G.56 (2025)

Te Tira Tiaki
Government Communications
Security Bureau

Government Communications Security Bureau

Annual Report 2025

www.gcsb.govt.nz

Preface

This is the annual report of the Government Communications Security Bureau (GCSB) for the year ended 30 June 2025, 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.

Contents

Foreword

Director-General Foreword

The past year has again been characterised by global conflict and an increase in volatility around the world. Large-scale conflicts remain, and the unpredictable geopolitical environment continues to challenge the rules-based international system, from which New Zealand has traditionally derived security. We work in a complex environment together with like-minded partners, in the context of supporting New Zealand's own sovereign interests, using unique capabilities under our governing legislation.

The GCSB is New Zealand's lead organisation for signals intelligence and cyber security. Our mission is to provide our customers with intelligence advantage and cyber resilience to successfully navigate this unpredictable world. Our work with partner agencies to support the safety of New Zealanders remains in demand. This includes supporting the safety of New Zealanders overseas, such as New Zealand Defence Force personnel deployed in conflict regions.

During the year we provided signals intelligence to Ministers and government agencies to support their decision making on a range of issues under our government's National Security Intelligence Priorities, ranging from transnational organised crime to foreign interference, to countering terrorism and violent extremism. We continue to make a highly valued contribution to global-counter-terrorism efforts, including assisting with the disruption of attack planning. We have played a critical role in helping our customers to make informed decisions. Our work also supports regional stability.

Events in the Pacific have a fundamental impact on New Zealand's own national security, and the region is increasingly an area of strategic competition for influence. Transnational serious organised crime is also impacting the security of the region. The GCSB provides SIGINT in relation to New Zealand's interests in the South Pacific. This focuses on providing support to other government agencies whose responsibilities include responding to security issues in the Pacific region.

While we are a predominantly outward-looking agency, we seek to protect and strengthen New Zealand's resilience to threats internally, too. Together with our partners, we continue to defend against a complex and persistent array of cyber threats on New Zealand's digital infrastructure. From individuals falling victim to cyber-dependent criminal activity, to government agencies being targeted by advanced actors and techniques, we are continually refreshing our understanding of the cyber security threats being felt across New Zealand.

We have stepped up work to help build New Zealand's cyber resilience in response. Following CERT NZ's integration with the GCSB, our cyber security support has been extended to all New Zealanders, with a streamlined incident reporting function. We have also increased our engagement, publishing a range of advice and guidance to help New Zealanders stay cyber-smart. And we are working with New Zealand's operators of critical infrastructure, as malicious cyber actors increasingly target systems supporting Western critical infrastructure.

We continue to meet with businesses, universities and associations to help build their defences, and continue to support countries in the Pacific to lift their own cyber resilience too. Through my role as Government Chief Information Security Officer, we continue to provide system stewardship for the public sector on information security issues, including emerging technologies such as artificial intelligence. Our international and domestic partnerships remain crucial to us as we work together to counter threats and increase our collective resilience.

Our services such as Malware Free Networks® (MFN®) play a key role in defending New Zealand from cyber threats, with the help of partner organisations. Between the introduction of MFN in 2021 and the end of this reporting year, MFN has now disrupted more than 473.4 million threats. In addition, we launched a Vulnerability Insights Programme this year, which detects and notifies customers in the public sector of their own cyber security vulnerabilities that could affect their systems. Since this launch, we have already expanded coverage to scan over 200,000 devices across 122 organisations.

This financial year also marked the opening of our new all-of-government data centre at Royal New Zealand Air Force (RNZAF) Base Auckland (Whenuapai). This data centre, named Mātai, was opened by the Minister Responsible for the GCSB, Hon Judith Collins KC. This facility was built to provide a safe, secure storage capability for New Zealand agencies to process and store the Government's most sensitive information. The GCSB is operating this data centre as the New Zealand government's lead agency for information security, and we are proud to be improving New Zealand's digital resilience through this facility.

Resilience has also been an internal theme for our agency this year. We work closely with the New Zealand Security Intelligence Service (NZSIS), with whom we share joint enabling functions and staff. Together with the NZSIS, we undertook a change process as part of a joint financial sustainability programme, to ensure we are efficient, financially sustainable, and well-equipped to face the evolving threatscape.

In the current unpredictable environment, it is imperative that the GCSB can continue to deliver on our mission. Our ability to meet this depends on our diverse and talented people, and their dedication to protect and serve New Zealanders. I am privileged to lead them, and thank them all.

Ngā mihi nui,

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

Statement of Responsibility

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

- The preparation of the GCSB's 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 2025.

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

30 September 2025

Who we are and what we do

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

Our mission

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.

Our functions

We use our intelligence collection capabilities, supplemented by intelligence received from partners, to support government agencies in their operations and decision making. 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 functions, and
- Co-operation with other entities to respond to imminent threat.

The 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 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.

Our people

As at 30 June 2025, the GCSB has 589.3 full time equivalent employees. We have shared enablement functions with the New Zealand Security Intelligence Service (NZSIS). Many of our shared staff are employed by the GCSB but work across both the NZSIS and the GCSB. This supports ease of cooperation between our agencies in a cost-efficient manner.

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 35.

