

New Zealand's telecommunications networks are a core part of critical national infrastructure. Organisations and individuals rely on network providers for safe and secure access to digital capabilities, and the secure provision of telecommunications services.

The purpose of TICSA in relation to network security is 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.

Part 3 of TICSA establishes a framework under which telecommunications network operators are required to engage with the GCSB about network changes or developments to their networks in areas of security interest. Many of these changes are currently driven by cloud adoption, increased demand for remote working, the rollout and expanded capacity of fibre optic cabling, and the transition to 5G services.

In 2022/23, the GCSB received 159 notifications for assessment of network changes. A significant number of these related to the continued rollout of 5G, the diversification of market offerings, international capacity increases, and hardware lifecycle upgrades.

In addition, we partner with the NZSIS to inform decision-making in other regulatory regimes. We work closely with the NZSIS to conduct national security risk assessments for the growing space industry under the Outer Space and High-altitude Activities Act 2017. This national security risk advice is used to inform Ministers, as required by the Act.

In 2022/23 the GCSB conducted:

- 20 national security risk assessments of applications under the Outer Space and High-altitude Activities Act 2017
- 45 assessments of satellite licensing requests made under the Radiocommunications Act 1989.

Overseas Investment

Foreign direct investment is regulated by the Overseas Investment Office within Land Information New Zealand. Overseas investments are broadly considered to provide positive outcomes for New Zealand. However, foreign investment occasionally involves risks, including national security risks.

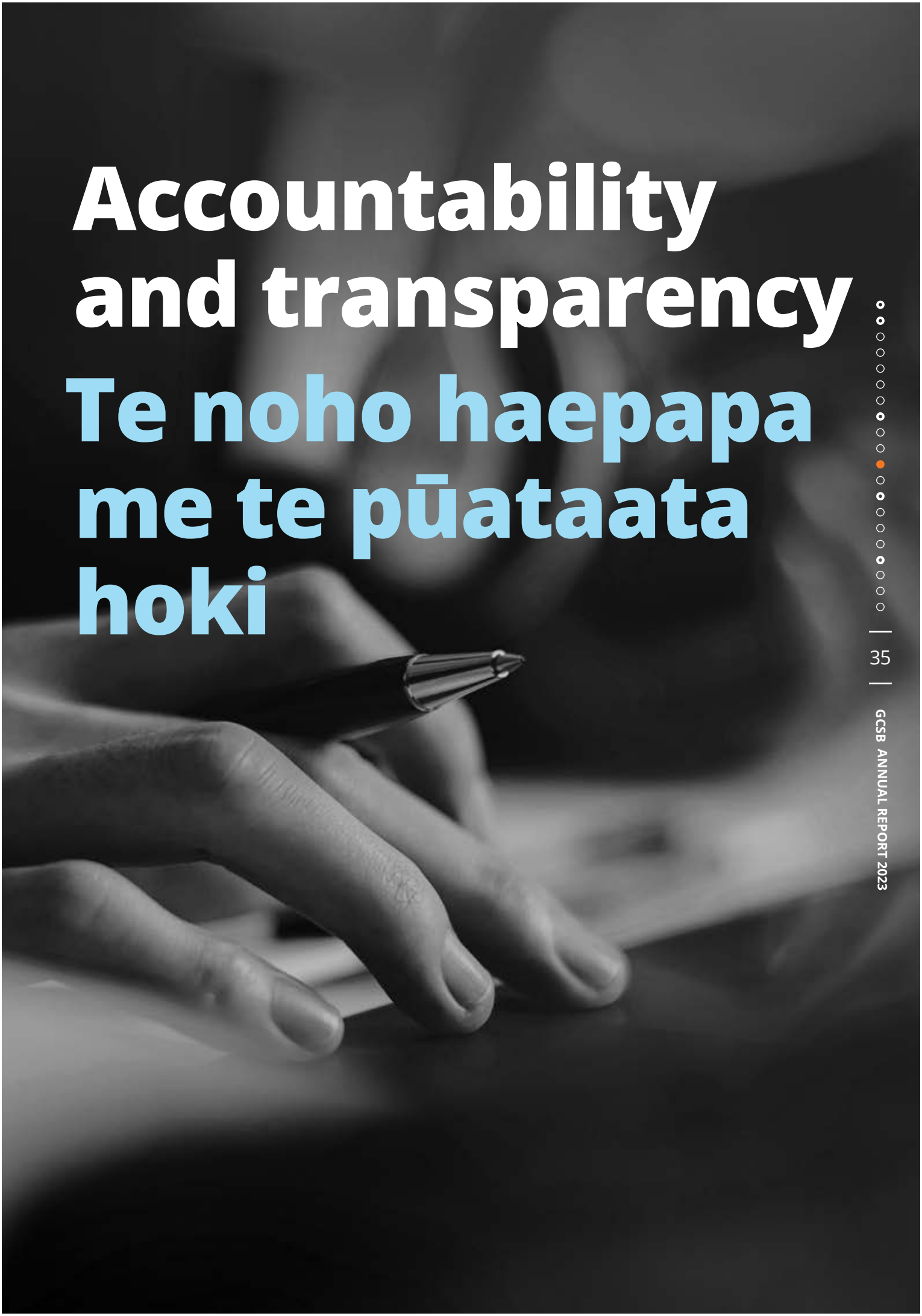
Both the GCSB and NZSIS support the Overseas Investment Office by providing national security advice on transactions which have been referred or notified under the Overseas Investment Act 2005. We work with the NZSIS to provide assurance to decision makers, as well as ensuring that investment into some of New Zealand's most important and sensitive assets is done in a way that takes into account national security.

