



**Te Tira Tiaki**  
Government Communications  
Security Bureau

**Annual Report 2024**  
**Te Pūrongo ā-Tau 2024**





## Preface

This is the annual report of the Government Communications Security Bureau (GCSB) for the year ended 30 June 2024, presented for consideration and scrutiny by the Intelligence and Security Committee.

This report is presented to the House of Representatives pursuant to section 221 of the Intelligence and Security Act 2017.

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



Director-General's Overview   Te Tiro Whānui a te Tumuaki Ahurei	5
<b>Who We Are and What We Do</b>	
<b>Ko Wai Mātou, ā, he Aha Hoki ā Mātou Mahi</b>	<b>7</b>
Overview   Tirohanga Whānui	8
Who We Are   Ko Wai Mātou	9
Organisational Strategy   Te Rautaki Whakahaere	10
Māori Cultural Capability   Te Whanaketanga o te Ao Māori	12
Our Partnerships   Ō Mātau Rangapūtanga	13
Year at a Glance   Te Rarapa i te Tau	16
<b>Our Work in Detail</b>	
<b>He Tirohanga Hōmiromiro ki ā Mātau Mahi</b>	<b>19</b>
Intelligence Advantage	20
The Pacific	22
The GCSB's Role and Remit for Cyber Security	23
Supporting the National Security Sector	33
Accountability and Transparency   Te Noho Haepapa me te Pūataata Hoki	35
<b>Organisational Capability</b>	
<b>Ngā Āheitanga Whakaharere</b>	<b>39</b>
Our People   Ō Mātau Tāngata	40
Our Finances   Ā Mātau Pūtea	48
<b>Financial Statements</b>	
<b>Ngā Tauākī Pūtea</b>	<b>49</b>
Statement of Responsibility	50
Independent Auditor's Report	51
Statement of Expenses and Capital Expenditure Against Appropriation	54





# Director-General's Overview

## Te Tiro Whānui a te Tumuaki Ahurei

**It is my privilege to bring you our first Government Communications Security Bureau (GCSB) annual report since I took up the role of Director-General in October 2023. I'd like to begin by acknowledging the leadership of Bridget White, who led the GCSB as Acting Director-General for the first part of this reporting year.**

The GCSB exists to help uphold New Zealand's democratic way of life. This undertaking was brought into sharp focus this year when, together with impacted partners, the New Zealand Government called out the People's Republic of China for an earlier intrusion into New Zealand's Parliamentary digital network.

This state-sponsored cyber intrusion is emblematic of the evolving nature of our security environment. While quick actions by the affected organisations and the technical expertise of the National Cyber Security Centre (NCSC) limited the extent of this intrusion, cyber threats to New Zealand's digital infrastructure are changing and growing. Together with our partners, we continue to defend against an increasingly complex array of threats.

Our operating environment across all of our work streams remains demanding. Geopolitical tensions continue to intensify as traditional great powers become increasingly polarised. Large-scale conflicts are taking place around the globe, including the illegal and unprovoked Russian invasion of Ukraine – now in its third year – and the Israel-Gaza conflict, which at the time of writing has the potential to spill into a yet broader conflict.

The pace of geopolitical deterioration in recent years, and its impact on the rules-based architecture, has placed a greater significance on the GCSB's unique and legally mandated capabilities. Our mission is to provide our customers with intelligence advantage and cyber resilience to successfully navigate an unpredictable world. This means better understanding the implications of conflict, including displaced populations and humanitarian crises, the erosion of rules-based norms,



disrupted supply chains and increased commodity prices. It also means understanding when some states are working counter to our values.

We also see activity of concern in our region. The Pacific faces a range of security issues, the most existential of which is climate change. However, we also note the familiar threats of transnational crime, corruption and foreign interference.

New Zealand's national security is intrinsically connected to the Pacific region. The strong relationships New Zealand has across the Pacific are of great significance to us.

We are also focused on national security threats within our borders. Over the past year we have partnered with domestic agencies to help disrupt a range of threats targeting New Zealand, including foreign interference, transnational criminal operations and violent extremist threats.

The GCSB makes a unique and highly valued contribution to global counter-terrorism efforts, including assisting with the disruption of attack planning. In addition to formally designated terrorist entities, this work has also focussed on identity motivated violent extremists. As current global conflicts and tensions increase, our efforts to counter terrorism will likely rise.

An enduring function of the GCSB is to support the safety of New Zealanders overseas, where there is a national security nexus. This includes supporting the safety of New Zealand Defence Force (NZDF) personnel, some of whom are stationed in conflict zones. In the reporting year, New Zealand sent personnel to the United States-led coalition working to uphold maritime security in the Red Sea, while sustaining the deployments of other NZDF personnel to various commands in the Middle East.

Returning to our cyber security mission, in the reporting year we recorded 7,122 incidents, of which 343 had the potential to cause high impact at the national level. Of these, 32 percent indicated links to state-sponsored actors, while 19 percent were likely criminal or financially motivated. Similar to last year, the most significant incidents we recorded were predominantly associated with ransomware or other extortion activity. The other 6,779 incidents mostly affected individual New Zealanders or small to medium businesses. While these did not require specialist technical attention, they remain highly impactful for those they affect.

The publicly attributed PRC cyber-attack on New Zealand Parliamentary systems in 2021 underscores why New Zealand needs robust and resilient cyber security. Our capability to defend New Zealand against threats such as these is expanding. Alongside our CORTEX suite of services, our Malware Free Networks® (MFN) service provides real-time detection and disruption of cyber threats. This is delivered through third-party cyber security services, and internet and mobile providers. As at the end of this reporting year, MFN had clocked up more than 10 million malicious cyber disruptions since its launch in 2021. To date, it has protected New Zealanders from 5.5 million attempts to find and exploit vulnerabilities, 3.3 million phishing links, and 4,000 attempts to download malware.

Our mandate to build New Zealand's cyber resilience to cyber-attacks also expanded this year. In July 2023, the Government announced the integration of New Zealand's Computer Emergency Response Team (CERT NZ) with the GCSB to create a single lead operational cyber security agency for New Zealand. Prior to this integration, the NCSC's support focused on government departments, key economic generators, niche exporters, research institutions and operators of critical infrastructure. With the integration of CERT NZ, our support is extended to a wide range of businesses, organisations and individuals who may be affected by cyber security incidents.

This reporting year, we stepped up our efforts to assist Pacific governments to bolster their cyber resilience. Our cyber security work now goes beyond our borders through our Pacific Partnership Programme, which provides cyber security support and capacity building, further strengthening resilience in the Pacific region.

The cyber threats we face are evolving at a remarkable pace, and so too must the public sector's approach to security as our digital infrastructure shifts further into a modern domain, and emerging technology, such as artificial intelligence and quantum computing play a larger role in our lives.

A critical part of the Government's future digital infrastructure is nearing completion with the all-of-government data centre at RNZAF Base Auckland (Whenuapai). Once completed, we will operate the facility on behalf of a range of New Zealand Government agencies, assisting them to securely store their most protected information. This build helps strengthen not just the GCSB's resilience but also that of other New Zealand Government agencies.

Resilience is a particular focus for us as we look to the future, not only in securing our information but in ensuring the GCSB is on financially sustainable footing. We have delivered Budget 2024 savings for the next financial year, and we have an agency-led programme in place to operate within our means.

Our ability to achieve our mission relies on our specialist intelligence and cyber security capabilities, our legal mandate, and our international and domestic partnerships. We must remain focussed and equipped to meet the challenges of a deteriorating international security environment.

Most of all though, our ability to achieve our mission depends on our diverse and talented workforce. Our people continue to demonstrate great resilience and stamina through several complex and challenging issues. To all those who have supported our mission this year, I thank you.

Ngā mihi nui,

**Andrew Clark**

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

# Who We Are and What We Do

## Ko Wai Mātou, ā, he Aha Hoki ā Mātou Mahi

Overview	8
Who We Are	9
Organisational Strategy	10
Māori Cultural Capability	12
Our Partnerships	13
Year at a Glance	16

PUZZLE #2

666#88#777#0#6#444#7777#7777#444#666#66#0#444#  
7777#0#8#666#0#7#777#666#888#444#3#33#0#666#88#  
777#0#222#88#7777#8#666#6#33#777#7777#0#9#444#  
8#44#0#444#66#8#33#555#555#444#4#33#66#222#33#  
0#2#3#888#2#66#8#2#4#33#0#2#66#3#0#222#999#22#  
33#777#0#777#33#7777#444#555#444#33#66#222#33#  
0#8#666#0#7777#88#222#222#33#7777#7777#333#88#  
555#555#999#0#66#2#888#444#4#2#8#33#0#2#66#0#  
88#66#7#777#33#3#444#222#8#2#22#555#33#0#9#666#  
777#555#3#0#2#2#222#3#33

# Overview

## Tirohanga Whānui

**The Government Communications Security Bureau (GCSB) is New Zealand's lead agency for signals intelligence (SIGINT) and provides intelligence to government customer agencies. It is also the lead operational agency for cyber security, through the National Cyber Security Centre (NCSC).**

Our mission is to provide our customers with intelligence advantage and cyber resilience to successfully navigate an unpredictable world. The GCSB is a crucial part of how our country makes sense of the world and manages national security threats.

### Who We Are – Whakapapa

The GCSB is a public service department, comprised of staff from across New Zealand's society working in a variety of roles. As at 30 June 2024, we have 596.7 full-time equivalent staff, made up from 605 staff. We strongly value the diversity that each person brings to our mission. Our close connection to the New Zealand Security Intelligence Service (NZSIS) is

recognised through our people, with roles in shared functions supporting both the GCSB and the NZSIS. Our whakapapa is built on respect for what has come before and pride in the unique things only we can do for New Zealand.

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 continues to evolve alongside technological developments. We continually assess and update our capabilities to ensure they fully contribute to the New Zealand Government's priorities.

The evolution of technology led to our role in New Zealand's cyber security. This role originally focussed on support to nationally significant organisations and the public sector. Following the integration of CERT NZ with the NCSC in August 2023, this mandate was expanded to a whole-of-economy remit. We continue to 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. 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 NCSC works to strengthen New Zealand's cyber security resilience. This includes ongoing work across Government and critical infrastructure organisations to ensure the data and online services that New Zealand relies on are protected against all hazards and risks. We host the Government Chief Information Security Officer (GCISO) function and provide system stewardship of information security for the public sector.

We are also responsible for providing cyber security advice and education to all New Zealanders, offering support to New Zealanders who have been the target of malicious cyber activity, and for helping to support cyber security resilience in the Pacific.

### 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 64. 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.

Public sector agencies were asked to identify savings through the Budget 2024 process. The GCSB will be making savings of \$7.62 million per year from 2024/25, through efficiencies in areas such as contractor and consultant spending, training and development, and travel.

In addition, funding of \$5.742 million over four years that had been set aside in a tagged contingency for the GCSB in Budget 2023 to expand the mandate of the GCISO to Crown Agents was returned. The GCISO mandate, refreshed by Cabinet in 2023, will not change. This function will continue to be delivered in support of existing mandated agencies.

# Organisational Strategy

## Te Rautaki Whakahaere

Our organisational strategy came into effect from 1 July 2023. It sets out the contribution the GCSB strives to make to New Zealand's national security and economic wellbeing, guiding our activities from 2023 to 2027. It has also informed our refreshed performance measures, reflecting our ongoing work to protect and build resilience, catalyse, and be a trusted organisation.