Progress on strategic intentions

Performance framework for 2024/25

Our Mission	Intelligence advantage and cyber resilience to successfully navigate an unpredictable world.
We support protecting New Zealand as a free, open, and democratic society by contributing to:	• The protection of New Zealand's national security • The international relations and well-being of New Zealand, and • The economic well-being of New Zealand.
We achieve this through:	**Intelligence collection and analysis** • Using our Signals Intelligence collection capabilities to produce intelligence that provides decision advantage to government agencies in conduct of their functions. **Detecting, disrupting and deterring high impact cyber threats** • The NCSC detects, disrupts and deters high impact cyber threats and provides cyber security services to individuals, businesses and organisations, government, and operators of critical infrastructure.
Our contributions to national security are formed around six outcomes	Of our six outcomes, three focus on our work to protect New Zealand, and three focus on ensuring that we are a strong and resilient agency: • **Protect – Tiaki Tangata:** We protect New Zealand; our people, infrastructure and information. • **Build resilience – Tiaki Oranga:** We build resilience in others so that New Zealand can confidently navigate future security challenges. • **Catalyse – Tiaki Hononga:** Our products and services are based on customer partnerships and enable real-world outcomes that advance New Zealand's values and interests. • **Resilient:** We invest in the GCSB's resilience so that we can better serve New Zealand. • **Trusted:** We are a trusted and confident organisation. We make positive impact, and the value we bring to New Zealand is well understood. • **Future focused:** We will ensure we have the right relationships, co-ordination, and tradecraft to respond to and counter both existing and emerging threats.
By pursuing our Strategy, we will achieve the following key shifts:	• 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. • 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. • Embed our responsibilities as a **Treaty Partner** to advance cyber resilience with iwi, hapū and Māori organisations. We will work with partners to define and give effect to our role in lifting the cyber resilience of iwi, hapū and Māori organisations. • 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. • **Catalyse** our customers' use of intelligence. We will work in a way that means 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. • Position ourselves to be **future focussed** to effectively meet security challenges and increased demand. We have a focus on continuing to make the GCSB a great place to work, prioritising 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.

Assessment of operations

Part A: Implementing the Government's priorities

The GCSB works 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.

Baseline savings

The GCSB's baseline was reduced by $7.62 million in 2024/25 through the Budget 2024 Initial Baseline Exercise. We achieved the savings targets through efficiency savings that could be managed without having a significant impact on operational activity, for example, by reducing spend on contractors and consultants, training and development, travel, and reduced financial contingencies.

Part B: Assessment of operations

Intelligence advantage

As New Zealand's signals intelligence (SIGINT) agency, our role involves collecting and analysing electronic communications of relevance to our objectives to produce intelligence. We also get great value from 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 he safety and security of New Zealanders.

Our legislation enables us to seek authorisation to carry out a range of activities to obtain intelligence including intercepting communications, receiving intelligence from our international partners, and accessing information infrastructures to retrieve digital information directly from where it is stored or processed. We can also seek assistance from telecommunications network operators and services providers to give effect to our authorisations.

Strategic competition

The GCSB works closely with the NZSIS and the wider national security system to understand how New Zealand's people and sovereign structures are at risk from national security issues including the foreign interference activities of other states. The NZSIS leads the NZIC's efforts to identify and understand foreign interference activity by other governments.

Regional Security

What happens in the Pacific has a fundamental impact on New Zealand's own national security, prosperity and identity. The GCSB provides intelligence reporting 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.

Transnational Serious Organised Crime

The GCSB provides intelligence and technical assistance to the New Zealand Customs Service (Customs) and New Zealand Police (NZP) to help counter Transnational Serious Organised Crime (TSOC).

This interagency work 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.

Counter-terrorism

The GCSB's counter-terrorism effort has both a foreign and a domestic focus, aimed at ensuring New Zealand, New Zealanders, and our interests overseas are protected from violent extremism. Internationally, we continue to make a unique and highly valued contribution to global counter-terrorism efforts.

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.

Support to the New Zealand Defence Force

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

Cyber Resilience

One of our core functions is to provide cyber security advice and assistance for all New Zealanders, which is delivered through our National Cyber Security Centre (NCSC). The NCSC was established in 2011 to support nationally significant organisations to improve their cyber security and resilience.

In July 2023, Cabinet determined New Zealand's Computer Emergency Response Team (CERT NZ) would be integrated with the NCSC, strengthening the GCSB's role as the New Zealand Government's lead operational cyber security agency.

The formal integration programme was completed by 30 June 2025. This programme has unified our functions to consolidate our view of the operating environment, create a unified cyber security incident response service, and offer an authoritative voice from the New Zealand Government on cyber security. This is a positive step for New Zealanders, as it simplifies the process of getting help in response to cyber security concerns.

We recorded 5,995 cyber security incidents this reporting year, of which 331 had the potential to cause high impact at the national level. Of these, at least 25 percent indicated links to state-sponsored actors, while at least 41 percent were likely criminal or financially motivated. The motivations of the remaining 34 percent remained unclear at time of reporting, but could also be state-sponsored, or criminally/financially motivated.

We help raise New Zealand's collective cyber resilience against incidents through three main approaches:

- We support New Zealanders and New Zealand organisations to act on informed decisions
- We work with key players to build a resilient cyber security ecosystem, and
- We use our mandate and specialist capabilities to counter the most serious harms.

Further information about our work under each of these approaches is outlined below.

Supporting New Zealanders and New Zealand organisations

We provide cyber security advice and education for all New Zealanders and New Zealand organisations. We focus on encouraging people to implement the most effective cyber security behaviours that would protect them from the vast majority of the cyber security threats they are likely to face. We also commission independent research to measure the uptake of these behaviours amongst individuals and small to medium enterprises, and we use this to tailor our engagement approach.

Our incident management function plays a vital role in safeguarding against cyber security threats that could impact our national security and wellbeing. We triage incidents according to their potential national impact, engage with victims to understand the scope of the activity, and provide targeted support throughout the incident's lifecycle. For incidents with potential national level impact, this involves performing investigations and providing recommendations to support malicious activity containment, remediation, and recovery.