In the past year the GCSB and NZSIS provided advice to the Overseas Investment Office on 42 instances of proposals for overseas investment subject to the national security and public order notifications regime of the Overseas Investment Act 2005.

Some applications trigger assessments or delivery of advice under more than one regulatory regime. The GCSB anticipates that this trend will continue, driven by rapid technological development and a broadening range and complexity of use cases.

Accountability and transparency

Te noho haepapa me te pūataata hoki



LEGAL COMPLIANCE AND OVERSIGHT
TE WHAI I TE TURE ME TE TIRO WHĀNUI

The Intelligence and Security Act 2017

The Intelligence and Security Act 2017 (ISA) provides the legal framework for the GCSB's activities. The ISA sets out the objectives and functions of the GCSB and NZSIS, and provides the mechanism for us to carry out otherwise unlawful activities. There are 10 Ministerial Policy Statements relevant to the GCSB that set out Ministerial expectations and provide guidance on how certain lawful activities should be conducted.

The ISA requires periodic reviews of the GCSB, NZSIS and the ISA itself. Sir Terence Arnold KC and Matanuku Mahuika, with Dr Penelope Ridings as a special advisor, completed the first review on 31 January 2023. This review was brought forward to address issues raised by the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain (the Royal Commission). The terms of reference focussed on considering the Royal Commission's recommendations about the ISA and identifying any improvements that could be made to the ISA to ensure it continues to be clear, effective and fit for purpose.

The ISA review's report, *Taumaru: Protecting Aotearoa New Zealand as a free, open and democratic society*, was made publicly available in May 2023. The report has 52 recommendations on a range of matters, which are being considered by Government. We provided information to assist the reviewers to conduct their review.

The Government response to the ISA report is being jointly led by the Prime Minister and the Minister Responsible for the GCSB and NZSIS. DPMC administers the ISA and is the lead agency for responding to the review. We are supporting the Government's response.

Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain

The GCSB continues to respond to recommendations made by the Royal Commission's Report and works closely with the NZSIS and New Zealand Police to support a number of domestic terrorism related investigations. Two of the initiatives we are involved in are outlined below.

Intelligence and Security Act Review – A number of recommendations related to the Intelligence and Security Act 2017 (ISA) were raised in the Royal Commission's report. An independent statutory review of the ISA was brought forward in response, with the recommendations informing the terms of reference. This report, *Taumaru: Protecting Aotearoa New Zealand as a free, open and democratic society* was publicly released on 29 May 2023. We will continue to support the Government's response.

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.

#7

GLCRBAROLGLCRGJBGUER
RFRIRARYRIRALUYESIGD
QMWLJSCDWGTWQJBZBYU
TIJWOQETASRJLULNVOV
HKWFGDMOYDNICQAAROR
GRMLQLOEJXCLMKPXORD
YXNVMQNPISFQHBCYXNA
LNXCBMZBPCQQTFTNSMH
RIXHEBESYQUAQLXQNPG
AJLMYVRNVXJKCZEHJHE
GXTOKPBDYOXYVSOKXYXR

Independent oversight

Aside from our own internal processes, the GCSB is subject to the oversight of several external bodies. Like other public sector agencies, this includes the Ombudsman, the Privacy Commissioner, Office of the Auditor-General, and Te Kawa Mataaho – the Public Service Commission. We are also subject to robust oversight from the Intelligence and Security Committee, and Office of the Inspector-General of Intelligence and Security.

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 must have between five and seven members, comprising the Prime Minister, the Leader of the Opposition, and other members of Parliament nominated by the Prime Minister and the Leader of the Opposition.

Office of the Inspector-General of Intelligence and Security

The Inspector-General of Intelligence and Security (IGIS) provides independent external oversight and review of the GCSB and NZSIS. The IGIS provides assurance to the public of New Zealand 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.

Statement of Warrants

In accordance with section 221(2) of the ISA, the following statements are provided for the period 1 July 2022 to 30 June 2023.

Co-operation

We did not provide any advice or assistance to the NZDF or the New Zealand Police for the purpose of exercising those agencies' functions under section 13(1)(b). However, we 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.

Intelligence Warrants

A total of 27 intelligence warrants were approved in 2022/23, of which 15 were Type 1 intelligence warrants and 12 were Type 2 intelligence warrants. No warrant applications were declined. The GCSB worked proactively with internet service providers to ensure that, as technology changes, warrants can continue to be implemented and assured effectively.

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.

Very Urgent authorisations

(section 221(2)(1)(e) of the ISA

Three very urgent authorisations were made 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. Such authorisations are automatically revoked 24 hours after the authorisation is given if an application for an intelligence warrant is not made.

Urgent warrants

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

Restricted Information

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

Business Records Directions

(section 221(2)(h) of the ISA)

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.

