G.56 (2021)

GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

ANNUAL REPORT 2021
TE PŪRONGO Ā-TAU 2021

Protecting and Enhancing New Zealand’s Security and Wellbeing.

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

Preface

This is the annual report of the Government Communications Security Bureau (GCSB) for the year ended 30 June 2021, presented for consideration and scrutiny by the Intelligence and Security Committee.

Presented to the House of Representatives pursuant to section 221 of the Intelligence and Security Act 2017.

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://creativecommoncs.org/licences/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.

CONTENTS

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

The Government Communications Security Bureau (GCSB) has contributed in important ways to key Government priorities throughout a year of high operational tempo, for both its cyber security and signals intelligence missions. Alongside our cyber security and signal intelligence work, we have also been focused on building new capabilities that will ensure the GCSB is prepared for the future.

The reverberations of the COVID-19 global pandemic continue to affect almost every aspect of how we go about our lives and conduct our business. These changes have also influenced the GCSB's operational focus and we have played a key role in providing cybersecurity advice and guidance to New Zealand's nationally significant organisations and government agencies.

COVID-19 has required a rapid shift in the way New Zealanders work, with the need to connect to central systems from dispersed locations, as well as an increased need for virtual meeting and communication tools. This new way of working creates new cyber security vulnerabilities and risks because it increases what we call the "attack surface", which malicious operators can exploit.

Cyber security threats are increasing in number, complexity and impact, and are coming from a range of sources including state-backed and criminal groups, and issue motivated individuals. Of the 404 recorded incidents during 2020/21, 28.4 per cent were attributed to state-sponsored actors. Non-state actors are also becoming far more sophisticated, with activity once seen only from well-resourced state-backed actors now being deployed by criminal actors motivated by financial gain.

Cyber incidents such as ransomware and supply chain attacks are becoming more prevalent as we see changes in the tactics, techniques and procedures that malicious actors employ. These changes, along with the continued blurring of lines between state sponsored and criminally motivated actors and the greater use of malware 'as a service' all contribute to a challenging operational environment for the GCSB.

Throughout 2020/21 the GCSB, through its National Cyber Security Centre (NCSC) has responded to several high profile cyber security incidents, including the Waikato District Health Board (DHB) ransomware attack, and the Denial of Service attacks on the New Zealand Stock Exchange.

As part of its role, the GCSB carries out technical analysis of malicious cyber activity, which informs our understanding of the scale of activity and impact on New Zealand. The New Zealand Government will, from time-to-time, publicly call out those responsible, as we saw in April 2021 with the Government joining international partners in attributing the exploitation of the SolarWinds Orion platform to Russian state actors. A significant compromise of the Microsoft Exchange service became publicly known during the year and was attributed to Chinese state actors by the New Zealand Government, and others, in July 2021. New Zealand has also added its voice to condemning malicious activity targeting COVID-19 research.

Our relationships with partners, both here and overseas, are a key part of the work we do. These relationships improve cyber resilience across the public sector and organisations of national significance, as well as supporting our response to cyber incidents.

The GCSB's Signals Intelligence (SIGINT) function has seen a similarly busy operational year. The GCSB has contributed intelligence to all 16 of the Government's National Security and Intelligence Priorities. This includes supporting the COVID-19 response and

recovery, support to military operations, informing New Zealand's understanding of geostrategic competition in our region and global efforts to counter violent extremism, including contributing to the disruption of terrorist attack planning overseas.

In November the Royal Commission of Inquiry into the terrorist attacks on Christchurch masjidain released its report. While the report made no specific recommendations in relation to the GCSB, the report noted that the GCSB should play a more active role in domestic counter-terrorism. The report suggested greater collaboration with our domestic partner agencies to help enhance the work they do.

The GCSB is committed to making our role and capabilities more widely understood and the unique intelligence we provide easier to access. This work has progressed throughout 2020/21 with the GCSB working closely with New Zealand Police, the New Zealand Security Intelligence Service (NZSIS) and other domestic partners, to support their investigations into specific threats. The provision of support to domestic counter terrorism is carefully balanced with the GCSB's contribution to other Government priorities, particularly where we are New Zealand's primary, or only, source of intelligence.