Key achievements

During 2024/25, we:

- Responded to 5,995 cyber incidents
- Ran a "Scamathon" campaign in this year's annual Cyber Smart Week event (see page 17)
- Launched BOSS – the Business Online Safety Series – to help small businesses start their cyber security journey
- Published cyber security guidance for high-profile individuals[1], and
- Joined the Anti-scam Alliance, a group of government agencies and private sector organisations working to improve New Zealand's ability to prevent and respond to online financial scams.[2]

Support to victims of cyber security incidents

This year we recorded 5,995 cyber incidents. To understand the impact of any one incident, we triage incidents into categories based on the severity of the compromise and the size of the impact, ranging from C1 (a national cyber emergency) to C6 (a minor incident). We did not record any C1 or C2 incidents this year, but did record eleven C3 incidents.

[1] Producing this guidance for high profile individuals was one of the recommendations of a review undertaken into our practices and procedures for our response to cyber security incidents, following phishing activity targeting members of the Inter-Parliamentary Alliance on China.

[2] As not all scams are cyber security issues, the GCSB's work in relation to addressing online financial fraud is on cyber-dependant crime, rather than cyber-enabled crime. Our expertise and resources are focused on cyber security threats and vulnerabilities, as well as raising cyber security resilience in New Zealand. We continue to deliver a range of existing cyber security services that help individuals and organisations better protect themselves from cyber security threats.

Our work in 2024/25

Case study	**The Scamathon campaign**
Context	Our annual Cyber Smart Week event took place in October 2024. For this year's event, we created the "Scamathon" campaign. While New Zealanders consider cyber security to be important, our research showed that many people are not proactively keeping themselves secure online. In particular, our research showed that New Zealanders are not implementing some of the most impactful cyber security behaviours: • Only 42 percent of New Zealanders feel vulnerable to cyber attacks • 32 percent do not use two-factor authentication • 30 percent admit to using weak passwords • 43 percent reuse passwords between different online accounts
What we did	To increase the uptake of these cyber security behaviours, we ran a "Scamathon" campaign to show New Zealanders that we are all vulnerable to cyber attacks and to highlight the importance of having strong, unique password practices, as well as two-factor authentication.
Our impact	Independent market research, commissioned by the NCSC, showed that 15 percent of New Zealanders saw the campaign within the first month, and that 62 percent of those people took action to improve their cyber security as a result of the campaign. Examples of actions were updating their passwords and enabling two-factor authentication. Over 1,300 businesses supported Cyber Smart Week – an increase from 1,200 last year. During the reporting period, research suggests the campaign reached a total of 1.97 million New Zealanders and had 9.2 million media impressions.

Building a resilient cyber security ecosystem

We work closely with key players in New Zealand's IT and communications ecosystem to build the resilience of New Zealand's cyber security ecosystem. These include government agencies, telecommunications network operators, critical infrastructure providers, and the digital supply chain. Decisions made by these key players have an outsized impact on the cyber security of all New Zealanders, and can also drive cyber security uplift in other areas of the economy.

Through our role as Government Chief Information Security Officer (GCISO), we provide system stewardship of information security for the public sector. We also provide national security advice to inform regulatory decision-making on technology investment in areas critical to New Zealand's national security.

Through our Pacific Partnerships Team we work with Pacific states to help improve their cyber resilience. This reflects the importance of a secure and resilient Pacific, and the value of our partnerships with our Pacific neighbours. Our Pacific Partnership Programme supports institution building, workforce development and awareness raising and leads New Zealand's engagement in regional cyber security. This includes co-chairing the workforce capability working group of the Pacific Cyber Security Operational Network (PACSON) and delivering its annual awareness raising campaign.

Key achievements

- In October 2024, we launched the Vulnerability Insights Programme: a service that proactively scans for and notifies customers in the public sector about cyber security vulnerabilities affecting their systems. Since launch, we have expanded coverage to scan over 200,000 devices across 122 organisations. In addition to monthly vulnerability reports for these organisations, we issued 92 alerts for high-impact vulnerabilities within 24 hours of identification. We have observed organisations patching or disabling vulnerable services after receiving reports, with positive feedback from customers relating to the discovery of vulnerabilities previously unknown to their organisations.
- We began consultation with government agencies on Minimum Cyber Security Standards, ahead of future publication. These standards will provide greater clarity for GCISO-mandated agencies about where to prioritise cyber security efforts. The standards are designed to focus on the basics, to create visibility of cyber security practices, and to drive an uplift. Reporting on the standards will provide system level insights; we will use this to improve our products and services.
- We co-chair Security Information Exchanges to share cyber security insights and best practice specific to different sectors. This year, we established two new groups and co-chaired 29 such exchanges across eight sectors: energy, finance, government, network-providers, universities, and transport and logistics, water, and health.
- We published 15 advisories with our international partners to raise awareness of cyber security threats and provide information of value to cyber defenders to mitigate malicious cyber activity. This included co-publishing advice with the Australian Signals Directorate to help organisations prepare for and respond to denial-of-service attacks, after we observed New Zealand organisations being increasingly targeted by such attacks last year.
- We continued to provide national security advice and risk assessments this year to inform regulatory decision-making on technology investment.

Our work in 2024/25

	2020/21	2021/22	2022/23	2023/24	2024/25
Number of network change proposal notifications received and processed under Telecommunications	141	179	159	143	122

(Interception Capability and Security) Act 2013					
Number of assessments of regulated space activities under the Outer Space and High-altitude Activities Act 2017	29	19	20	21	25
Number of assessments of regulated radio spectrum activities under the Radiocommunications Act 1989	Not recorded	55	45	74	65
Number of proposals for overseas investment that we provided advice on under the Overseas Investment Amendment Act 2021	69	42	42	39	46

Countering serious harms

We have the mandate, relationships and capability to understand and counter the most serious potential cyber security harms New Zealand faces. Where we have visibility, we can identify threats to New Zealand systems, and can block or remediate these threats before they can cause an impact. We also work with other government agencies to ensure that New Zealand's classified information is protected.