Information requests

The GCSB is subject to the Official Information Act 1982 (OIA) and the Privacy Act 2020. We aim to be as transparent as possible in responding to requests made under these Acts while safeguarding important matters such as the security or defence of New Zealand. Each request is assessed individually, and matters such as national security concerns are considered within the guiding statutory principles. The GCSB aims to complete all information requests within the legislated timeframe.

For the period from 1 July 2022 to 30 June 2023, the GCSB:

- completed 59 OIA requests, with two requests not completed within the legislated timeframe
- completed 23 Privacy Act requests, with one request not completed within the legislated timeframe.

The median response time was 19 working days across all OIA and Privacy Act requests.

TABLE: NUMBER OF INFORMATION REQUESTS COMPLETED

	2018/19	2019/20	2020/21	2021/22	2022/23
OIA	76	51	49	70	59
PA	31	28	27	16	23

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

The GCSB was not notified of any complaints by the Office of the Ombudsman during the reporting period. One complaint received in the previous reporting period was resolved, with the Ombudsman finding in the GCSB's favour.

The GCSB was notified of one complaint by the Office of the Privacy Commissioner during this period. The complaint was resolved to the satisfaction of the Office of the Privacy Commissioner, which found the GCSB had not breached the complainant's privacy.

TABLE: PERFORMANCE MEASURE: MINISTERIAL SUPPORT AND RESPONSES TO INFORMATION REQUESTS

ASSESSMENT OF PERFORMANCE	BUDGET STANDARD	ACTUAL
Advice to Minister responsible for GCSB		
Minister responsible for GCSB satisfaction with GCSB advice.	3.5 or above on a 5 point scale	4.86
Responses to requests for information under the Official Information Act 1982 (OIA) and Privacy Act 2020		
Percentage of agency OIA requests completed within the legislated timeframe.	100%	96.6%
Percentage of agency Privacy Act requests completed within the legislated timeframe.	100%	95.7%

Our Sustainability Reporting

We are working towards 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 our operations.

Independent Verification

The GCSB completed independent emission verification for 2018/19 (our baseline year) and 2021/22. The emissions reported here for 2022/23 have not been independently verified at the time of reporting.

The greenhouse gas emissions measurement (emissions data and calculations) reported in this annual report have been calculated in a variety of ways. These are based on solid supplier data, where it is available and practical, internal records, and an extrapolation of a sample of underlying financial records for certain emission sources.

In 2022/23 we estimate we emitted 2,318 Tonnes CO2-e, based on our sampled data and extrapolation. This compares to our verified figure of 1,777 Tonnes CO2-e in 2021/22. Most of our emissions came from passenger transport, as well as electricity and motor vehicles.

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 1,875 Tonnes CO2-e, or a 21 percent reduction in gross emissions (all Categories) compared to the base year 2018/19.
- **2030 target:** Gross emissions (all Categories) to be no more than 1,376 Tonnes CO2-e, or a 42 percent reduction in gross emissions (all Categories) compared to base year 2018/19.

Initiatives for reducing emissions, and progress towards out these

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.

Now that we have verified baseline year data, we have the opportunity to have more meaningful conversations surrounding the exact emission sources.

Work is underway to develop a carbon reduction plan, for approval in the coming months.

Improving our data

The GCSB is in the early stages of the CNGP. We have identified that we need to make improvements to our emission data collection methods, and are planning on making these improvements over the next year. We have improved our supplier relationships and have better source data quality than previously. We are looking to launch a Carbon data capture process to improve our Carbon data at a transaction level.

Organisational Capability

Ngā Āheitanga Whakaharere

OUR PEOPLE
Ō MĀTAU TĀNGATA

Recruiting and retaining our talent

The Intelligence Community Shared Services People and Capability team provides a number of initiatives to the GCSB and NZSIS, to support the continued growth of their workforces, and to help retain and develop existing staff. This work aims to ensure the NZIC has the best and most representative workforce possible to meet the expectations of the New Zealand Government and the public.

Beyond Ordinary People

The GCSB is a public service department with 539.8 full-time equivalent staff made up from 546 staff, as at 30 June 2023. As we have a number of shared functions with the NZSIS, there are additional staff employed by the NZSIS who work across both agencies.

The success of our agency does not just depend on our technological capabilities, our legal authorities, our strong partnerships or our social licence. Ultimately it depends on the quality, diversity, professionalism and technical capabilities of our people.

In recent years we have faced workforce disruptions from Covid-19, building remediation and increased competition from public and private sectors for the skills and expertise of our people. The GCSB continues to prioritise initiatives to attract and retain a diverse workforce, including competitive remuneration, closing gender and ethnic pay gaps, enabling more flexible working, investing in employee development and fostering an inclusive culture.

Turnover

The GCSB has seen a reduction in staff turnover by 3.7 percentage points – from 19.3 percent in the 2021/22 financial year to 15.6 percent at 30 June 2023. When investigated, employees consistently report the primary reason for leaving is career development.

Our average tenure for permanent staff is 6.3 years. This has decreased by 0.2 years from 2021/22. Over the 12 months to 30 June 2023, the majority of our core workforce (53 percent) who ended their employment with us left between one and five years of joining.