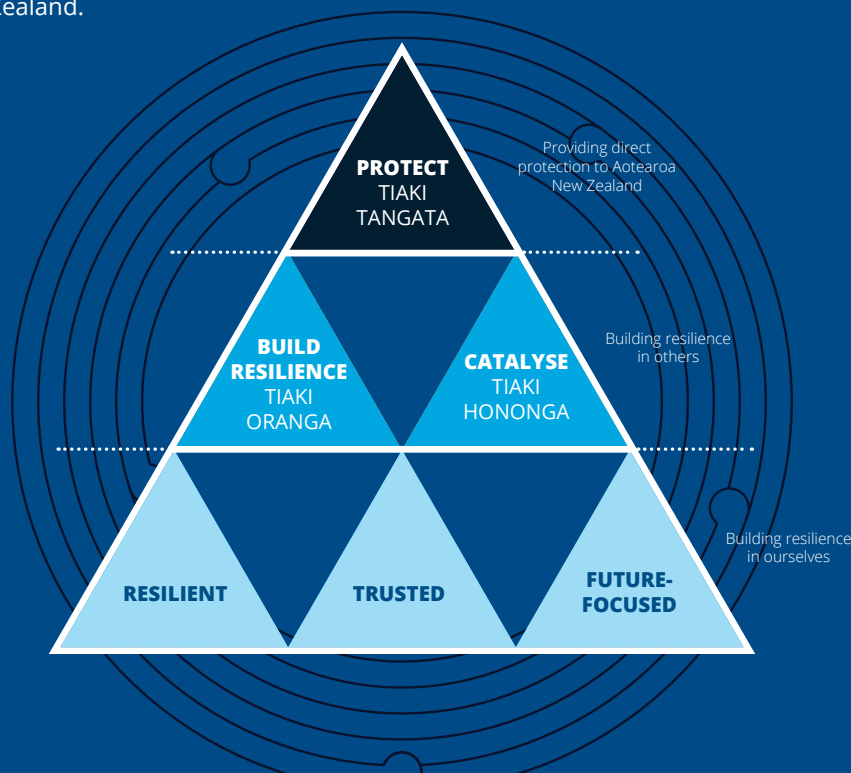
This strategy shaped our work over the reporting year, supporting us to deliver on our mission to equip our customers with the intelligence and cyber resilience necessary to forecast and successfully navigate New Zealand's changing strategic environment.

Our organisational strategy is formed around six outcomes. Three focus on what we do 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

These outcomes are underpinned by our six key shifts. Through pursuing our strategy these are the key shifts we will achieve for New Zealand.

- **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.





## KEY SHIFTS

1

### **Deep insights on regional security – for New Zealand and for the Pacific.**

We will prioritise our work on regional security to ensure the New Zealand Government has deeper insight and forewarning on the array of security challenges facing the Pacific. We will develop our role in building regional resilience by providing support to government agencies whose responsibilities include responding to security issues in our region.

4

### **Lift New Zealand's ability to keep pace with emerging technology risks and opportunities.**

We will employ a more structured approach, which combines insight from all of the GCSB's functions and capabilities, to assist the Government to keep pace with the risks and opportunities that emerging technologies present to New Zealand.

2

### **Consolidate national cyber security leadership.**

We will establish the GCSB's role as the lead agency for cyber security operations in New Zealand. We will consolidate reporting pathways and response triage for cyber security incidents.

5

### **Catalyse our customers' use of intelligence.**

This strategy is designed to get the GCSB working in a cross-mission way, so that our customers benefit from the full range of what we have to offer. We will join the dots for our customers, including on how they can use our products, advice and services.

3

### **Embed our responsibilities as a Treaty partner to advance cyber resilience with iwi, hapu and Māori organisations.**

We will work with partners to define and give effect to our role in lifting the cyber resilience of iwi, hapu and Māori organisations.

6

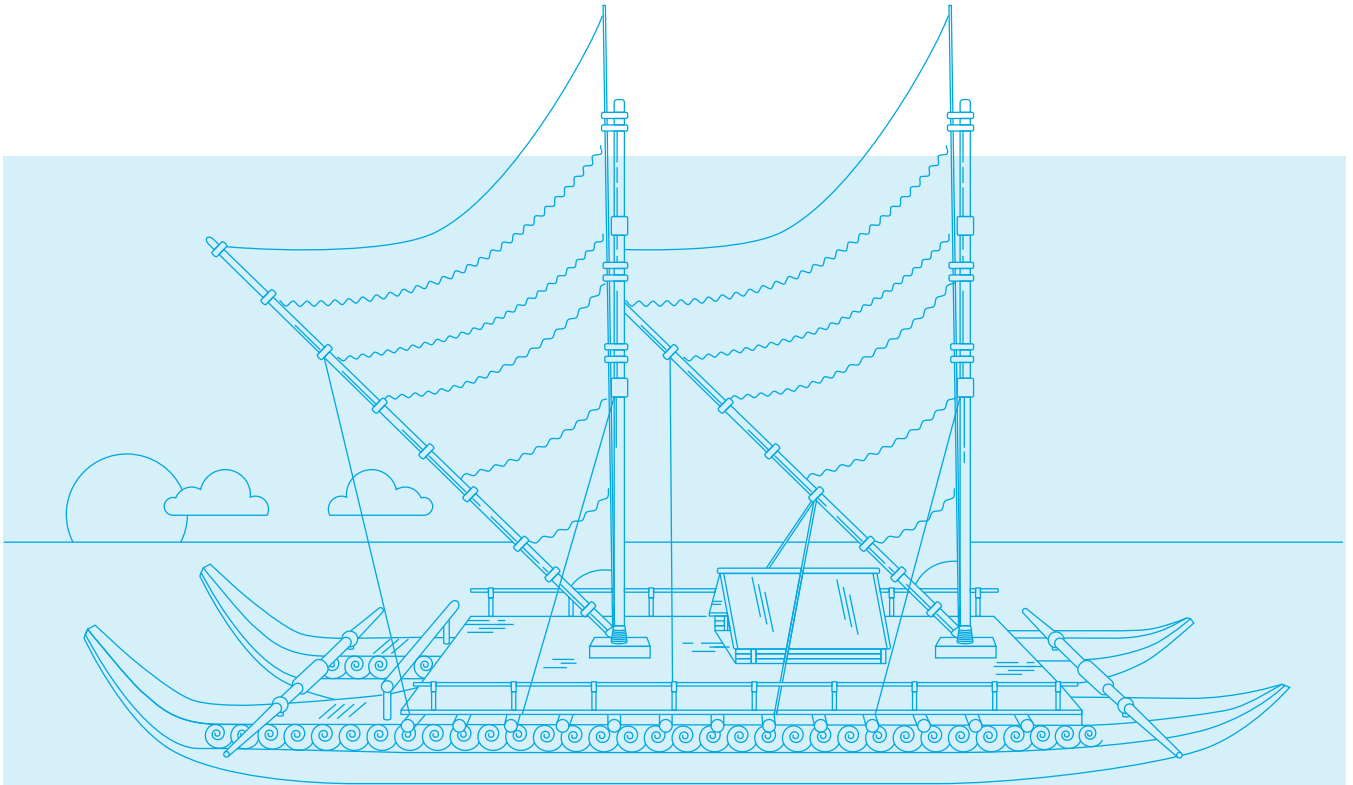
### **Positioning ourselves to effectively meet security challenges and increased demand.**

We have a focus on continuing to make the GCSB a great place to work, prioritising our recruitment and our physical work environment. We will modernise our workplace, enhancing how we connect and collaborate with our customers, partners and suppliers and build adaptability to short-term shocks and longer-term changes in our operational environment.

As part of our commitment to improve public trust and understanding of the value we bring to New Zealand, this year we made our strategy publicly available on the GCSB website.

# Māori Cultural Capability

## Te Whanaketanga o te Ao Māori



**Kua huri te kei o te waka ki te pae tawhiti,  
kua tīmata te hoe ngātahi ki te pae tata,  
ā, e tere ana te waka ki te whei ao, ki te ao mārama**

The waka has turned towards the distant horizons and set sail, we have collectively begun making headway on-board this kaupapa and continue to paddle together as one, through the glimmer of dawn to the break of day

The GCSB and the NZSIS have a shared Te Ao Māori team, which played a pivotal role in the reset of our organisational strategy. This ensured that kaupapa Māori principles are woven into objectives and waypoints aimed at improving national security outcomes for iwi, hapū, Māori partners and organisations.

The GCSB has set three initial objectives for this kaupapa:

- Continue to build positive relationships with iwi at each of our locations
- Work with iwi and Māori organisations to support them in securing their digital information and systems, and
- Continue to build the GCSB's own cultural competence.



# Our Partnerships

## Ō Mātau Rangapūtanga

### Domestic Partnerships

As part of New Zealand's national security community, we work together with a range of agencies and organisations to help enhance our national and regional 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).

We work most closely with the NZSIS, sharing a number of enablement functions including People and Capability, Technology Directorate, Financial 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. This is aided by our agencies' co-location.

Together with the NZSIS, we published a Joint Statement of Common Purpose this reporting year. While the GCSB and NZSIS each has its own strategic focus and unique identity, the nature of our work and the complex threat environment we face create a strong partnership between us. Our joint statement speaks to the functions we share and our commitment to aligning with each other for greater national security outcomes.

We also work alongside other agencies, such as New Zealand Police, New Zealand Customs Service, and Immigration New Zealand, to contribute to our national security and the wellbeing of New Zealanders.

The NCSC engages with organisations in the public sector, to help build understanding of their cyber security risk and provide guidance. 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. We partner with the private sector to deliver our cyber defence capabilities at scale. We also engage with the digital supply chain to increase cyber resilience for New Zealand users.

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

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 strives to advance New Zealand's international interests and reputation. We articulate New Zealand's national security priorities and interests on a global stage in our work with international partners.

## International Partnerships

The reporting year has seen the beginning of a foreign policy reset by the New Zealand Government, reflecting the changing geostrategic landscape and the role New Zealand plays in this. 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.

We value the international partnerships we have with like-minded states. Our relationships with a range of regional and international security and intelligence partners are significant to New Zealand. This includes the international intelligence and security partnership known as the Five Eyes, which is comprised 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.

Our engagement with international partners aligns with New Zealand's foreign policy and the New Zealand Government-set National Security Intelligence Priorities. These are enduring priorities across successive governments, subject to rigorous oversight.