Key achievements

- Our cyber defence capabilities – including our CORTEX suite of detection services and flagship Malware Free Networks® (MFN®) threat detection and disruption service – continued to prevent harm to New Zealanders this year.
- Our CORTEX suite of services prevented approximately NZ$47.9 million worth of worth of harm to New Zealanders in 2024/25.
- A combined total of 473.4 million malicious cyber incidents have now been disrupted through MFN. This is a significant increase from last year's cumulative 10 million disruptions, and 390,000 cumulative disruptions the year before. MFN helps New Zealanders avoid costly security incidents and makes a real difference to everyday New Zealanders' lives. These figures reflect our efforts to automate the disruption of malicious cyber activities through MFN that have been detected through CORTEX.
- We help ensure New Zealand's most sensitive communications are not intercepted or compromised. We carry out accreditation services to check that highly classified information systems and sites are safe and secure for use, and undertake inspections to counter the potential for hostile actors to intercept information through eavesdropping, video surveillance, or the collection of unintentional emanations signals from ICT equipment.

Part C: Year-end performance information on appropriations

How we measure performance

Reporting entity

The GCSB is a New Zealand government department as defined by section 5 of the Public Service Act 2020. The relevant legislation governing our operations includes the Public Finance Act 1989, Public Service Act 2020 and Intelligence and Security Act 2017.

The GCSB is New Zealand's lead agency for signals intelligence (SIGINT) and lead operational agency for cyber security. We do not operate to make a financial return, and we are a Public Benefit Entity (PBE) for performance reporting purposes.

Our performance framework (see page 10) sets out how we measure, track, and report on our strategic intentions and outcomes. We measure the services we provide to the Government, our customers, and the public that support us to achieve these outcomes. We measure our outputs across these outcomes.

We are funded through one appropriation, Vote Communications Security and Intelligence. The appropriation contains a group of output performance measures and standards to assess how well we deliver our services and activities.

The majority of our performance information is classified and cannot be released publicly. Where performance information is unclassified and can be released, it is set out in the following pages (pages 20-25).

Statement of Compliance

Our performance information is prepared in accordance with Tier 1 PBE accounting standards, which have been applied consistently throughout the 2024/25 financial year.

This includes compliance with the new PBE FRS 48 Service Performance Reporting standard. The standard sets principle-based requirements around the selection and presentation of performance information that is appropriate and meaningful to readers.

Critical reporting judgements, estimates, and assumptions

We use a framework of performance measures to help us achieve outcomes for New Zealand, contribute to Government priorities, improve outcomes for customers and deliver high-quality services. The measures included this year help assess our progress and results.

Our performance measures are reviewed each year. Performance measures are selected through consultation with subject matter experts with consideration for measures that best demonstrate performance against our key functions and activities, the availability of data and relevance to the result or outcome we are trying to achieve. We have discretion to select our measures and targets.

For comparability and consistency, we maintain a core set of performance measures each year. This allows us to compare performance from prior years and maintain visibility of critical performance areas over time.

Contextual information

We have included comparison of our 2024/25 performance measures against the results for 2023/24. The 2024/25 actual results in this section are audited. The 2023/24 comparative results are unaudited.

We provide additional information to explain any significant changes in performance or where standards have not been met.

Minister satisfaction surveys

In keeping with the Policy Quality Framework provided by the Department of the Prime Minister and Cabinet (DPMC) we survey our Minister each year to assess their satisfaction with the policy advice and ministerial servicing we provide (page 23). The survey measures our Minister's satisfaction across four areas on a five-point scale. The survey is amended slightly from DPMC's Ministerial Policy Satisfaction Survey to reflect the

Minister's role in signing intelligence warrants. The survey was completed by the Minister Responsible for the GCSB in July 2025.

How we performed against our output measures

	Standard	Results	
Impact	**Standard**	**2025**	**2024**
New Zealanders' ability to secure their information technology systems and infrastructures continuously improves	There is a year-on-year increase in consumption of NCSC's content and services (measured by web traffic, social media engagement, and advisory subscribers)	Achieved	Not achieved

Assessment of achievement

On average, there was a 4.47 percent increase in the consumption of NCSC's content and services this year. This considers the following statistics:

- Website visits increased by 15.10 percent
- Twitter followers went down by 13.87 percent
- Subscribers to four CERT NZ channels went up 12 percent.

In 2024, our content consumption was 86 percent, which was 7 percent lower than the previous year (93 percent). This was due to:

- Heightened traffic in 2022/23 caused by national and international cybersecurity events that were not repeated in 2023/24
- An increased cost in advertising, reducing the potential reach of our advertising, and
- The reduced popularity of X (formerly Twitter) as a social media platform this year.

Impact	**Standard**	**2025**	**2024**
Nationally Significant Organisations embrace technology responsibly and securely	*Regulatory responsibilities fulfilled in accordance with service agreements 95 percent of time.*		
	95% of responses made to notifications made under section 48 of the Telecommunications (Interception Capability and Security) Act 2013 provided in 20 days or less	95%	99%
	Percentage of national security risk assessments completed within 30 days of receiving an application under the Outer Space High-altitude Activities Act 2017	100%	100%
	Percentage of national security risk assessments completed within 50 days of receiving an application under the Outer Space and High-altitude Activities Act 2017	100%	100%
	Percentage of advice provided to the Overseas Investment Office within 10 working days of receiving notification of the transaction	98%	97%

Notes:

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 the TICSA. Part 3 of the 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.