TABLE 1: THE GCSB'S CORE UNPLANNED STAFF TURNOVER (2018 TO 2023)

	2018/19	2019/20	2020/21	2021/22	2022/23
Staff Turnover	12.0%	13.7%	8.1%	19.3%	15.6%
Public Service	11.8%	10.1%	10.5%	17.3%	15.9%

Retention and Recruitment

The tight and competitive labour market, building remediation issues, and the five year high turnover of 19.3 percent in 2021/22 resulted in the GCSB carrying a number of vacancies throughout 2022/23.

We responded by placing significant effort on ensuring recruitment activities were prioritised, and increasing induction intakes to expedite the on-boarding of new employees. Additionally, we completed implementation of our new joint remuneration framework that provides market aligned remuneration for our people and enables us to compete for talent more effectively in the market.

Work was also undertaken this year to improve the end-to-end recruitment process. People & Capability, Technology Directorate and Protective Security collaborated to design a workflow tool to improve transparency across the recruitment pipeline. The tool will be implemented in July 2023 and we look forward realising the benefits of this significant project in 2024.

While the GCSB turnover remains higher than desired, it has continued a steady decline following these activities, returning to 15.6 percent at 30 June 2023.

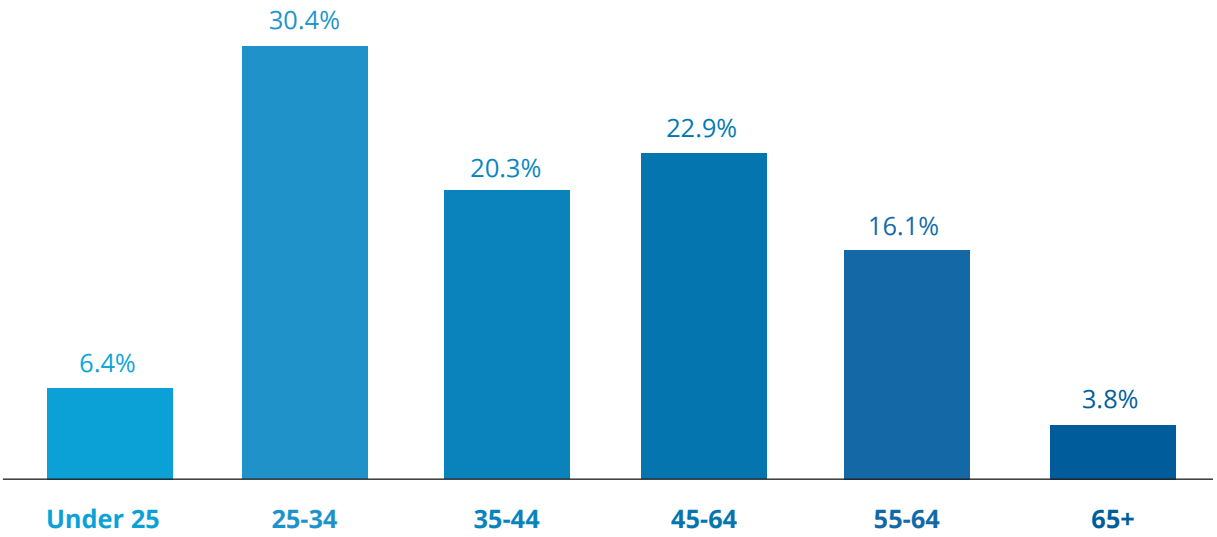
#8

Promoting diversity and inclusion

Age demographics

The majority of our workforce is younger than 45 years old (57.7 percent). This is reflective of our average age (42.3 years), which has decreased slightly by 0.5 years since 2021/22. Of our workforce, almost half (44.3 percent) started within the last three years.

GRAPH: GCSB AGE DEMOGRAPHIC BREAKDOWN AS AT 30 JUNE 2023



Gender diversity

As at 30 June 2023 women made up 60 percent of the GCSB's senior management. We have continued to successfully meet our diversity and inclusion aspiration of women forming no less than 50 percent of our senior management group.

TABLE 2: THE GCSB'S GENDER REPRESENTATION (2018 TO 2023)[3]

	2018/19	2019/20	2020/21	2021/22	2022/23
Senior Management (Tier 2 and 3)					
Men	48.0%	54.5%	47.8%	36.8%	40.0%
Women	52.0%	45.5%	52.2%	63.2%	60.0%
All Staff					
Men	63.8%	64.4%	64.5%	61.1%	63.2%
Women	36.2%	35.6%	34.9%	37.9%	35.5%
Another Gender	–	–	0.2%	0.2%	0.6%
Undisclosed	–	–	0.4%	0.8%	0.7%