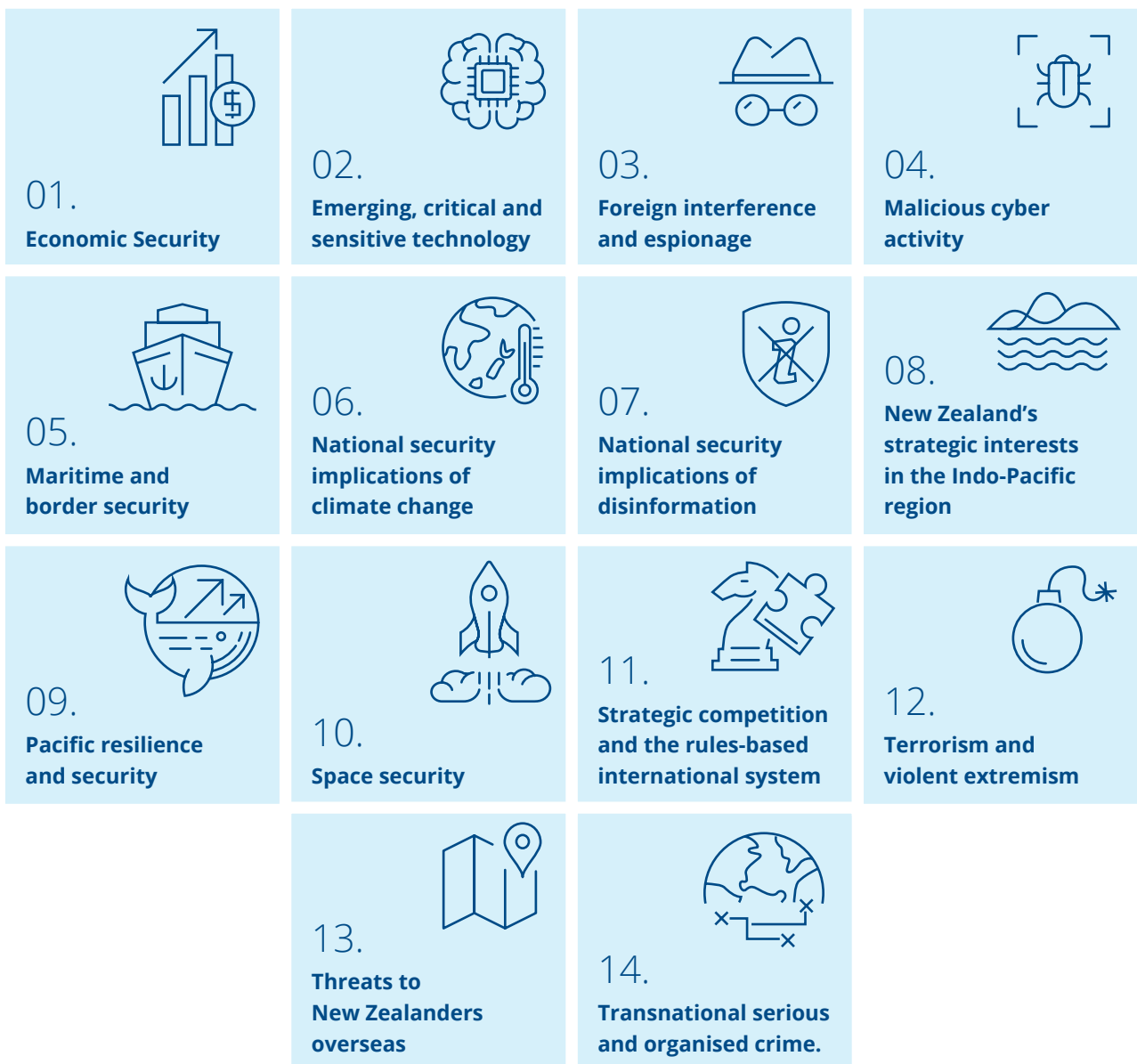




# National Security Intelligence Priorities Whakaarotau Marumaru Aotearoa

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. These NSIPs were agreed by Cabinet in June 2023. Further information about the NSIPs is available on the Department of the Prime Minister and Cabinet (DPMC)'s website.

Our work is guided by, and contributes to, all of the NSIPs:



# Year at a Glance

## Te Rarapa i te Tau

---



# 10.3m

10,334,448 Cyber threats disrupted by Malware Free Networks®.

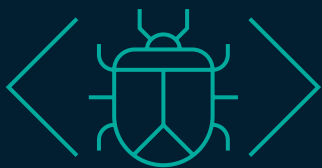
---



# 343

Cyber security incidents triaged for specialist technical support because of the potential to cause high impact at the national level.

---



# 6,779

Cyber security incidents handled through general triage process, often affecting individual New Zealanders or small to medium businesses.

---





**30**

Vulnerability alerts published.



**\$38.8m**

Approximate harm prevented through CORTEX.



**143**

Network change proposal notifications.



**21**

Assessments of regulated space activities.



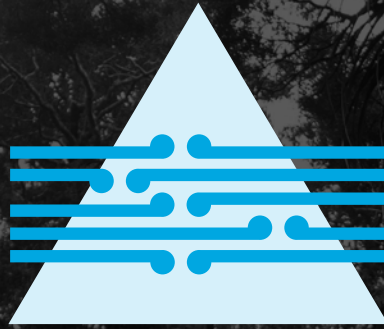
**74**

Assessments of regulated radio spectrum activities.



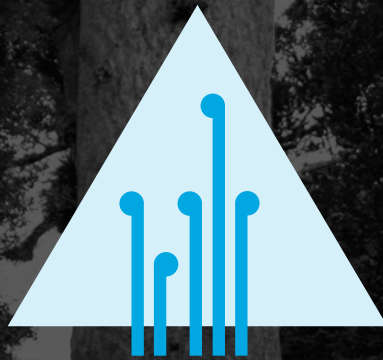
**27**

Intelligence warrants.



## **PROTECT TIAKI TANGATA**

We protect New Zealand  
Aotearoa; our people,  
infrastructure and information.



## **BUILD RESILIENCE TIAKI ORANGA**

We build resilience in others so that  
New Zealand Aotearoa can confidently  
navigate future security challenges.





# Intelligence Advantage

As New Zealand's signals intelligence (SIGINT) agency, our role involves collecting and analysing electronic communications of significance to national security to produce intelligence. When appropriate, these products include intelligence sourced through our international partnerships.

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.

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 Parliament's Intelligence and Security Committee.

## **Regional Security and Geostrategic Competition**

What happens in the Pacific has a fundamental impact on New Zealand's own national security, prosperity and identity. We provide 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 and the wider national security system to understand how New Zealand's people and sovereign structures are at risk from the foreign interference activities of other states. The NZSIS leads the NZIC's efforts to identify and understand foreign interference activity by other governments.

## **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. 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 formally designated terrorist entities and identity-motivated violent extremists.

Violent extremist attacks worldwide continue to be inspired by online extremist rhetoric. The spread of extremist content and ideologies online remains a threat to New Zealand's 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

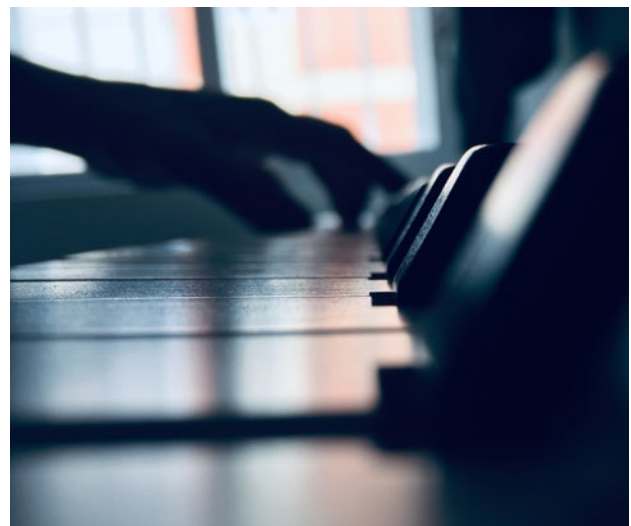
The Intelligence Customer Centre leads the provision of intelligence products to customers on behalf of the GCSB, NZSIS and DPMC. Our customers have a single point of contact and get the right information at the right time in a coordinated way. This is done through a range of activities, including in-person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

## Sharing of Intelligence

The GCSB shares a significant amount of intelligence with foreign parties. This includes processing requests from Five Eyes partners to on-share GCSB intelligence with other parties. When the GCSB considers requests to share intelligence, we consider human rights risks alongside other considerations, such as whether the intelligence sharing may disclose intelligence sources or methods, or provide support to military operations.



Image: NZDF Supplied



# The Pacific

Events of national significance in the Pacific have a fundamental impact on New Zealand's own national security, prosperity and identity.

We and our Pacific neighbours exist in a security environment that is increasingly challenging for governments to navigate. The strong relationships New Zealand has with our Pacific neighbours are of great significance to us.

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 has a detrimental effect on regional security. Transnational organised crime also impacts the security of the region.

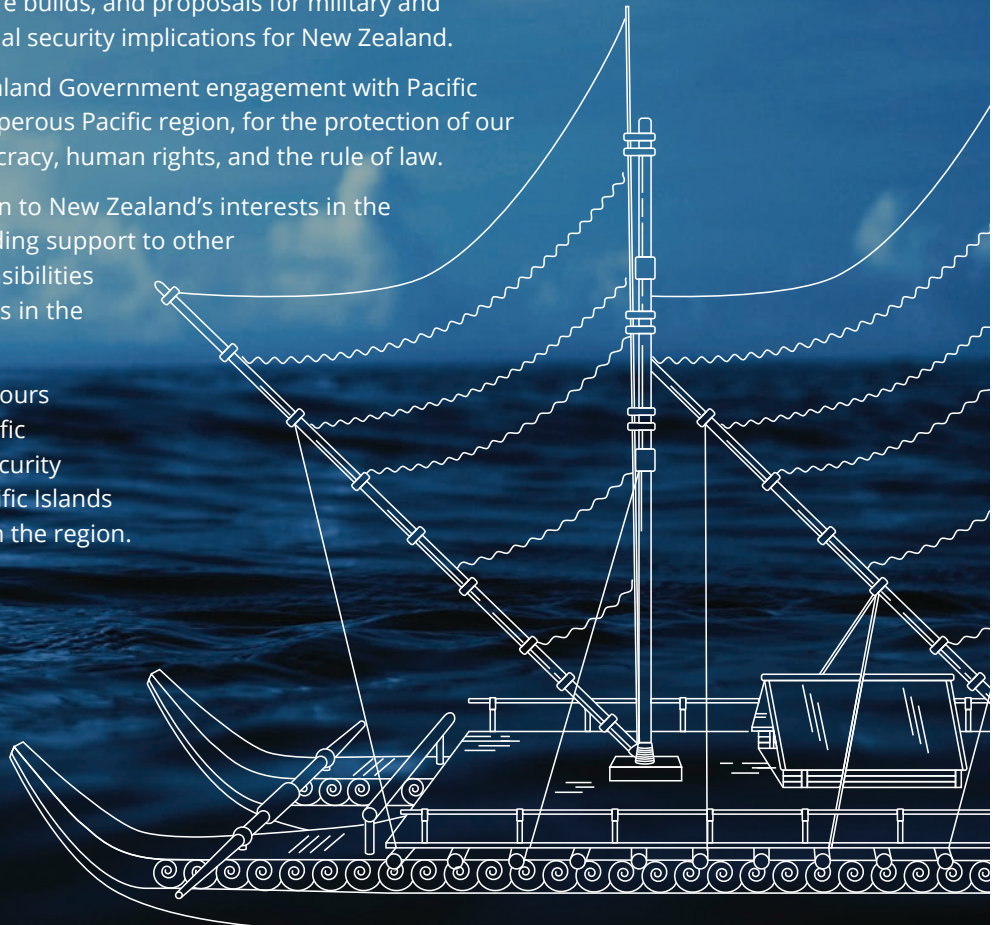
One of the Government's National Security Intelligence Priorities is "Pacific resilience and security", which focuses on understanding domestic and regional security issues in Pacific countries - those located in the New Zealand Realm, Polynesia, Melanesia, and Micronesia. This priority reflects the interconnectedness of the Pacific region and New Zealand's security.

An increased number of countries compete for influence in the Pacific region through developmental funding, infrastructure builds, and proposals for military and security cooperation. This has national security implications for New Zealand.