An example of our contribution to other Government priorities was our support to New Zealand Police on Operation Van, which targeted a transnational organised crime group in New Zealand. The GCSB continues to work with New Zealand Customs Service to better target drug networks, with the aim of disrupting their efforts before they reach our shores. The GCSB's collection and analysis activity enhances New Zealand Customs' understanding of drug networks that seek to smuggle drugs to New Zealand.

Against this fast-paced and ever-evolving operational backdrop we continue to focus on developing our people, capabilities and relationships. We need to ensure we have the capabilities to continue to deliver high value intelligence services and products to the Government to contribute towards keeping New Zealand safe, as well as to making a significant contribution to our international partners.

This year saw the completion of a multi-year programme of work to update New Zealand's high-grade cryptographic infrastructure and progress on the GCSB-led programme to deliver the New Zealand Top Secret Network (NZTSN), a set of technology capabilities for New Zealand's national security sector.

Along with developing our technical capabilities I am committed to our efforts to build a diverse and inclusive workplace. As New Zealand faces a changing security outlook it is important that the GCSB has a workforce with a broad skillset, with different ways of thinking and life experiences.

Significant progress has continued to be made on increasing our ethnic diversity, reducing the gender pay gap and maintaining a majority of women in senior leadership roles. It is encouraging to see this progress, and this will continue to be an area of focus, including through support to initiatives such as our women in STEM scholarship and our graduate programme.

This year has shown, once again, the dedication and resilience of the GCSB's staff. I am incredibly proud of the work they have delivered through this reporting period, in a challenging and high tempo environment. As much of our work remains secret, our staff often do not receive public acknowledgement for their contribution to New Zealand's safety and security. I would like to take this opportunity to express my gratitude for their continued efforts; it is a privilege to lead them.

Andrew Hampton

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

NOTABLE ACHIEVEMENTS
NGĀ EKENGA TAUMATA

Impenetrable Infrastructure

Cyber security incidents

The National Cyber Security Centre (NCSC) recorded 404 incidents in the 12 months to 30 June 2021, involving organisations of national significance and/or having the potential to have a national impact. This compares to 353 incidents in the 2019/20 year. The NCSC has identified that 28.4 per cent of these incidents were linked to state-sponsored cyber actors.

Throughout 2020/21 the NCSC responded to several high profile cyber security incidents. These included Denial of Service (DDoS) attacks on the New Zealand Stock Exchange, and other organisations, and ransomware attacks on the Waikato District Health Board.

The NCSC responded to supply chain attacks involving malicious actors taking advantage of vulnerabilities, such as the SolarWinds compromise and Microsoft Exchange. The NCSC also provided support to the response to the Reserve Bank cyber incident.

2020 General Election and referendums security

In 2020 the GCSB, along with the NZSIS, contributed to multi-agency support for New Zealand's General Election and referendums. Part of this work included updating principles and protocols to establish thresholds for escalating cyber security threats to the broader national security system. This principles and protocols were not triggered.

COVID 19 response and recovery

The NCSC is working alongside CERT NZ and other New Zealand government agencies to support the Ministry of Health's COVID 19 Immunisation Programme. As part of its support for the COVID-19 vaccine rollout programme, the NCSC prepared a cyber security threat assessment. To date, the NCSC has no information to indicate that malicious cyber actors plan to directly or indirectly target organisations involved in the rollout of the vaccine in New Zealand.

APEC Support

The NCSC provided ongoing support to the Ministry of Foreign Affairs and Trade's hosting of APEC21. This included the provision of cyber security advice and guidance for delivery of the APEC21 virtual meetings.

CORTEX cyber defence

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

In 2020/21 the detection and disruption of malicious cyber activity, by CORTEX capabilities, prevented $119 million worth of harm to New Zealand's nationally significant organisations. This means that since June 2016, CORTEX capabilities have reduced harm from hostile cyber activity by around $284.2 million.

Malware Free Networks

The GCSB's Malware Free Networks (MFN) capability is a threat intelligence feed that contains indicators of malicious activity generated from a range of sources. MFN is a new malware detection and disruption service that enables us to significantly scale our cyber defence effort across a much larger range of New Zealand organisations.

The MFN capability went live in June 2021. Over the past 12 months the NCSC has worked with a range of network operators and commercial security service providers to expand the number of organisations able to be protected by the MFN threat intelligence service.