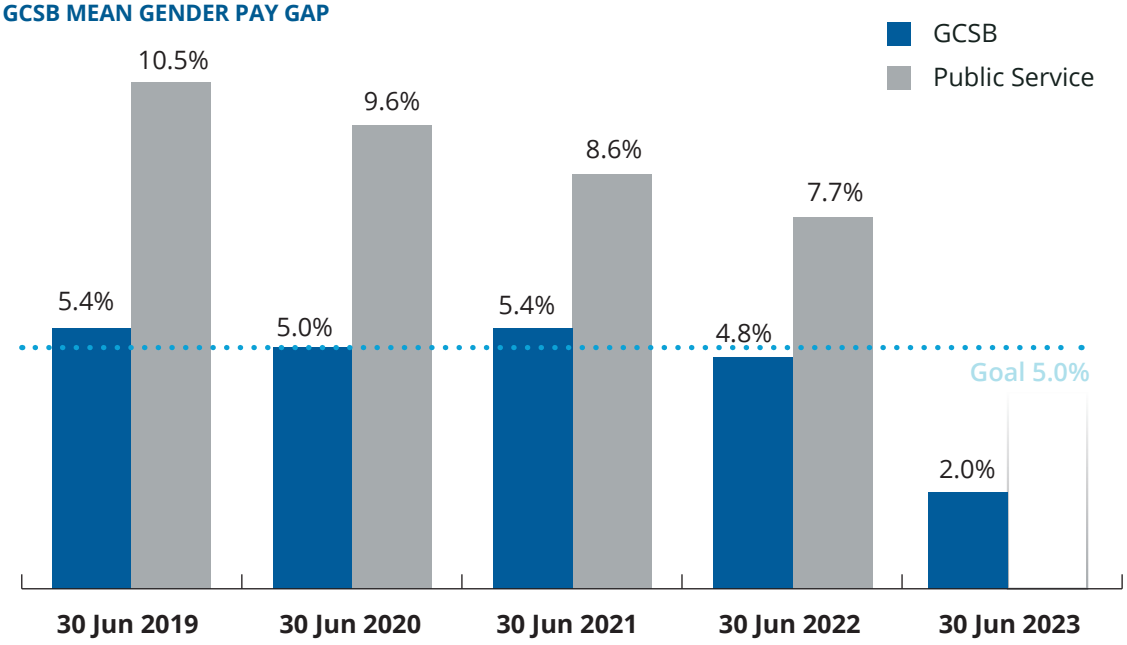
[3] This year we have excluded those roles that are professional, specialist or support staff that do not have a management function as a significant part of their role to align with Te Kawa Mataaho The Public Service's definition of Senior Management.

Gender Pay Gap

Addressing our gender pay gap is a key feature of our 2021-2025 Diversity and Inclusion Strategy. We have met our goal of no more than 5 percent. At 30 June 2023, our average gender pay gap was 2.0 percent. This was a 2.8 percentage point decrease from 2021/22.

In the past year we have seen a decrease in the representation of females at lower paying bands. This has caused the average female salary to increase.

GRAPH: GCSB MEAN GENDER PAY GAP



Ethnic diversity

Staff can choose whether or not to disclose their ethnicity. In our workforce, 93.4 percent disclosed at least one ethnicity, exceeding our targeted percent disclosure rate of 90 percent for robustness of analysis. This is an increase of 0.7 percentage points since last year. Twenty-one percent of staff identify as any of New Zealand Māori, Asian, Pacific Peoples, or MELAA.

TABLE 3: GCSB STAFF DISCLOSED ETHNICITY (2018 TO 2023)[4]

ALL STAFF	2018/19	2019/20	2020/21	2021/22	2022/23
European	67.8%	71.2%	76.0%	74.6%	77.5%
New Zealander[5]	29.4%	26.8%	22.8%	18.5%	-
New Zealand Māori	7.2%	7.3%	7.2%	9.1%	9.8%
Asian	5.4%	5.5%	7.2%	7.3%	7.3%
Pacific Peoples	2.3%	1.6%	2.6%	3.2%	3.1%
MELAA	0.9%	1.1%	1.2%	1.6%	0.8%
Other	–	–	0.2%	0.2%	15.7%

[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 percent. Metrics are taken 'as at 30 June' of the relevant year.

[5] For 2022/23, staff who self-identified their ethnicity as New Zealander fall under "Other" based on Statistics NZ ethnicity groupings.

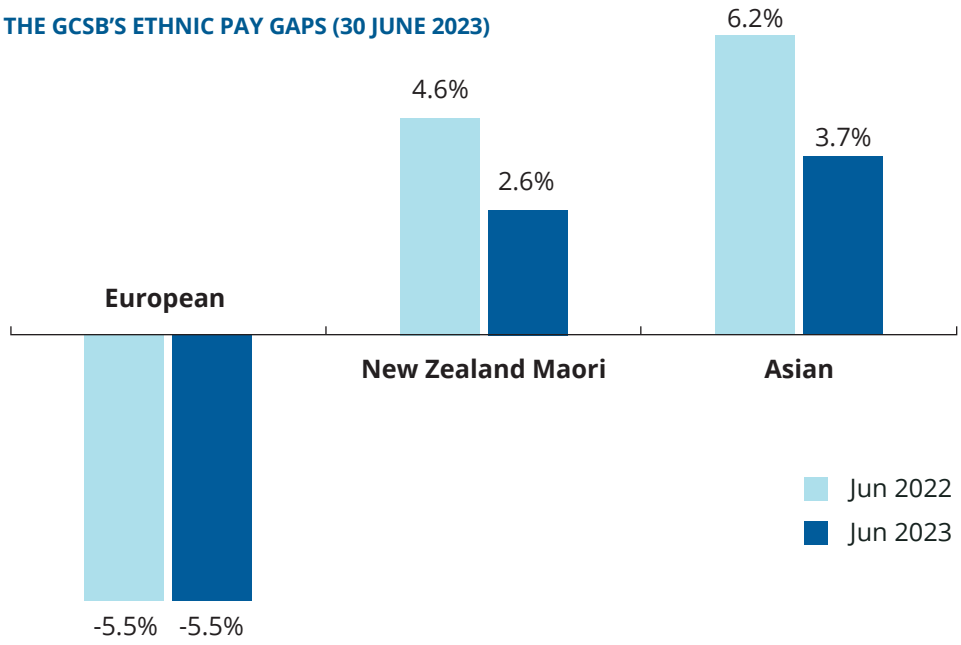
TABLE 4: THE GCSB'S SENIOR MANAGEMENT DISCLOSED ETHNICITY (2023)