Our role is to support wider New Zealand Government engagement with Pacific partners to enable a stable and prosperous Pacific region, for the protection of our shared fundamental values of democracy, human rights, and the rule of law.

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.

We also work with our Pacific neighbours to improve cyber resilience. Our Pacific Partnerships team provides cyber security support and capacity building to Pacific Islands countries, building cyber resilience in the region.





# The GCSB's Role and Remit for Cyber Security

One of our core functions under the Intelligence and Security Act 2017 is to provide security advice and assistance, including conducting information assurance and cyber security activities. Our National Cyber Security Centre (NCSC) provides cyber security services to New Zealanders to support this remit.

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.

We work to strengthen New Zealand's cyber security resilience against these threats, helping our digital environment to withstand adversity. Our efforts to build cyber resilience include ongoing work across Government and critical infrastructure organisations to ensure the data and online services New Zealand relies on are protected against all hazards and risks. In addition, through our Director-General's role as Government Chief Information Security Officer (GCISO), we provide system stewardship of information security for the public sector.

Following the integration of CERT NZ, we are also responsible for providing cyber security advice and education to all New Zealanders, offering support to New Zealanders who have been the target of malicious cyber activity, and for uplifting cyber security resilience in the Pacific.

Cyber threats are commonplace and becoming more complex. New technologies and threats continue to emerge, challenging existing cyber security practices. Incidents are having a larger impact on New Zealanders, causing economic and social harm. Cyber security is a core national security issue, as set out in the National Security Strategy. Together with DPMC, we are jointly responsible for leading New Zealand's response to cyber security challenges.

Our cyber security remit is extensive – we are responsible for helping protect New Zealand from the most advanced cyber threats, while also providing support and advice to individual New Zealanders and New Zealand organisations when they are affected by cyber incidents.

We fulfil this remit through the following functional domains:

- **We guide and govern** cyber security decision making by developing standards, frameworks, policy advice, and governance.
- **We identify and understand** the New Zealand cyber security landscape to inform policy and operational decision-making.
- **We prevent and protect** New Zealand's critical and classified information systems to reduce the potential impact of threats.
- **We detect and contain** malicious activity impacting New Zealand through our technical capabilities and partnerships.
- **We respond and recover** to reduce the impact of incidents by providing advice and incident response services across the whole economy.

## The 2023/24 Year at a Glance

This was a year of significant change for the NCSC. We integrated with CERT NZ to become the lead operational cyber security agency for New Zealand, expanding our remit from nationally significant organisations and the public sector to include all New Zealanders.

### Integrating CERT NZ with NCSC

In July 2023, Cabinet designated the GCSB as the lead government agency with whole-of-economy responsibility for cyber security operations. To give effect to this authority, the Government directed the transfer of CERT NZ from the Ministry of Business, Innovation and Employment to the GCSB. This transfer took place in August 2023.

In the immediate months after the transfer, CERT NZ remained a separate branch within the NCSC to ensure minimal disruption to staff and customers. Over the 2023/24 financial year, a new organisational structure was developed to more effectively align the two functions. We look ahead to the 2024/25 financial year with a merged organisational structure, upcoming co-location, and ongoing activity to align our products and services.

We continue to closely monitor the changing cyber landscape. As noted earlier, this year we recorded 7,122 incidents. Of these 6,779 were handled through our general triage process. Often these incidents impacted individuals or small to medium businesses. The other 343 incidents were triaged for more specialist technical support because of the nature of the victim, or the nature of the incident. These incidents have the potential to cause high impact at the national level.

Our annual Cyber Smart Week event took place in October 2023. This year, we created our 'EXPOSED' campaign, which told the real stories of 10 New Zealanders affected by cyber incidents. The week was successful, with over 1,200 businesses supporting the campaign, and 19,000 visits to the new Own Your Online website. Research showed that 70 percent of people who saw the campaign took action to be more secure online.

In March 2024, we called out malicious cyber activity targeting the Parliamentary Counsel Office and the Parliamentary Service. Our analysis of the tactics and techniques used by the actor enabled us to confidently link the actor to a PRC state-sponsored group known as APT40. We worked with the affected organisations to develop a comprehensive remediation plan, and joined partners in calling out these cyber actors.

This reporting year saw us undertake a review of our practices and procedures, to ensure we better consider the wider implications of cyber security incidents beyond our technical response. This review arose following phishing activity targeting members of the Inter-Parliamentary Alliance on China, where, although the malicious cyber activity was unsuccessful, the potential victims of the activity were not notified by the NCSC. The review showed there were aspects of our practice that could be improved and, at close of the reporting year, are working to implement the recommendations.

We also continued to advance our existing services and capabilities. This reporting year, our flagship Malware Free Networks® (MFN®) threat detection and disruption service achieved over 10 million disruptions since its launch in 2021. This is a significant increase from last year's reported number of 390,000 disruptions, and reflects in part the uptake by partners including One NZ and Spark. MFN has helped New Zealanders avoid costly security incidents, and it makes a real difference to everyday New Zealanders' lives. The positive impact MFN has had on New Zealand's cyber threatscape received acclaim this reporting year, winning the 2023 Te Hāpai Hapori Spirit of Service Award for Service Excellence, as well as winning the overall Prime Minister's Award.

## The Threat Landscape

The GCSB continues to observe increasingly complex cyber threats from a growing number of sources, enabled by rapid advancements in technology, such as artificial intelligence, and the ever-increasing connectivity of devices and networks.

Malicious cyber actors are more agile in adapting to new technological environments, and they regularly change their methods in response to shifts in the cyber ecosystem. This includes the use of remote access operations, mass-exploitation of software vulnerabilities, supply chain compromises, and human-enabled cyber operations. Techniques, including sophisticated botnets and living off the land, continue to enable malicious cyber actors to evade detection and strengthen their ability to conduct successful computer network exploitation operations.

Globally, there has been a rise in the targeting of critical infrastructure. Government and critical infrastructure networks in New Zealand are almost certainly high-priority targets for both state-sponsored and financially motivated cyber criminals. State-sponsored actors likely intend to target these sectors for espionage activity, including the gathering of non-public government information, research data and intellectual property. Cyber criminals are attracted to these targets given disruption of important services may increase the chances of financial compensation. Operational technology connected to the internet and into corporate networks without proper controls also creates vulnerabilities for malicious cyber actors to breach these critical systems.

Cybercrime (such as ransomware) poses an immediate and widely experienced threat to New Zealand. Cyber-criminal activity is inherently opportunistic, but there is fast growth in its evolution owing to the worldwide industry of enablers, including access brokers and extortionists. Ransomware actors are increasingly taking advantage of exfiltrated data to extort payment from their victims, increasing the potential for reputational and economic harm, and impact to critical services. State-sponsored cyber threat actors have also employed ransomware directly in their operations, both as a precursor to physical warfare and for profit.

State-sponsored malicious cyber activity remains the most significant espionage threat to New Zealand organisations. New Zealand's position in the world, including our international relations, involvement in global organisations, technological innovations and research is likely considered information of high intelligence value. State-sponsored cyber actors continue to demonstrate the intent and capability to target us for its acquisition.

### Living off the Land

Living off the land refers to a technique used by malicious cyber actors to use tools already in their targeted environment to carry out an attack, rather than require the installation of scripts or codes within the target system. This can conceal the malicious cyber activity and make it harder for such attacks to be detected.

Cyber threat actors, including PRC and Russian state-sponsored actors, have been identified as using living off the land techniques in compromised critical infrastructure organisations. The US has observed indications of actors maintaining access and footholds for at least five years.

The NCSC joined international partners in publishing joint guidance in February 2024. The guidance provides information on common LOTL techniques and gaps in cyber defence capabilities.



## Guide and Govern

We support New Zealand's cyber security system by setting expectations about what good practice looks like through policies and standards, coordinating information sharing between organisations, and providing advice to the New Zealand Government on settings for critical infrastructure, cyber security procurement and communications security material.

Our work to Guide and Govern includes the GCISO system leadership role, providing strategic leadership as the authoritative Government voice on cyber security. Strong cyber security is a key enabler of productivity, economic growth, and the modernisation of public services.

We published version 3.7 of the New Zealand Information Security Manual (NZISM) in February 2024. The NZISM is a key part of our standards-setting role under the GCISO, establishing security expectations for agencies. This latest version of the NZISM includes technical guidance on cryptographic key management, embedding industry best-practice.

Work was also completed on an index to measure New Zealand's ability to prepare for, respond to, and recover from cyber attacks. The Cyber Resilience Framework measures resilience in both consumer and business audiences and will help government agencies to track progress and improvements.

Reflecting the value of our partnerships with our Pacific neighbours, we work with Pacific states to help improve their cyber resilience. Our Pacific Partnership Programme (funded through the Ministry of Foreign Affairs and Trade) provides cyber security advice, training, and capacity building to Pacific Islands countries to help build cyber resilience. This programme supported the delivery of a Cyber Smart campaign to 15 partner countries, as well as cyber reporting tools, advisories, and technical training sessions.

In 2023/24, the Pacific Partnership Programme completed over 14 bilateral engagements and technical training sessions to both grow our understanding of Pacific nations' cyber security needs and to develop cyber security skills across the Pacific, including taking part in the Samoa Cyber Roadshow. The team delivered multiple advisories and reporting tools to the Pacific, including the first Pacific Insights Report, and supported the delivery of a Pacific-specific cyber awareness campaign called 'Cyber UP Pacific' to 15 partner countries. In addition, we provided cyber security support to the Government of the Cook Islands when it hosted the Pacific Islands Forum meeting in 2023.

We also continue to work closely with our international partners on industry best practice and guidance. This reporting year, our products included the co-sealed guidance Guidelines for Secure AI, published alongside 23 agencies from 18 countries. This guidance helps organisations make informed secure decisions on the design, development, deployment, and operation of their AI systems.

### Emerging Technologies

We continue to closely monitor the progress of emerging technologies, including artificial intelligence, and quantum computing.

We are interested in the potential AI has for supporting our work, as well as the national security risks it could pose. Like most organisations, the GCSB has been exploring AI's potential benefits and developing our understanding of potential risks.

Regardless of the potential of AI to support our work, the legal safeguards and oversight arrangements we operate under will continue to apply. Like all disruptive technologies, the impact AI will have on our work and the operation of those safeguards is something we are taking time to understand fully. We are working with other government agencies on a framework for using AI in government and the wider economy.

Quantum computing is another advancement that offers opportunities and risks. The GCSB is working closely with our partners, and other international cyber security and standards bodies, to prepare for uptake in quantum computing. This includes providing new guidance to agencies through the NZISM on preparing for the impacts of quantum computing on information security controls, specifically related to encryption.

## Identify and Understand

Part of our role is to identify, understand, and improve information security issues in the public sector. We work with agencies to monitor, measure, and analyse issues, and provide advice to mitigate vulnerabilities. The NCSC has unique insight and understanding of the cyber landscape and can use this to inform policy and operational decision making, aided by our GCISO function.

We also work to raise everyday New Zealanders' awareness of cyber security issues, to help protect and improve individuals' resilience to cyber threats. We do this through cyber security awareness campaigns, publishing quarterly reports about what is happening in the cyber threatscape, and providing advice and alerts to customers about how to respond to, and prevent, future attacks.

We publish alerts about high-priority vulnerabilities and provided them to our customers in order to support their decision making. This year we published 30 vulnerability alerts, 80 percent of which were published within 1 day of triage. We also co-seal advisory and attribution statements in conjunction with our international partners to raise awareness of cyber threats and provide information of value to cyber defenders to mitigate malicious cyber activity.