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 (OSHAA), and Radiocommunications Act 1989. This national security risk assessment advice is used to inform Ministers.

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 considers national security.

Assessment of achievement

- The GCSB received 122 notifications under TICSA. We responded to 95% within 20 working days or less.
- The GCSB received 25 notifications under OSHAA. We responded to 100% within 30 working days and 100%within 50 working days.
- The GCSB received 46 notifications from the Overseas Investment Office. We responded to 98% within 10 working days.

	Standard	Results	
Impact	**Standard**	**2025**	**2024**
The Minister responsible for the GCSB receives best possible advice	The Minister Responsible for the GCSB rates GCSB's advice at least 3.5 (average) on a 5-point scale.	Achieved (4.46)	Achieved (4.6)

We survey our Portfolio Minister each year to assess their satisfaction with the advice we provide. The survey measures Ministerial satisfaction across four areas: general satisfaction, quality of advice, warrants, and overall performance.

	Standard	Results	
Outcome: Social licence from New Zealand's public allows GCSB to operate effectively			
Impact	**Standard**	**2025**	**2024**
Oversight agencies are confident in GCSB's legal compliance	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.	Achieved	Achieved
Notes The IGIS rates the GCSB's compliance across five categories, with a rating assigned from a four-level scale: strong, well-developed, under-developed, inadequate. To achieve this measure, the GCSB must be well-developed or strong in four of the five categories. Assessment of achievement As at 30 June 2025, the IGIS provided the following ratings for the GCSB's compliance performance. • Operational policy and procedure: Under-developed • Internal compliance programmes: Well-developed • Self-reporting and investigation of compliance incidents: Well-developed • Training: Well-developed • Responsiveness to oversight: Well-developed These ratings will be confirmed when the IGIS Annual Report is published following the Prime Minister's presentation to the House. The IGIS notes the ratings are extremely unlikely to change.			
GCSB meets its legal obligations: Official Information Act 1982	100 percent of OIA requests are completed within the legislated timeframe	Not achieved	Achieved
	More than 50 percent of Ombudsman complaints are resolved or found in favour of the GCSB	Achieved	Achieved
Assessment of achievement The GCSB completed 68 OIA requests during the performance year, with a median response time of 20 working days. The GCSB responded to 98.5 percent of requests within the legislated timeframe, with one request responded to late. The GCSB was notified of two complaints to the Office of the Ombudsman during the reporting period. Both complaints were resolved with the Ombudsman finding in the GCSB's favour: one by 30 June 2025 and the other after 30 June 2025. One complaint was resolved with the Ombudsman finding in the GCSB's favour; the other was resolved in the GCSB's favour outside of the reporting period.			
GCSB meets its legal obligations: Privacy Act 2020	100 percent of Privacy Act requests are completed within the legislated timeframe	Achieved	Achieved
	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	Achieved	Achieved
Assessment of achievement The GCSB completed 34 Privacy Act requests during the performance year, with a median response time of 12			

working days. All requests were responded to within the legislated timeframe.

The GCSB was not notified of any complaints to the Office of the Privacy Commissioner during this period.

Organisational health and capability

Our people

The GCSB continues to prioritise initiatives to attract and retain a diverse workforce, including competitive remuneration, closing gender and ethnic pay gaps, enabling more flexible working, investing in employee development and fostering an inclusive culture. The GCSB shares corporate service functions with the NZSIS.

Workforce changes

The GCSB and the NZSIS undertook a joint work programme in late 2023 to ensure our two agencies are financially sustainability in the longer term, and in the context of the current fiscal environment. This included a joint review of our workforces in 2024. This was separate from the efficiency savings sought through the Budget 2024 Initial Baseline Exercise. The change process also focused on maintaining core business, maximising alignment between the agencies and reducing unnecessary duplication.

The change process addressed these cost pressures in the near term. It involved the reallocation of vacancies and certain roles, including disestablishing some roles, and redeploying some of our shared staff in joint enabling functions between the NZSIS and the GCSB. A small number of people from across the GCSB and NZSIS were made redundant through this change process. This change process also led to the creation of roles within new organisational structures. The changes were implemented in early March 2025, with recruitment underway.

The overview of the change process provides an account of the agencies evolving role structure, highlighting both current vacancies and filled positions in the context of recent workforce changes, including role reallocations, disestablishments, and redeployments. In contrast, the table below outlines data related to our current workforce, reporting solely on roles that are currently filled. Vacant positions are not reflected in the table.

Workforce profile as at 30 June 2025

	2020/21	2021/22	2022/23	2023/24	2024/25
Headcount	551	535	546	605	601
Full-time equivalents (FTEs)	543.9	527.6	539.8	596.7	589.3
Average age (years)	43.1	42.7	42.2	41.7	42.4
Unplanned turnover (percent)	8.1	19.3	15.6	11.2	10.9
Average length of service (years)	6.4	6.5	6.3	5.9	6.3

Promoting diversity and inclusion

Like New Zealand, our workforce and work environment is diverse, and our collective diversity is celebrated and embraced. Our mission of keeping New Zealand and New Zealanders safe from significant national security threats is strengthened through the different ideas, perspectives, skills, and experiences of staff.

What we did to promote diversity and inclusion in 2024/25

We focused on maintaining work underway, for example, our Kia Toipoto Pay Gap Action Plan. A key highlight of this was the finalisation of our Behavioural Competency Framework, and work to embed this into relevant people policies, processes and practices.

In addition, we developed and implemented our People Leader programme. This is a compulsory programme for all new managers, which embeds our essential Diversity and Inclusion training. We also continued to work on improving our data collection to better measure the impact of activities undertaken to embed diversity and inclusion within our people policies, processes and practices.