SENIOR MANAGEMENT (TIER 2 AND 3)					
European	New Zealand Māori	Asian	Pacific Peoples	MELAA	Other
84.6%	23.1%	–	–	–	11.5%

Ethnic Pay Gaps

European is the only ethnicity with a negative average ethnic pay gap (in favour). This means on average Europeans are earning 5.5 percent more than non-Europeans. We are seeking to improve this.

TABLE 5: THE GCSB'S ETHNIC PAY GAPS (30 JUNE 2023)



Kia Toipoto Pay Gap Report and Action Plan

In 2022 the Public Service Commission Te Kawa Mataaho provided new guidance and expectations for reducing pay gaps. This is known as the Kia Toipoto Pay Gap Action Plan. It is a three year plan focused on addressing all pay gaps – gender, Māori, Pacific, ethnic, and other minorities (i.e. Rainbow and disabled communities).

From August to October 2022 we partnered with staff to develop an action plan for our agency. We developed simple achievable actions for the short, medium, and long term.

Since November 2022 we have:

- Increased the number of ethnicities we can collect information on, and run a campaign to encourage staff to self-identify their ethnicities
- Updated our job and pay band matrix to provide transparent data to staff
- Developed a myth busting booklet to help break down barriers to entry in the NZIC.

Te Kawa Mataaho has openly acknowledged the quality of our report and action plan, highlighting it as an exemplar for the public service.

Neurodiversity Support Group – Stepping into the light

Our employee-led-networks help develop and implement policy, process, and change initiatives. They give valuable insights to help create a culture of belonging. The Neurodiversity Support Group recently helped to review, update and implement our Reasonable Accommodation policy. Collaborative workshops were held with Neurodiversity Support Group members to help the GCSB and NZSIS to:

- Understand what a day in the life of our neurodiverse staff looked like – the challenges they faced and what was working well.
- Explore the future workplace and what was needed to support our neurodiverse staff to thrive.

Members had the opportunity to help shape the policy and ensure what we created addressed the real challenges faced by the neurodiverse community. The Neurodiversity Support Group also came up with the theme "Step into the light", which will be woven throughout associated documentation and communications.

The Neurodiversity Support Group continue to provide support with the implementation of the policy. The group is helping to develop training and education resources for our managers and staff. This will help our people better understand neurodiversity and how they can support, work with, or manage neurodiverse staff.

Winners of the 2022 Diversity Works Leadership Award

Together with the NZSIS we won the Medium-Large Organisation Award in the Leadership category. We were awarded for driving diversity and inclusion across our agencies, and creating a welcoming and inclusive environment.

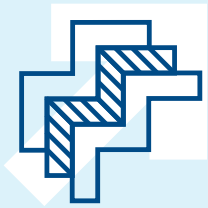
Our application focused on how we have built leadership capability for everyone. We spoke about our targeted diversity and inclusion learning programme for leaders and staff; and how this positively changed our workforce demographics and the experiences of our people.

Our success at the Awards comes down to a genuine belief in diversity and inclusion, supported by strong leadership, and a clear strategy to build a more diverse and inclusive workplace.

Progress against Te Kawa Mataaho Papa Pounamu Commitments

Addressing bias

- 84.48 percent of GCSB leaders and 72.41 percent of our Tier 2 and 3 leaders completed our Understanding & Managing Unconscious Bias learning module.
- We launched the Reasonable Accommodation policy alongside our neurodiverse and disabled staff, and ongoing work to implement training and education for managers and staff.

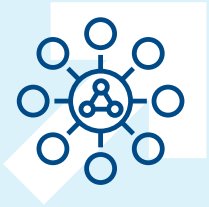


Cultural competence

- 66.38 percent of GCSB leaders have completed the Crown-Māori Relations programme, leading to increased understanding of New Zealand's history and the Treaty of Waitangi.
- Offerings will be expanded in 2023/24 to include workshops on engagement and application in the workplace.
- Continued development of our Māori cultural capability, including design and development of learning resources for managers and staff. More information can be found in our Māori cultural capability section.

Inclusive leadership

- Development of a manager induction pathway is underway, to build management capability in alignment with inclusive leadership practices. Implementation is planned for late 2023.
- Awarded the Leadership Award at the 2022 Diversity Works Awards with the NZSIS, recognising our efforts to drive diversity and inclusion and create a welcoming and inclusive environment.



Employee-led networks

- Regrouped after Covid-19 and building disruptions to reinvigorate our employee-led networks.
- Reviewed how we engage with networks, which resulted in better engagement with senior leadership and increased organisational support with network initiatives.
- Workshop held with networks to better understand what they wanted to achieve in 2023/24 and where support was required.