Working with our international partners is key to understanding the cyber security trends globally and how these may impact domestically. We participate in a range of international cyber security forums for sharing of information and best practice.

We continue to participate in the international CERT community through CERT-to-CERT engagements and contributions through forums. We contribute to these international groups with the goal of sharing our own expertise and supporting New Zealand's own cyber resilience.

As cyber security is an area where the bulk of cyber security protections happen outside government, it is crucial we work with other sectors. To aid this, we facilitate information-sharing among organisations facing similar threats and challenges, especially where sharing requires a high level of trust. This primarily takes place through Security Information Exchanges focused on critical infrastructure. In the 2023/24 year, we co-chaired 24 Security Information Exchanges across the following six sectors: energy, finance, government, network-providers, universities, and transport and logistics.

We 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 are usually classified, the New Zealand Government can choose to publicly release the conclusions when it is in New Zealand's interests to do so.

### Case study: Parliamentary network breached by the PRC

In August 2021, the computer networks associated with New Zealand's Parliamentary Counsel Office and the Parliamentary Service were comprised by malicious cyber actors. We attributed these malicious actors to a PRC group known as APT40. During the last three years, the PRC has demonstrated ongoing targeting of democratic institutions globally, and the targeting of critical infrastructure networks in the United States. We provided support against this attack.

This APT40 activity against Parliament was made public during the reporting year. Following the announcement, we joined partner agencies to highlight evolving tactics, techniques and procedures used by APT40. Its observed activity has included using compromised small-office/home-office devices as operational infrastructure, and exploiting newly public vulnerabilities in applications and devices.

By sharing this information publicly, we and other authoring agencies are raising awareness of, and resilience to, the tactics associated with significant cyber threats, to help protect and build resilience.

## Prevent and Protect

We protect New Zealand's information and prevent malicious cyber activity. We do this by maintaining New Zealand's classified information and cryptographic systems, providing national security advice to inform regulatory decision-making on technology investment, and pre-emptively acting to disrupt threats to New Zealand. We also provide support to multi-agency events, such as the General Election and the Census.

### Cryptographic Solutions and Development

Our Cryptographic Solutions and Development team ensures the New Zealand Government's classified information systems mitigate emerging cryptographic and cyber threats. As New Zealand's national authority for communications security, we build the maturity and capability of New Zealand by leading the cryptographic community towards fit-for-purpose, trusted and agile cryptographic solutions that conform to international standards.

We are currently developing a New Zealand cryptographic roadmap, which outlines the cryptographic modernisation initiatives being undertaken to ensure that classified information continues to be protected against emerging threats and known risks. The roadmap will help inform information owners and decision-makers, enabling owners of National Security Systems to plan for required upgrades and replacements for cryptographic solutions.

We continue 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 that handles the majority of encryption products provided by the GCSB. Through CPMI, we provide 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 New Zealand Defence Force. We continue to support CPMI, including by maintenance, helpdesk and on-site support for client hosts.

### Support to Major Events

The NCSC continues to provide cyber security support to major national events in coordination with cross-government efforts. The key events we provided cyber security support for in 2023/24 were the 2023 General Election, and the Pacific Islands Forum annual leaders' meeting. 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.

### Regulatory Functions

We deliver regulatory functions under the following Acts:

- Telecommunications (Interception Capability and Security) Act 2013
- Outer Space and High-altitude Activities Act 2017
- Radiocommunications Act 1989, and
- Overseas Investment Amendment Act 2021.

### The Telecommunications (Interception Capability and Security) Act 2013

Given its pervasiveness and comparative ease of access, telecommunications infrastructure is a highly attractive target for states seeking to engage in espionage, sabotage, or foreign interference, or for criminal actors looking to exploit New Zealand businesses and individuals. Network security has therefore become a key area of concern for preserving New Zealand's national security, including its economic well-being.

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 the Telecommunications (Interception Capability and Security) Act 2013 (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.

The TICSA established obligations for New Zealand's telecommunications network operators regarding network security. The Director-General of the GCSB has a regulatory role for network security under Part 3 of TICSA.

Part 3 of TICSA also established 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 2023/24, the GCSB received 143 notifications network change proposals under TICSA.

### **Outer Space and High-altitude Activities Act 2017 and Radiocommunications Act 1989**

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, and Radiocommunications Act 1989. This national security risk assessment advice is used to inform Ministers, as required by the Act.

In the 2023/24 year, we conducted 21 assessments of regulated space activities under the Outer Space and High-altitude Activities Act 2017.

We conducted 74 assessments of regulated radio spectrum activities 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 Amendment Act 2021. 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 we provided advice to the Overseas Investment Office on 39 instances of proposals for overseas investment subject to the national security and public order notifications regime of the Overseas Investment Amendment Act 2021.



## Detect and Contain

One of the NCSC's core functions is to detect threats on New Zealand systems (where we have visibility), and to block these threats before they can cause an impact. We also issue critical alerts to potential victims that may be compromised, once we are made aware of vulnerabilities.

### Cyber Defence Capabilities

Our cyber defence capabilities continue to improve security for New Zealand by protecting networks from malicious cyber activity. Through the provision of capabilities including the CORTEX suite of services and MFN, we ensure that organisations are less exposed to threats from malicious cyber actors. Our services are provided by express consent.

Collectively, these capabilities are provided to a subset of New Zealand's central and local government, key research institutes, infrastructure providers, and key economic generators. These services are complementary to an organisation's own security suite, and provide another layer of protection against malicious cyber activity affecting some of New Zealand's most significant organisations. Our CORTEX suite of services prevented approximately NZ\$38.8 million worth of harm to New Zealanders this year.

Our Phishing Disruption Service also extended its reach significantly during the year. Now, 85 percent of core public service agencies are benefiting from the service, which provides subscribers with high-quality phishing indicators they can block.

### Technical Counter-Surveillance Unit

The NCSC's Technical Counter-Surveillance Unit helps ensure New Zealand's most sensitive communications are not intercepted or compromised. It provides technical security, emanations security, and accreditation services to ensure this information is not intercepted or compromised.

Technical security services are focused on countering technical surveillance techniques used by hostile actors, including eavesdropping and video surveillance. Emanations security services are focused on countering the threat posed by a spread of unintentional signals from ICT equipment that could be intercepted and interpreted by malicious actors. Our accreditation services check that highly classified information systems and sites are safe and secure for use.

## Respond and Recover

We help New Zealanders to respond and recover once threats are found. The NCSC assists with incident responses, especially when incidents are of national significance.

### 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 inter-agency, sector, and wider government actions, our responses often involve working closely with partners such as the New Zealand Police, and the private sector.

We recorded 6,779 incidents through our general triage process. Often these incidents affected individual New Zealanders and New Zealand businesses. Of these incidents, 99.6 percent were responded to within 4 working hours. Our quick response ensures that New Zealanders supported as soon as possible when an incident happens.

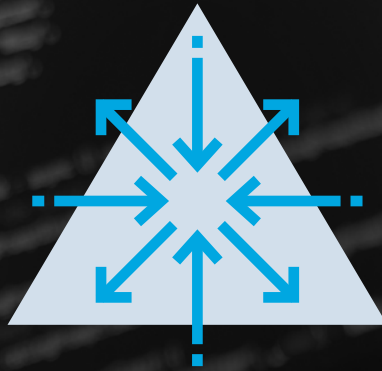
We continue to closely monitor the changing cyber landscape. As noted earlier, this year we recorded 7,122 incidents. Of these 6,779 were handled through our general triage process. Often these incidents impacted individuals or small to medium businesses. The other 343 incidents were triaged for more specialist technical support because of the nature of the victim, or the nature of the incident. These incidents have the potential to cause high impact at the national level trended upwards this year – from 316 in 2022/23 to 343 in 2023/24 - there has been a notable decline in the severity of the impact to New Zealand organisations.

This difference may reflect a number of contributing factors in the threat environment, including: recent disruptions to cyber-criminal infrastructure, changing state priorities or tactics, or the NCSC's increasing ability to disrupt activity before harm takes place. Developments in our cyber defensive capabilities have allowed us to scale some services to a significant number of organisations, and even to home users.

Of the incidents we recorded 32 percent indicated links to suspected state-sponsored actors, compared to 28 percent in 2022/23. Nineteen percent were likely criminally or financially motivated. Although the total of criminal-linked incidents reduced by 19 percent in 2023/24, this reduction is likely to be temporary; there has been an upward trend in the first half of 2024, and we recorded a higher percentage of cyber-criminal-linked incidents than incidents linked to state-sponsored actors for the first time in the previous financial year. This suggests the increasing volume of incidents from cybercrime is likely to continue in the coming years.

The remainder of incidents, 49 percent, were unattributed. These either represented preventative efforts undertaken by the GCSB before the activity could have a significant impact, or lacked the information needed to attribute the malicious activity.

In our triage process for specialist technical support we categorise incidents based on the severity of the compromise, as well as the significance of the victim organisation. The scale, from C1 being the most severe, to C6 being a minor incident, enables us to differentiate between a major and minor incident. This year's most severe incidents were rated C3, with no C2 or C1 incidents recorded. Similar to the 2022/23 year, our most significant incidents were predominantly associated with ransomware or other extortion activity.



## 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.



## TRUSTED

We are a trusted and confident organisation. We make a positive impact and the value we bring to New Zealand is well understood.

# Supporting the National Security Sector

## All-of-Government Data Centre

In addition to providing customers with signals intelligence and improving cyber resilience, we work to support New Zealand's National Security Sector to securely store sensitive information.

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.

Earth works commenced on the Whenuapai site in 2021, with construction beginning on the facility in September 2022. The data centre was publicly announced in April 2023 by the then 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 New Zealand government agencies for at least 25 years.

## Ministerial Responsibility for the GCSB

As a public sector agency, the GCSB is politically neutral, providing impartial intelligence to our customers to enable their decision making. We also have a small policy function, which provides policy advice regarding issues of relevance to our portfolio.

When appropriate, we provide products, such as National Security Risk Assessments, to the Minister Responsible for the GCSB, to assist with their legislative responsibilities. The Minister, together with a Commissioner of Intelligence Warrants for activities in respect of New Zealanders, is the issuing authority for intelligence warrants that authorise GCSB activities that would otherwise be unlawful.

Given the joint enabling functions and similar focuses our agencies share, the Minister with portfolio responsibility for the GCSB is typically also the Minister Responsible for the NZSIS.

A General Election was held this reporting year. Prior to the election, our Minister was Hon Andrew Little. Following this, Hon Judith Collins KC was sworn in as the Minister Responsible for the GCSB in November 2023.

The below measure reflects her assessment, as responsible Minister at the close of the reporting year.

### PERFORMANCE MEASURE: CATALYSE

#### OUTCOME: Minister trusts GCSB's advice

Assessment of Performance 2023/24	Budget Standard	Actual
<b>The Minister responsible for the GCSB receives best possible advice</b>		
The Minister Responsible for the GCSB rates GCSB's advice at least 3.5 (average) on a 5-point scale	At least 3.5 / 5	✓ (4.6)



# Our Sustainability Reporting

We continue to work towards meeting the requirements of the Carbon Neutral Government Programme (CNGP) and operating in an emissions and energy friendly manner.

## Independent Verification

The GCSB completed independent emission verification for 2018/19 (our baseline year), and subsequent financial years.

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.