Demographic profiles of our workforce as at 30 June 2025[3]

Gender (percent)	2020/21	2021/22	2022/23	2023/24	2024/25
Male	64.5	61.1	63.2	64.0	64.2
Female	34.9	37.9	35.5	35.2	34.9
Another gender	0.2	0.2	0.6	0.8	0.7
Undisclosed	0.4	0.8	0.7	0.0	0.2

Ethnicity (percent)	2020/21	2021/22	2022/23	2023/24	2024/25
European	76.0	74.6	77.5	77.7	76.9
New Zealander	22.8	18.5	-	-	-
New Zealand Māori	7.2	9.1	9.8	9.5	9.7
Asian	7.2	7.3	7.3	9.0	8.8
Pacific Peoples	2.6	3.2	3.1	3.3	3.6
Middle Eastern, Latin American, and African (MELAA)	1.2	1.6	0.8	1.1	1.1

[3] Staff can choose whether or not to disclose their ethnicity. The ethnicity metrics 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.

Other	0.2	0.2	15.7	13.0	14.4

Demographic profile of our senior management as at 30 June 2025

Gender (percent)	2020/21	2021/22	2022/23	2023/24	2024/25
Male	47.8	36.8	40.0	46.9	48.5
Female	52.2	63.2	60.0	53.1	51.5
Undisclosed	-	-	-	-	-

Senior Management (Tier 2 and 3) percent					
European	New Zealand Māori	Asian	Pacific Peoples	MELAA	Other
77.4	22.6	6.5	-	-	16.1

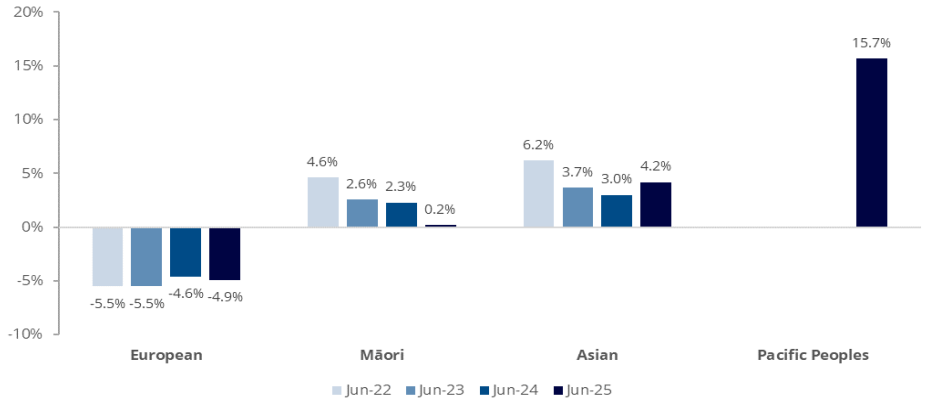
Gender Pay Gap

The gender pay gap is a high-level indicator of the difference between female and male earnings. It is a comparison of the annual fulltime salary earned by male and female staff, including permanent, fixed-term and seconded out staff in accordance with Te Kawa Mataaho guidance on calculating the gap.

Addressing our gender pay gap was a key feature of our 2021-2025 Diversity and Inclusion Strategy. As at 30 June 2025 our average gender pay gap was 1.4 percent. This is an increase of 0.3 percentage points since last year.

Ethnic Pay Gaps

Each category requires 20 or more staff to identify as part of this group to enable this reporting. This is the first year that Pacific Peoples has been included as a category in our agency's data as there are now 20 or more staff that identify within this group.



Progress against Te Kawa Mataaho Papa Pounamu Commitments

Te Urupae i te Mariu | Addressing bias

- 72.2 percent of GCSB people leaders and 87.5 percent of our senior management completed our Understanding & Managing Unconscious Bias learning module.

Te āheinga ā-ahurea | Cultural competence

- We have further refined our Pasifika Matters Workshop, which explores the diversity of the Pacific Island region and the relationship with, and experience of, Pasifika people in Aotearoa New Zealand.
- We continued to deliver workshops which develop our people's capability to engage effectively with Iwi and Māori in undertaking our national security functions. These are key to ensuring we can attract and retain the talent required to achieve our national security outcomes.

Hautūtanga Ngākau Tuwhere | Inclusive leadership

- We launched our new People Leaders programme, designed to provide a clear understanding of how to manage, and also manage within the context of our workforce. The programme follows best practice inclusive leadership practices, as well as other internal frameworks, such as our recently completed Behavioural Competency Framework – which is being implemented in 2025/26. All current People Leaders are expected to complete the programme. Following this, all new People Leaders will complete the programme within three months of beginning their Leadership position.
- We finalised our new People Leader Pathway. The pathway is designed to support our People Leaders accessibility to essential learning, as well as recommended learning, all of which covers content from Management, Leadership, and Coaching practices. This will be launched to all People Leaders in 2025/26.

Ngā tūhohonga e kōkiritia ana e ngā kaimahi | Employee-led networks

- We formally launched our newest employee-led network, Te Kāhui Māori, which is open to all staff who identify as Māori and/or have a strong interest in, or connection to, Te Ao Māori.
- Together, our Te Kāhui Māori employee-led network and Te Ao Māori team developed tikanga and kawa guidance for the NZIC, aimed at ensuring our people are able to lead and support mihi whakatau and pōwhiri.

Hautūtanga Kākano Rau | Fostering diverse leadership

- We will be exploring this further in the next iteration of our Diversity and Inclusion Strategy, and new Workforce Capability Strategy, which are due to be delivered in 2025/26 and 2026/27 respectively.