Building relationships

- Established quarterly morning teas for new and existing staff to introduce our employee-led networks and groups, contributing to enquiries from staff interested in finding out more, or looking to join.
- Supported networks to attend partner diversity and inclusion conferences to enable them learn from others and share our ongoing journey in this space.

TOOLS AND SYSTEMS
NGĀ TAPUTAPU ME NGĀ PŪNAHA

Providing a safe and healthy work place

While our people are focused on the protection of New Zealand, our Health and Safety Team are focussed on the ongoing health, wellbeing and physical safety of our people. We continue to take a pragmatic approach to health and safety, while ensuring that we are complying with the Health and Safety at Work Act 2015.

Risk Management

To reduce the likelihood of low-frequency, high-impact catastrophic incidents our focus continues to identify and improve outcomes for the GCSB critical risks by putting controls and monitoring processes in place.

The Health and Safety Risk Management focus is split across safety risks and psychosocial risks, such as engaging with objectionable material or working unsociable hours.

Infrastructure

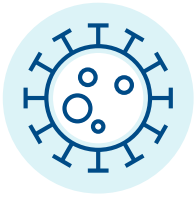
The GCSB entered a period of construction with the ground breaking development of the Data Centre. During this period there was one notifiable event recorded relating to a contracted party being injured. The case was closed without further investigation from WorkSafe NZ.

The GCSB Head Office on Pipitea Street operated at reduced occupancy between December 2021 and June 2023 due to an earthquake risk assessment of the building. Engineers prepared detailed seismic assessments and remedial works was undertaken. The building is now cleared to return to full occupancy.

Worker Engagement and Participation

We focused on improving worker engagement. The inaugural NZIC Health and Safety Representative Conference was held in May 2023 bringing together 33 representatives across the GCSB and NZSIS.

We have a 100 percent completion rate for all new starters completing the Health and Safety Induction Module.



Covid-19

The establishment of the Covid-19 Management Team enhanced our capability and preparedness for future emergencies and incidents.

Covid-19 changed some of the ways we work. We responded to that change and put in systems and processes to promote sustainable worker health and wellbeing.

Annual Safety Performance Scorecard – GCSB

Close calls / non injury	Restricted work Injuries	First aid Injuries	Environmental Events

A restricted work injury is any work-related injury that prevents an employee or contractor from performing one or more of the routine functions associated with their job for a full working day.

All-of-government data centre

We partnered with the NZDF to construct an all-of-government data centre at Royal New Zealand Air Force Base Auckland (Whenuapai) to house New Zealand's sensitive official information. As the government's information security lead, we will operate the data centre on behalf of a range of government agencies.

Final funding was received via Cabinet in June 2022, with earth works commencing on the Whenuapai site in 2021, and construction on the facility beginning in September 2022. Once security milestones in the build had been achieved, the data centre was publicly announced in April 2023 by the Minister Responsible for the GCSB, Hon Andrew Little.

The data centre is expected to be operational by mid 2025, and will provide data storage for agencies for at least 25 years.

MĀORI CULTURAL CAPABILITY
TE WHANAKETANGA O TE AO MĀORI

Ka huri te kei o te waka ki te pae tawhiti
Kia hoe ngātahi ki te pae tata
Ki te whei ao, ki te ao mārama
The waka turns to-wards the distant horizon

Let us collectively make headway and paddle together as one, through the glimmer of dawn to the break of day

This past year has seen the GCSB, together with the NZSIS, succeed in initiatives and efforts to enhance our understanding and integration of Māori culture and values. The GCSB acknowledges it is 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. As part of the NZIC, we have continued to build on last year's progress by seeking out distant horizons, drawing them nearer and holding fast to the achievements in which we attain along the way.

The NZIC has made headway on board our waka. One notable achievement is the introduction of Te Tiriti o Waitangi into our organisational strategy. This key shift is a step towards recognising how Māori values and principles should be incorporated into our operations and shows our strong commitment to being part of an honourable treaty partner.

As we continue on our journey towards te pae tawhiti 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 aspiration for improved cultural capability

To promote capability uplift, the agencies recruited staff with a specific focus on Māori cultural capability. Their role is to build our capability framework and begin language planning; this will outline how we mature as an organisation on this cultural capability journey. This mahi will significantly contribute to how we as a community effectively integrate and improve our understanding of Māori language, customs and culture.

We held Māori capability workshops to ensure all staff are informed and engaged in the capability uplift process. We also conducted a capability survey, which will inform our capability uplift plan and te ao Māori strategy. A high response rate was received, with results indicating a widespread desire among staff to continue improving their understanding and engagement with Māori culture and values.

We remain committed to continuing to build greater understanding of te ao Māori, te reo Māori, tikanga and Te Tiriti o Waitangi (the Treaty of Waitangi / te Tiriti) throughout our day-to-day activities and interactions. The GCSB continues to draw close to our distant horizons.

Whāia kia tata
pursue and draw near

How our progress tracks against the objectives set

We developed interactive pepeha and mihi tools with the NZSIS in the previous financial year. These continued to be popular with staff from both the GCSB and NZSIS this year, with 115 staff accessing the resources. These resources facilitate understanding and engagement with Māori cultural protocols, helping our staff take steps towards improving their cultural competence.

We continued to grow Māori language class options for staff.