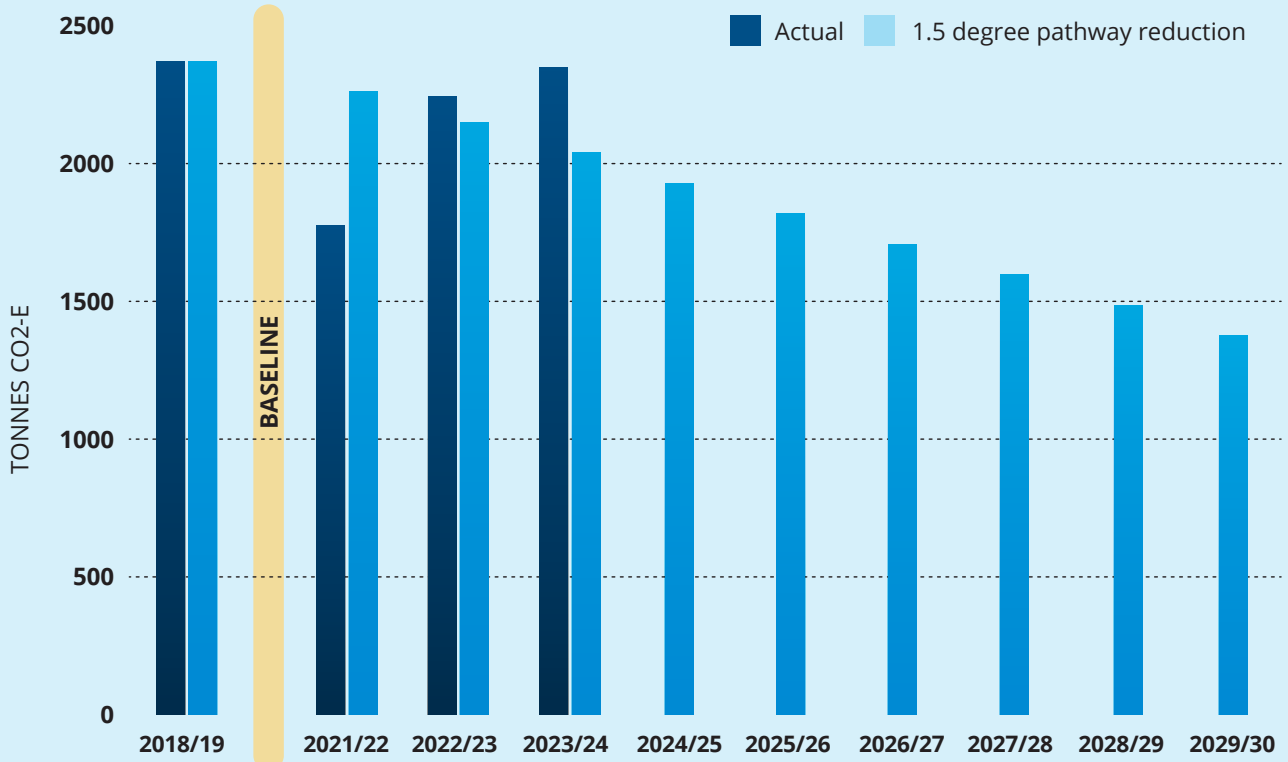
In 2023/24 we estimate we emitted 2,350 Tonnes CO<sub>2</sub>-e, based on our sampled data and extrapolation. This compares to our verified figure of 2,244 Tonnes CO<sub>2</sub>-e in 2022/23. Most of our emissions came from passenger transport, as well as electricity and motor vehicles.

## Our Reduction Targets

The Government 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 CO<sub>2</sub>-e, or a 21 percent reduction in gross emissions (all Categories) compared to the base year, and
- **2030 target:** Gross emissions (all Categories) to be no more than 1,376 Tonnes CO<sub>2</sub>-e, or a 42 percent reduction in gross emissions (all Categories) compared to base year.

### GCSB Actuals vs 1.5 degree pathway reduction



# Accountability and Transparency

## Te Noho Haepapa me te Pūataata Hoki

### 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. The resulting report, Taumaruru: Protecting Aotearoa New Zealand as a free, open and democratic society, was made publicly available in May 2023.

The Government response to the ISA review 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 working closely with DPMC 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, and support a strong compliance culture. Our policies are also reviewed in response to any relevant findings or recommendations made by the Inspector-General, or other Inquiries or independent oversight bodies.

### Independent Oversight

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.

This reporting year, the IGIS published a report into the GCSB's previous hosting of a foreign capability. While the report notes that at the time the GCSB undertook a reasonably robust investigation into the capability and the potential issues with hosting it, the GCSB accepts there were some failings in the decision-making processes that followed. The capability operated from 2013 until 2020, when the GCSB self-reported the capability to the IGIS.

As the IGIS report noted, our operations, governance, legal mandate, policies and compliance systems have changed significantly since the time the capability was operating. We are continually looking to improve how we work.

## Statement of Warrants

In accordance with section 221(2) of the ISA, the following statements are provided for the period 1 July 2023 to 30 June 2024.

### 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 2023/24, of which 14 were Type 1 intelligence warrants and 13 were Type 2 intelligence warrants. No warrant applications were declined.

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)

There were no very urgent authorisations 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. Two business records directions were issued by the GCSB to business agencies under section 150.

## PERFORMANCE MEASURE: TRUSTED

### OUTCOME: Social licence from New Zealand's public allows GCSB to operate effectively

Assessment of Performance 2023/24	Budget Standard	Actual
<b>Oversight agencies are confident in GCSB's legal compliance</b>		
The Inspector-General of Intelligence and Security (IGIS) rates GCSB's compliance performance at or above the well-developed level in at least four of the five headings in the IGIS Annual Report certification of compliance systems		
<b>New Zealand public has trust and confidence in the GCSB</b>		
Public Service Commission Trust and Confidence survey Kiwis Count: Responses above 60 percent level for Q3B "Overall, to what extent do you trust the public service?"		 <sup>1</sup>
 Achieved  Not achieved  Not applicable		

## 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. Due to the joint enabling functions we share with the NZSIS, we provide combined OIA responses when appropriate with the NZSIS.

### Number of information requests completed

	2019/20	2020/21	2021/22	2022/23	2023/24
OIA	51	49	70	59	75
PA	28	27	16	23	19

The median response time was 16 working days across all OIA and Privacy Act requests. This compares to 19 working days in the previous reporting year. All requests were responded to within the legislated timeframe.

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

The GCSB was notified of three complaints by the Office of the Ombudsman during the reporting period. One complaint was resolved with the Ombudsman finding in the GCSB's favour; one found against the GCSB. The third complaint remained under consideration at the close of the reporting period.














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

<sup>1</sup> At June 2024, Trust in the Public Service was reported at 56 percent. This figure reflects reported trust across all New Zealand public services.



## PERFORMANCE MEASURE: TRUSTED

### OUTCOME: Social licence from New Zealand's public allows GCSB to operate effectively

Assessment of Performance 2023/24	Budget Standard	Actual
<b>GCSB meets its legal obligations: Official Information Act 1982</b>		
100 percent of OIA requests are completed within the legislated timeframe		
More than 50 percent of final opinions formed by the Ombudsman are found in favour of GCSB		
<b>GCSB meets its legal obligations: Privacy Act 2020</b>		
100 percent of Privacy Act requests are completed within the legislated timeframe		
More than 50 percent of investigations by the Office of the Privacy Commissioner found that GCSB did not breach the Privacy Act and cause the complainant harm		
<b>New Zealand media and commentators are well informed about the GCSB</b>		
Assessment by the GCSB communications team about the accuracy of media reporting about the GCSB		 <sup>2</sup>
 Achieved  Not achieved  Partially achieved		

<sup>2</sup> We continue to work to improve media and commentators' understanding of the GCSB's roles and functions.

# Organisational Capability

## Ngā Āheitanga Whakaharere

Our People | Ō Mātau Tāngata

40

Our Finances | Ā Mātau Pūtea

48

PUZZLE #4

QBY EKUYOJIYJQ TKIIRJDTCQDKJP PYTRODQX AROYCR  
 DP JYV ZYCHCJL'P HYCL CEYJTX SKO PDEJCHP  
 DJQYHHDEYJTY CJL MOKUDLYP DJQYHHDEYJTY QK  
 EKUYOJIYJQ TRPQKIYO CEYJTDYP. DQ DP CHPK QBY  
 HYCL KMYOCQDKJCH CEYJTX SKO TXAYO PYTRODQX,  
 QBOKREB QBY JCQDKJCH TXAYO PYTRODQX TYJQOY. VY  
 RPY KRO DJQYHHDEYJTY TKHHYTQDKJ TCMCADHDQDYP,  
 PRMMHYIYJQYL AX DJQYHHDEYJTY OYTYDUYL SOKI  
 MCOQJYOP, QK PRMMKOQ EKUYOJIYJQ CEYJTDYP DJQBYDO  
 KMYOCQDKJP CJL LYTDPKJ ICGDJE, CJL QK TCOOX  
 KRQ QBYDO HYEDPHCQDUYHX ICJLCQYL SRJTQDKJP. KRO  
 JTPT VKOGP QK PQOYJEQBYJ JYV ZYCHCJL'P TXAYO  
 PYTRODQX OYPDHDYJTY. QBDP DJTHRLYP KJEKDJE VKOG  
 CTOKPP EKUYOJIYJQ CJL TODQDTCH DJSOCPQORTQROY  
 KOECJDPCQDKJP QK YJPROY QBY LCQC CJL KJHDJY  
 PYOUDTYP QBCQ JYV ZYCHCJL OYHDYP KJ COY  
 MOKQYTQYL CECDJPQ CHH BCZCOLP CJL ODPGP. JKMOQ

# Our People

## Ō Mātau Tāngata

### Recruiting and Retaining Our Talent

The Intelligence Community Shared Services People and Capability team provides advice, support and strategic workforce development initiatives to the GCSB and NZSIS. This work supports the continued growth of their workforces, and retention and development of existing staff. These activities ensure the NZIC has the best and most representative workforce possible to meet the expectations of the New Zealand Government and the public.

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.

#### Beyond Ordinary People

The success of our agency depends on our technological capabilities, our legal authorities, our strong partnerships and our social licence. But above all, it depends on the quality, diversity, professionalism and technical capabilities of our people.

The GCSB is a public service department with 596.7 full-time equivalent staff made up from 605 staff, as at 30 June 2024. The NZIC operates shared corporate service functions employing both GCSB and NZSIS staff to work across both agencies.

#### Turnover

The GCSB has seen a reduction in staff turnover by 4.4 percentage points - from 15.6 percent in the 2022/23 financial year to 11.2 percent at 30 June 2024. When investigated, employees consistently report the primary reason for leaving is career development.

Our average tenure for permanent staff is 5.9 years. This has decreased by 0.4 years from 2022/23. Over the 12 months to 30 June 2024, the majority of our core workforce who ended their employment with us (68.3 percent) left within five years of joining.

**Table 1: The GCSB's Core Unplanned Staff Turnover (2019 to 2024)**

	2019/20	2020/21	2021/22	2022/23	2023/24
Staff Turnover	13.7%	8.1%	19.3%	15.6%	11.2%
Public Service	10.1%	10.5%	17.3%	15.9%	11.9%

## Retention and Recruitment

In response to recruitment and retention challenges of the previous financial years, the GCSB and NZSIS endorsed a Joint Recruitment Transformation Programme, which commenced in September 2023.