Providing a safe and healthy workplace

The health, safety and wellbeing function exists to protect our people and support our People Leaders to meet their responsibilities under the Health and Safety at Work Act 2015. This includes providing clear advice, building capability and enabling leaders to exercise due diligence. By fostering safe, healthy and supportive environments, we support the mission by helping everyone succeed in their roles and thrive at work.

Governance and leadership

As part of the transition programme, a new vision for future-state governance was developed. This included the finalisation of new terms of reference for our joint GCSB and NZSIS Health and Safety Governance Groups. These groups include all senior leaders from each agency. Together, they exercise due diligence and ensure health, safety and wellbeing are strategically prioritised.

We continue to strengthen engagement through our Health and Safety Representatives. Investment in Health and Safety Representative training and support was highlighted by our 2025 Health and Safety Representative Conference. Leaders also joined Health and Safety Representatives on frontline work area walks to better understand the realities of "work as done".

This year, we reviewed our Health, Safety and Wellbeing Policy to reinforce our commitment to continual improvement and practical risk management. Our Wellbeing Psychology Services Policy, including psychosocial and psychological support services, was also reviewed to better reflect the needs of our people.

Capability and capacity

Senior leaders are active participants in the Business Leaders' Health and Safety Forum. We are also members of the Government Health and Safety Lead, where we delivered a Positive Workplace Cultures programme in July 2024, to support safer, more respectful workplaces.

In delivering Mātai, our all-of-government data centre, we demonstrated how overlapping duties can be managed in practice. A dedicated Senior Health and Safety Advisor supported the coordination of contractors and partners. The project was completed with one notifiable (non-injury) incident reported, and no notifiable events in the 2024/25 year.

Risk management

We continue to build a deeper understanding of our critical risks by engaging directly with workers through targeted surveys and structured analysis. These insights help us explore how our people interact with high-consequence risks in practice and ensure our risk management strategies reflect real-world work.

At the same time, we are strengthening our approach to more frequent, lower-impact risks by embedding hazard and risk management frameworks that build frontline capability and ownership. This includes equipping workers and teams with the tools and confidence to proactively identify, assess and respond to risk in diverse working environments.

Building our Māori Cultural Capability

Like other enabling functions in our agencies, the GCSB and the NZSIS have a shared Te Ao Māori team, whose insights helped reset our respective organisational strategies. Our Māori Cultural Capability is key to both organisational strategies, which signal the shared ambition to be an honourable and capable Treaty partner. Building our Māori cultural capability therefore continues to be a critical factor in enabling our people, systems and processes to give effect to the Treaty of Waitangi.

The Māori Outcomes Strategy – He Waka Haumaru continues to provide a roadmap in lifting organisational Māori cultural capability. The strategy is supported by three strategic pou outlined below, which are each underpinned with objectives and initiatives.

Kia Hono - Trusted partnerships

We continued to engage with Iwi Chairs and strengthen relationships with mana whenua this year. Work remains underway to enhance our service delivery to improve national security outcomes for Māori.

Kia Maia – Culturally Capable

We continue to provide various learning and development opportunities for staff to build their competency in te reo Māori. During the reporting period, we released new online courses focussed on increasing knowledge in Te Ao Māori and the Treaty of Waitangi. Tikanga Māori continues to be an integral part of workplace culture, extending through to the formal welcomes for new staff, international guests and delegations. Our Māori staff network, Te Kāhui Māori, plays a leading role in uplift activities and events.

Kia Manawanui – Building Resilience

We initiated the formation of a Protective Security Māori Stakeholder Reference Group. The purpose of establishing this group was to seek expert advice on shaping protective security guidance to increase the accessibility, resonance and impact for Māori. The Reference Group meets on a bi-monthly basis and is assisting in the design and delivery of a new product for Māori audiences, and is identifying effective engagement channels and opportunities to partner for impact.

Delivery of Mātai, our 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 most sensitive official information. This was an important build that will significantly strengthen the resilience of the Government's digital infrastructure.

The Minister Responsible for the GCSB, Hon Judith Collins KC officially opened the Data Centre on 27 June 2025. The Data Centre is an investment that had been years in the planning, with earthworks commencing in 2021, and construction beginning in September 2022.

Carbon Neutral Government Programme

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

Independent Verification

The GCSB has completed independent emission verification with Toitū against ISO14064-1:2018 for 2018/19 (our baseline year), as well as 2021/22, 2022/23, and 2023/24. The emissions reported here have not been independently verified for 2024/25 at the time of reporting.