We also actively participated in the review of the Intelligence and Security Act 2017 and the national security strategy. Our te ao Māori team provided advice relating to te Tiriti in these reviews, ensuring that the principles of te Tiriti are duly considered in this legislation and policy-making process. We continue our mahi to pursue and draw near our objectives.

Notably, our pōhiri process for new staff Inductions has been updated to better reflect appropriate mihi or whaikōrero. By providing an opportunity for our leaders to welcome staff with the appropriate mihi or whaikōrero we continue to show our commitment to being a culturally responsive workplace.

Whakamaua kia tīna
hold fast to those of which we have attained

Objectives we achieved and celebrate

We continue to strengthen our practice and recognise our achievements. In line with our efforts to promote the principles of te Tiriti, we conducted workshops with leaders, agency partners, and key Māori stakeholders, including Iwi Chairs representatives. This enabled open dialogue and reflection on our roles and responsibilities as a treaty partner. Through this, we are developing our robust te Tiriti framework that helps us promote fairness, equity, and partnership, and represent Māori perspectives in our decision-making processes.

We were proud to reflect Māori customs, values and protocols at the Five Eyes conference we hosted in September 2022. At this, we incorporated Māori practices alongside mana whenua (pōhiri, karakia, whaikōrero, and mihimihi).

We celebrated Matariki 2022, the first Mātauranga Māori public holiday, by organising a hāngī for all staff. This event aimed to foster a sense of unity and appreciation for Māori culture among staff and an opportunity to grow awareness around the significance and importance of this national event.

We also observed Māori Language Week with enthusiasm. This event marked 50 years since the Māori language petition was taken to Parliament. Māori language activities were organised throughout the week to encourage engagement and support for te reo.

We are also proud to have embraced te ao Māori into our induction process, inter-weaving appropriate pōhiri and encouraging our leaders to welcome staff with mihi or whaikōrero. We remain committed to being a culturally responsive workplace.

Hei whakakapi – Conclusion

We acknowledge that while our movement is steady we are making headway on-board our waka towards te pae tawhiti. In the last year we have taken significant steps to understand and embrace Māori culture and values in our mahi. This illustrates the GCSB's desire to uplift Māori capability and our efforts to build a culturally competent organisation. We have a long journey ahead of us and we acknowledge we are still in the phase of gathering resource, however, we are proud of how we are tracking on our journey of 'he waka eke noa'.

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 GCSB's financial statements, and the statement of expenses and capital expenditure, and for the judgements made in them;
- Having in place a system of internal control designed to provide reasonable assurance as to the integrity and reliability of financial reporting;
- Ensuring that end of year performance information on each appropriation administered by the GCSB is provided in accordance with sections 19A to 19C of the Public Finance Act 1989, whether or not that information is included in this annual report; and
- The accuracy of any end of year performance information prepared by the GCSB, whether or not that information is included in the annual report.

In my opinion:

- This annual report fairly reflects the organisational health and capability of the GCSB.
- The Statement of Expenses and Capital Expenditure against Appropriation fairly reflects the total actual expenses and capital expenditure incurred for the year against the GCSB's appropriation for the financial year ended 30 June 2023.

Bridget White

Te Tumu Whakarae Rangitahi mō Te Tira Tiaki
Acting Director-General, of the GCSB

29 September 2023

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 2023

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 2023 on page 59.

Opinion

In our opinion the statement of expenses and capital expenditure against appropriation of the GCSB for the year ended 30 June 2023 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 29 September 2023. 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 2022/23 for Vote Communications Security and Intelligence.

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

As part of an audit in accordance with the Auditor-General's Auditing Standards, we exercise professional judgement and maintain professional scepticism throughout the audit. Also:

- We identify and assess the risks of material misstatement of the information we audited, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for our opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.
- We obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the GCSB's internal control.
- We evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by the Director-General of the GCSB.
- We conclude on the appropriateness of the use of the going concern basis of accounting by the Director-General of the GCSB and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the GCSB's ability to continue as a going concern. If we conclude that a material uncertainty exists, we are required to draw attention in our auditor's report to the related disclosures in the information we audited or, if such disclosures are inadequate, to modify our opinion. Our conclusions are based on the audit evidence obtained up to the date of our auditor's report. However, future events or conditions may cause the GCSB to cease to continue as a going concern.
- We evaluate the overall presentation, structure and content of the information we audited, including the disclosures, and whether the information we audited represents the underlying transactions and events in a manner that achieves fair presentation in accordance with the requirements of the Intelligence and Security Act 2017.

We communicate with the Director-General of the GCSB regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal control that we identify during our audit.

Our responsibilities arise from the Public Audit Act 2001.

Other information

The Director-General of the GCSB is responsible for the other information. The other information comprises the information included on pages 5 to 55, 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 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 (including International Independence Standards) (New Zealand) (PES 1) issued by the New Zealand Auditing and Assurance Standards Board.

Other than in our capacity as auditor, we have no relationship with, or interests in, the GCSB.

S B Lucy
Audit New Zealand
On behalf of the Auditor-General
Wellington, New Zealand

AUDIT NEW ZEALAND
Mana Arotake Aotearoa

STATEMENT OF EXPENSES AND CAPITAL EXPENDITURE AGAINST APPROPRIATION

FOR THE YEAR ENDED 30 JUNE 2023

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

	$000
Total appropriation	$319,707
Actual expenditure	$238,716

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