The primary objective of this work is to address the strategic, technological and capability challenges that are barriers to us engaging effectively in the market. The programme also recognises the need for targeted interventions to address the agency's workforce needs in the face of a global talent shortage, changing workforce expectations, commitment to our diversity and inclusion targets, and the unique challenges of acquiring talent for national security roles.

Our Recruitment Transformation programme is focused on ensuring our systems, processes and practice are positioned to engage with the market effectively and at pace; prioritise internal mobility in support of talent development and retention; and our market presence contributes to better national security outcomes by attracting and retaining diverse and high performing talent in our community.

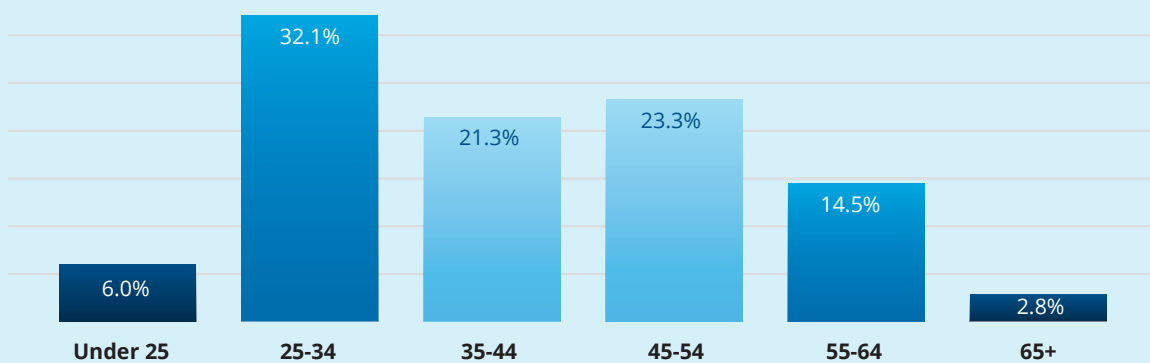
Starting with an efficiency and quality focus in 2023/24, we have improved transparency across the recruitment pipeline through the adoption of new, and development of existing tools. We improved data capture and analysis to assess channel effectiveness and inform the quality and efficiency of initiatives. As a result of these insights we were able to undertake a series of process and practice improvements, resulting in tangible reductions in cost and time to hire.

## Promoting Diversity and Inclusion

### Age demographics

The majority of our workforce is younger than 45 years old (59.4 percent). Our average age is 41.7 years, which has decreased slightly by 0.6 years since 2022/23. Of our workforce, almost half (45.1 percent) started within the last three years.

**Graph: GCSB Age Demographic Breakdown as at 30 June 2024**





## Gender Diversity

As at 30 June 2024 women made up 53.1 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.

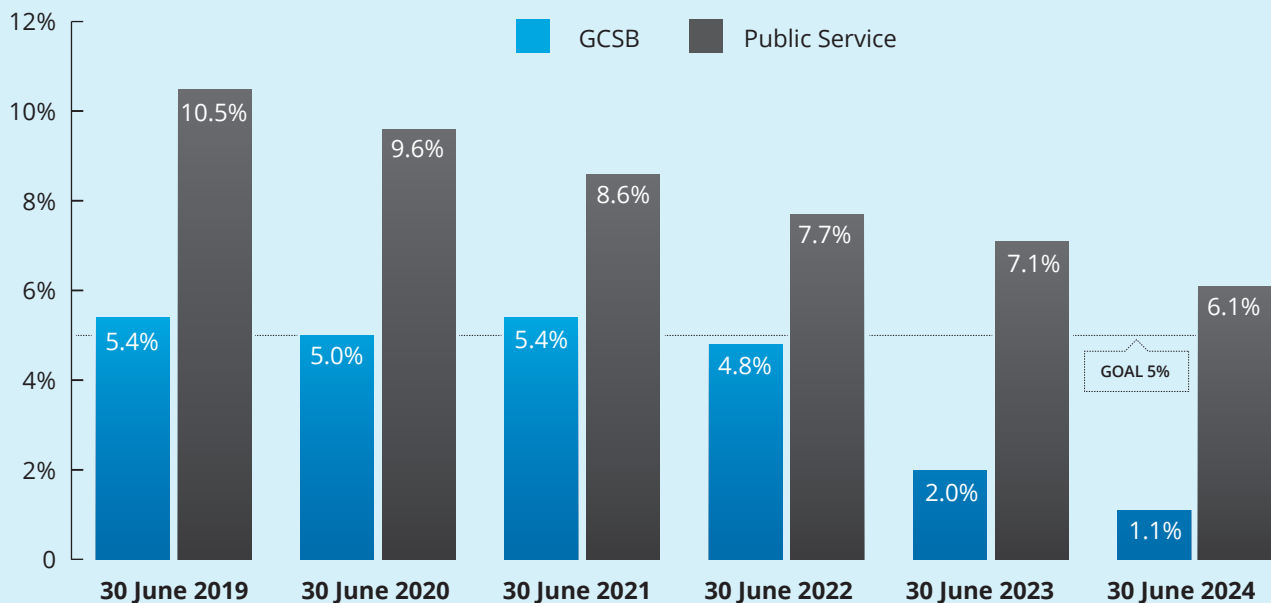
**Table 2: The GCSB's Gender Representation (2019 to 2024)<sup>3</sup>**

	2019/20	2020/21	2021/22	2022/23	2023/24
<b>Senior Management (Tier 2 and 3)</b>					
Men	54.5%	47.8%	36.8%	40.0%	46.9%
Women	45.5%	52.2%	63.2%	60.0%	53.1%
<b>All Staff</b>					
Men	64.4%	64.5%	61.1%	63.2%	64.0%
Women	35.6%	34.9%	37.9%	35.5%	35.2%
Another Gender	-	0.2%	0.2%	0.6%	0.8%
Undisclosed	-	0.4%	0.8%	0.7%	0.0%

## Gender Pay Gap

Addressing our gender pay gap is a key feature of our 2021-2025 Diversity and Inclusion (D&I) Strategy. We have met our goal of no more than 5 percent. At 30 June 2024, our average gender pay gap was 1.1 percent. This was a 0.9 percentage point decrease from 2022/23.

**GCSB Average Gender Pay Gap (2019 to 2024)**



<sup>3</sup> 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's definition of Senior Management.

## Ethnic Diversity

Staff can choose whether or not to disclose their ethnicity. In our workforce, 90.4 percent disclosed at least one ethnicity, exceeding our targeted percent disclosure rate of 90 percent for robustness of analysis.

**Table 3: The GCSB's Staff Ethnicity (2019 to 2024)<sup>4</sup>**

	2019/20	2020/21	2021/22	2022/23	2023/24
<b>All Staff</b>					
European	71.2%	76.0%	74.6%	77.5%	77.7%
New Zealander <sup>5</sup>	26.8%	22.8%	18.5%	–	–
New Zealand Māori	7.3%	7.2%	9.1%	9.8%	9.5%
Asian	5.5%	7.2%	7.3%	7.3%	9.0%
Pacific Peoples	1.6%	2.6%	3.2%	3.1%	3.3%
MELAA	1.1%	1.2%	1.6%	0.8%	1.1%
Other	–	0.2%	0.2%	15.7%	13.0%

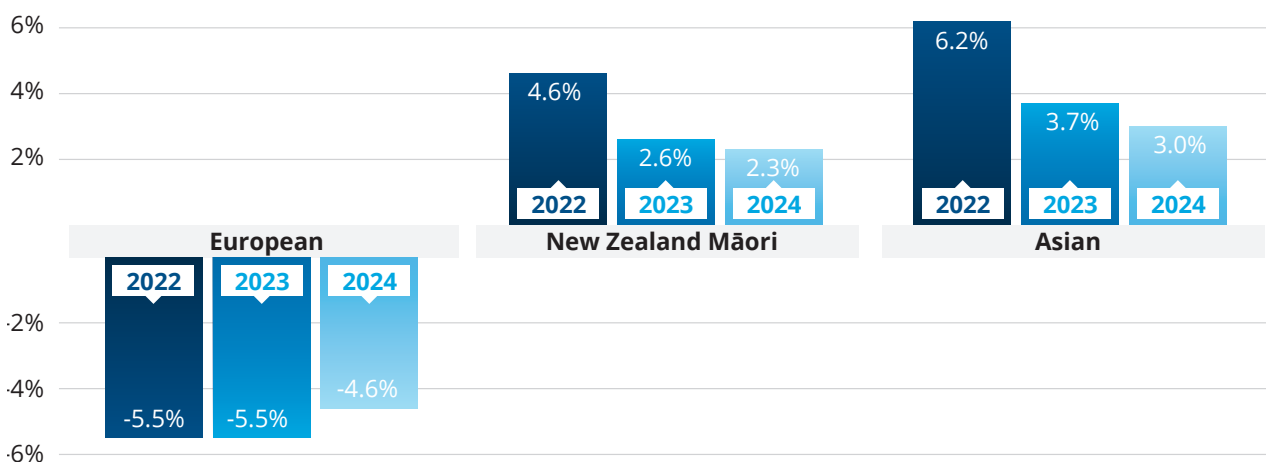
**Table 4: The GCSB's Senior Management (Tier 2 and 3) Disclosed Ethnicity (2024)**

European	New Zealand Māori	Asian	Pacific Peoples	MELAA	Other
80.6%	22.6%	6.5%	–	–	12.9%

## Ethnic Pay Gaps

European is the only ethnicity with a negative average ethnic pay gap (in favour). This means on average Europeans are earning 4.6 percent more than non-Europeans. Of the three groups with sufficient numbers for statistical robustness, European has the highest average pay gap.

**Table 5: The GCSB's Ethnic Pay Gaps (30 June 2024)<sup>6</sup>**



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 From 2022/23, staff who self-identified their ethnicity as New Zealander fall under 'Other' based on Stats NZ ethnicity groupings.

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

## 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, known as the Kia Toipoto Pay Gap Action Plan. This is a three-year plan focused on addressing all pay gaps - gender, Māori, Pacific, ethnic, and other minorities (i.e. Rainbow and disabled communities).

In 2023 we partnered with staff to develop a 2023/24 action plan for our agency. We developed simple achievable actions for the short, medium, and long term. Since November we have:

- Surveyed our women staff to understand their experiences within the NZIC, including questions to

measure the uptake of flexible working and barriers to this

- Translated our myth busting booklet into multiple languages to help break down barriers to entry
- Worked with our Military Network to explore how we measure pay gaps for our ex-military staff, and
- Established a new mentoring programme for staff.

We will review our progress against our action plan in mid-2024, and once again partner with staff to develop and agree an action plan for 2024/25.

## Experience of Women

We remain committed to increasing the representation of women in our workforce and ensuring their experiences lead to positive, fulfilling careers in national security.

In 2019 we researched the experiences of women in the NZIC and set an action plan to address the research findings. The plan focused on four identified themes – culture, leadership, career development and flexibility, with regular monitoring of progress against each action.

In 2024 we invited our female staff to respond to a further survey, to understand whether the initiatives implemented following the 2019 survey had any impact on their experience in the workplace. The 2024 survey was structured around the employee lifecycle. This allowed us to identify touchpoints that are particularly impactful for women and their careers within our agency.

In particular, we wanted to understand how attitudes and behaviours had changed within the workplace since 2019. We also wanted to gain insights into women's career aspirations, how they are supported/guided to achieve these, and what contributes to women wanting to continue their career within the intelligence community.