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

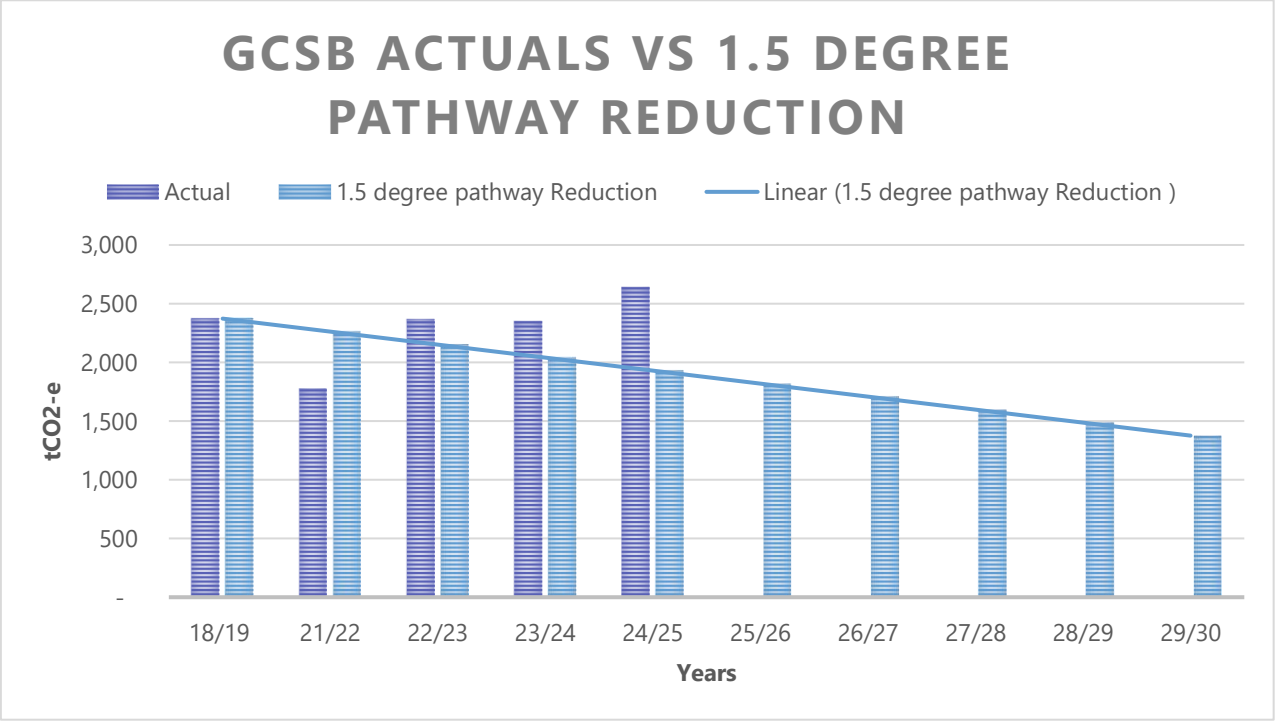
In 2024/25 we estimate we emitted 2,645 Tonnes CO2-e, based on our sampled data and extrapolation. This compares to our verified figure of 2,350 Tonnes CO2-e in 2023/24. Most of our emissions came from passenger transport, as well as electricity and motor vehicles.

Our all-of-government data centre is not included in the inventory for 2024/25, as it was officially opened on 27 June 2025. It will be included in the inventory for the next financial year.

Our Reduction Targets and Results to 1.5 Degree Pathway Reduction

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 1,930 Tonnes CO2-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 CO2-e, or a 42 percent reduction in gross emissions (all Categories) compared to base year



Financial Statements

Statements of Expenses and Capital Expenditure against Appropriation

For the year ended 30 June 2025

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

	$000
Total appropriation	$384,549
Actual expenditure	$287,638

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.

Independent Auditor's Report

Independent Auditor's Report

AUDIT NEW ZEALAND
Mana Arotake Aotearoa

To the readers of the Government Communications Security Bureau's annual report for the year ended 30 June 2025

The Auditor-General is the auditor of the Government Communications Security Bureau (the GCSB). The Auditor-General has appointed me, Kelly Rushton, 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 of the GCSB for the year ended 30 June 2025 on page 35.
- The end-of-year performance information of the GCSB for the year ended 30 June 2025 on pages 20 to 25. The end-of-year performance information presented is the unclassified performance information and is a subset of the GCSB's full performance information for the appropriation.

Opinion

In our opinion:

- The statement of expenses and capital expenditure incurred in relation to the appropriation for the year ended 30 June 2025 is presented fairly, in all material respects, in accordance with the requirements of section 221(4)(a) of the Intelligence and Security Act 2017.
- The presented end-of-year performance information accurately reports, in all material respects, the GCSB's actual performance against the presented performance measures.

Our audit was completed on 30 September 2025. This is the date at which our opinion is expressed.

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, the International Standards on Auditing (New Zealand), and New Zealand Auditing Standard 1 (Revised): The Audit of Service Performance Information 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 of the GCSB that is presented fairly, in all material respects, in accordance with the requirements of section 221(4)(a) of the Intelligence and Security Act 2017.
- Preparing end-of-year performance information for the appropriation that provides an appropriate and meaningful basis to assess what has been achieved with the appropriation and fairly presents what has been achieved and that complies with generally accepted accounting practice in New Zealand.

- Selecting from the full end-of-year performance information for the appropriation the unclassified performance information, that is a subset of the GCSB's full performance information, and presenting unclassified performance information that accurately reports, in all material respects, the GCSB's actual performance against the unclassified performance measures.

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's responsibilities arise from the Intelligence and Security Act 2017 and the Public Finance Act 1989.

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 of Appropriations for the Government of New Zealand for the Year Ending 30 June 2025.

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 evaluate whether the end-of-year performance information that is presented accurately reports, in all material respects, the GCSB's actual performance against the presented performance measures.
- We evaluate whether the statement of expenses and capital expenditure has been prepared in accordance with legislative requirements.
- We conclude on the appropriateness of the use of the going concern basis of accounting by the Director-General of the GCSB.

- 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.

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 all of the information included in the annual report other than 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) 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.

Kelly Rushton
Audit New Zealand
On behalf of the Auditor-General
Wellington, New Zealand

Other matters

Statement of Warrants

In accordance with section 221(2) of the ISA, the following statements are provided for the period 1 July 2024 to 30 June 2025.

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 of the ISA.

Intelligence Warrants

A total of 22 intelligence warrants were issued in 2024/25, of which 12 were Type 1 intelligence warrants and ten 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.

Urgent warrants

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

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 of the ISA. Very urgent authorisations are authorised by the Director-General where a situation of urgency exists and the delay in making an application for an urgent warrant to a Commissioner of Intelligence Warrants and the Minister orally 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.

Restricted Information

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

Business Records Directions (section 221(2)(h) of the ISA)

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