We are reviewing and analysing the data from the survey and will share the results with all staff when available. This will include opportunities to continue improving the experience of women within the NZIC, and address any issues that have been highlighted in the feedback.

While it was our women's voices and experiences that were shared, any opportunities we take to continue to improve experiences and address identified issues will benefit not just women, but all staff within the NZIC.

## Mentor<sup>Lite</sup>

Mentor<sup>Lite</sup> is a self-service mentoring programme introduced in early 2024, allowing any staff member to participate in this programme, either as a mentor or a mentee. The programme is designed to make it easy for staff to find more experienced colleagues to help them develop, learn and grow through:

- Providing opportunity for sharing best practice, knowledge and experience
- Building relationships throughout our community
- Encouraging our people to work together across different work areas and disciplines, and
- Creating an opportunity for fresh ideas and innovations to be created/shared.

It is important that staff are able to find a mentor they can connect with, and our mentors come from all levels, areas and backgrounds. They are able to support staff in a number of areas, including communication, leadership, personal development and risk management.

People & Capability also worked closely with our Women in Operations employee-led network to establish a bespoke mentoring programme for them, based on the Mentor<sup>Lite</sup> framework. This aligned with an action in our *2023/24 Kia Toipoto Pay Gap Action Plan* to support employee-led networks who wish to establish their own mentoring programmes.

## Looking Ahead

We continue to be mindful of the need to be financially sustainable in the medium term. We are reflecting on our staff structure and adapting as appropriate. Considerations in this area have included a joint work programme with the NZSIS. At the end of the 2023/24 reporting year, this agency-driven work was still underway, with change and consultation processes not yet initiated, and decisions still to be taken.

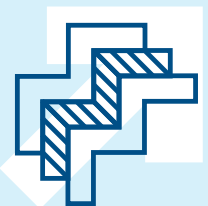


## Progress against Te Kawa Mataaho Papa Pounamu Commitments



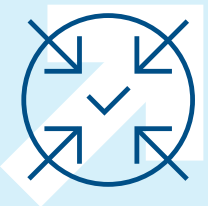
### Te Urupae i te Mariu Addressing Bias

- Of our GCSB leaders, 81.6 percent, and 71 percent of senior management completed our Understanding & Managing Bias learning module.
- We surveyed women to understand their experience within the NZIC. This included questions to understand if women felt they were treated differently due to their gender. Findings of the survey will identify focus areas to improve women's experiences.



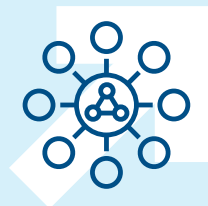
### Te Āheinga ā-Ahurea Cultural Competence

- Our new Pasifika Matters Workshop explores the diversity of the Pacific Island region and the relationship with, and experience of, Pasifika people in New Zealand.
- We introduced new workshops to develop our people's capability so that they are able to engage effectively with iwi and Māori when undertaking our national security functions. This is also key to helping us attract and retain the talent required to achieve our national security outcomes.



### Hautūtanga Ngākau Tuwhere Inclusive Leadership

- Development of our Manager Induction Pathway, which aims to build management capability in alignment with inclusive leadership practices, continues. The programme will be compulsory for all managers, new to role and/or new to the organisation.
- Our Manager Essentials toolkit has been built to sit alongside and support our Manager Induction pathway. Our D&I practices, including inclusive leadership, are embedded into the toolkit.



### Ngā Tūhohonga e Kōkiritia ana e Ngā Kaimahi Employee-led Networks

- Worked with our Women in Operations network to develop a bespoke mentoring programme, based on our MentorLite framework.
- With our Rainbow network, initiated a project to successfully develop and deliver a human-centric process to enable anyone to change their name (legal and preferred) easily, within our strict security environment.
- Alongside our ELNs, reviewed and made changes to improve and enhance our Introduction to ELNs and Staff Group sessions.



### Hautūtanga Kākano Rau Fostering Diverse Leadership

- Delivered an International Women's Day workshop series to empower women. The workshops provided personal and professional growth, and the tools needed to proactively address challenges women may face when advancing their careers.
- We will be exploring this further, including establishment of actions and/or pieces of work, in the next iterations of our Kia Toipoto Pay Gap Action Plan and D&I Strategy.

## 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 Critical Risk Management continues to focus on physical, health and psychosocial risks such as driving, hazardous substances and working unsociable hours with critical controls identified to ensure the ongoing safety and wellbeing of our people.



### Infrastructure

The GCSB construction of the all-of-government data centre continues. During this period there was one notifiable event recorded relating to an uncontrolled fall from heights involving building material. No serious injury was obtained; the case closed without further WorkSafe NZ investigation.



### Worker Engagement and Participation

We focused on improving worker engagement and education. The second NZIC Health and Safety Representative Conference was held in April 2024, bringing together 30 representatives across the GCSB and NZSIS. We also focused on providing health and safety training to our managers and staff that manage building contractors.

We continue to have a 100 percent completion rate for all new starters completing the health and safety Induction Module.

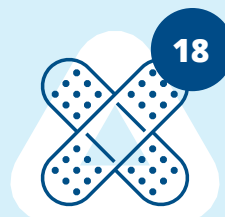
## Annual Safety Performance Scorecard – GCSB



Close calls / non injury



Restricted work Injuries<sup>7</sup>



First aid Injuries



Environmental Events

<sup>7</sup> 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.

# Our Finances

## Ā Mātau Pūtea

### Being Financially Responsible

The GCSB is committed to being financially sustainable and a responsible user of public funds. We completed a rapid savings exercise during the reporting period which aligned with our ongoing work programme on financial sustainability. Our budget holders are aware of the ongoing importance of financial management.

#### Rapid Savings

Public sector agencies were asked to identify savings through the Budget 2024 process. The GCSB will be making savings of \$7.62 million per year from 2024/25, through efficiencies in areas such as contractor and consultant spending, training and development, and travel.

In addition, funding of \$5.742 million over four years that had been set aside in a tagged contingency for the GCSB in Budget 2023 to expand the mandate of the GCISO to Crown Agents was returned. The GCISO mandate, refreshed by Cabinet in 2023, will not change. This function will continue to be delivered in support of existing mandated agencies.

As a result of the efficiency savings of \$7.62 million, we will be operating with a higher degree of financial risk than previously. This means operating with smaller financial contingencies in place, which may diminish our ability to meet the costs of surge or unscheduled activity without identifying trade-offs.

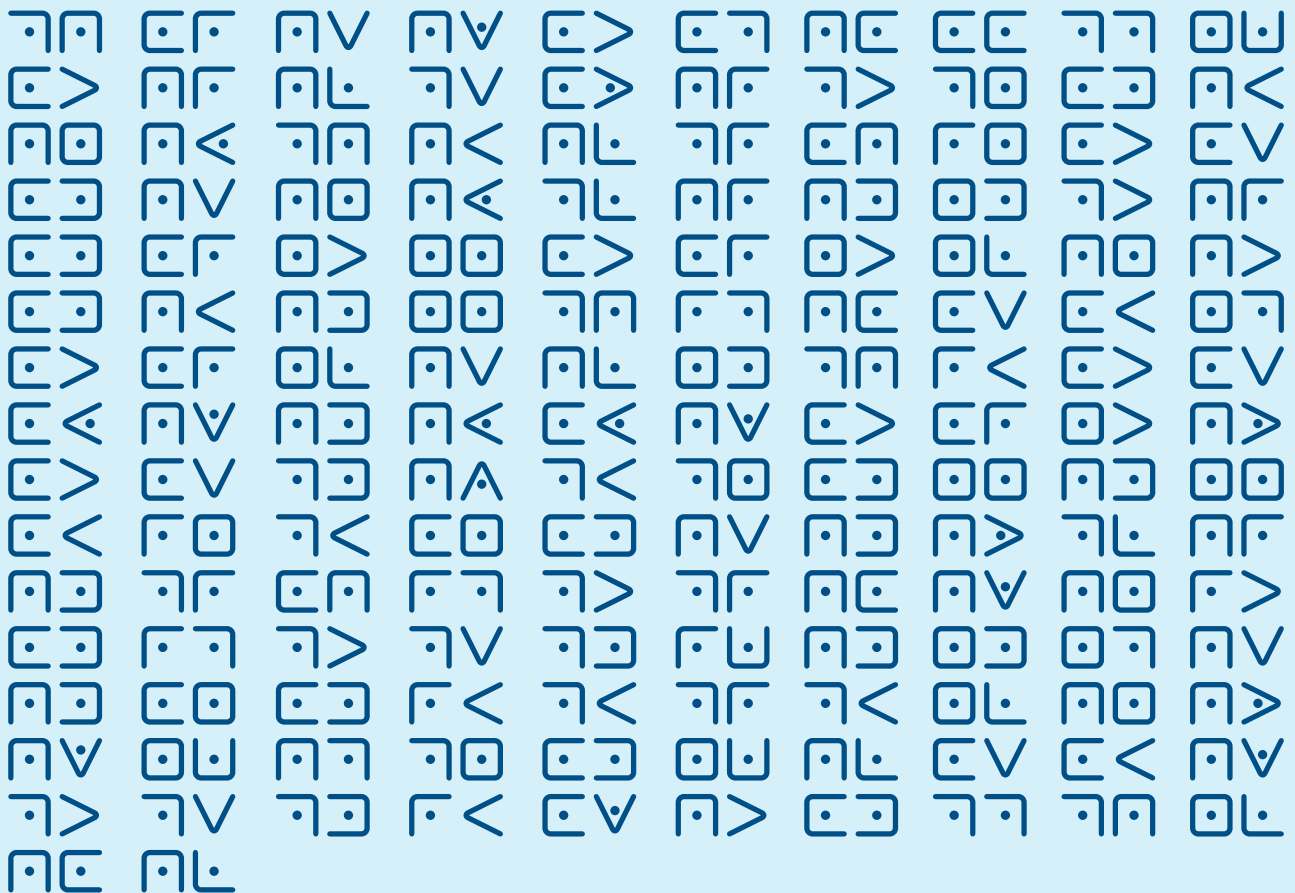
#### Financial Sustainability

At the close of the reporting year, the GCSB and NZSIS were undertaking a joint work programme to ensure the financial sustainability of the agencies in the longer term, as well as in the context of the current fiscal environment. This began before the rapid savings exercise as a separate process where our agencies both recognised we need to be sustainable over the long term and initiated work to ensure this.

# Financial Statements

Statement of Responsibility	50
Independent Auditor's Report	51
Statement of Expenses and Capital Expenditure incurred Against Appropriation	54

PUZZLE #5





# 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 2024.



**Andrew Clark**

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

30 September 2024

# Independent Auditor's Report

AUDIT NEW ZEALAND  
Mana Arotake Aotearoa

To the readers of the Government Communications Security Bureau's statement of expenses and capital expenditure against appropriation for the year ended 30 June 2024.

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 2024 on page 54.

## Opinion

In our opinion the statement of expenses and capital expenditure against appropriation of the GCSB for the year ended 30 June 2024 is presented fairly, in all material respects, in accordance with the requirements of section 221(4)(a) of the Intelligence and Security Act 2017.

Our audit was completed on 30 September 2024. 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 2023/24 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 2 to 50, 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



# STATEMENT OF EXPENSES AND CAPITAL EXPENDITURE INCURRED AGAINST APPROPRIATION

## FOR THE YEAR ENDED 30 JUNE 2024

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

	\$000
Total appropriation	402,163
Actual expenditure	324,839

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.