Cyber security customer engagement

The NCSC works closely with a range of nationally significant organisations to understand their level of cyber resilience and vulnerability to attack. As part of this work the NCSC provides advice, support and cyber threat alerts to help organisations lift their overall cyber security resilience.

The Cyber Resilience Unit (CRU) coordinates security information exchanges. These information sharing sessions provide participating organisations with opportunities to share information in a confidential and trusted environment. This work enhances collaboration on cyber security challenges and opportunities across a broad range of nationally significant sectors. In this reporting period the CRU hosted 22 information exchanges and is in the early stages of standing up two more. These information exchanges resulted in 1867 engagements with customers across a broad spectrum of public and private sector organisations.

Cyber security advisories

In the 2020/21 year the CRU published 31 reports for general customers identifying specific cyber security vulnerabilities, providing cyber threat mitigation advice and reinforcing cyber security best practice to raise overall cyber security resilience.

In addition to the above there were 16 publications released on the NCSC website. This included two campaigns targeting Incident Management and Supply Chain Cyber Security risks.

Government Chief Information Security Officer

The Government Chief Information Security Officer (GCISO) role helps the GCSB to improve government agencies' cyber resilience. Through this role we support the Government's digital transformation programme. In the 2020/21 year this included working with major cloud service providers to develop security templates for the implementation of their cloud products. These templates help increase the baseline security of those products by building core New Zealand Government information security standards into their basic implementation.

The GCSB, in its GCISO role, continues to work with the Department of Internal Affairs' Government Chief Digital Officer, on system settings and leadership needed to improve how the public service operates in a digital environment.

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

The GCBS's role under TICSA is to assess any changes to public telecommunications networks that may introduce network security risks.

During the reporting period, the GCSB received 141 notifications from network operators regarding proposed changes to their networks. The GCSB continues to see a trend in these notifications in relation to the rollout of fifth generation mobile services (5G).

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

The GCSB, in conjunction with the NZSIS, undertakes a national security risk assessment for any application for a license or permit submitted under OSHAA. During the reporting period, the GCSB conducted 29 national security risk assessments. These assessments provided the basis for advice from the Minister responsible for the GCSB and NZSIS to the Minister of Economic and Regional Development, who is responsible for OSHAA.

Overseas Investment Act 2005

On 16 June 2020, an emergency notification regime for foreign investment came into force, overseen by the Overseas Investment Office. The GCSB supports the NZSIS in the assessment of transactions that may raise a national security risk. The GCSB undertook 69 assessments under the Urgent Measures amendment of the Overseas Investment (Urgent Measures) Amendment Act 2020 (OIAA).

On 7 June 2021, the emergency notification regime was replaced by a more targeted national security and public order notification regime. The GCSB, working in conjunction with the NZSIS, continues to provide assessments on relevant transactions that may raise a national security risk under this regime.

Indispensable Intelligence

Provision of Signals Intelligence

Throughout 2020/21 the GCSB has continued to provide signals intelligence against all 16 of the National Security and Intelligence Priorities (NSIPs), to agencies and their Ministers. This includes providing intelligence to support the COVID-19 response and recovery and on the geostrategic competition in our region.

Transnational Organised Crime

The GCSB works closely with a variety of government agencies, including New Zealand Police and New Zealand Customs Service to contribute to the prevention and detection of transnational organised crime. Our focus is on providing intelligence leads that will assist New Zealand Customs to prevent large scale drug importation.

In 2020/21 this work included the GCSB partnering with New Zealand Police on Operation Van, which targeted a transnational organised crime group in New Zealand.

Counter-Terrorism

The GCSB's primary focus for counter-terrorism is making a contribution to global efforts to counter violent extremism. The past year has seen the GCSB working closely with international partners to counter violent extremism, including contributing to the disruption of attack planning overseas.

Support to military operations

The GCSB continued to provide support to the New Zealand Defence Force (NZDF) for the purposes of its operations. The GCSB contributes to NZDF efforts to detect and counter threats to New Zealand military personnel deployed overseas.

Joint Customer Service Centre

In 2020/21, the joint Customer Service Centre, a joint business unit between the GCSB, the NZSIS and the Department of the Prime Minister and Cabinet (DPMC) continued to improve our approach to provision of intelligence and assessments to support our customers.

This function was established in 2019/20 and is designed to improve our understanding of our customers' business needs and how to provide high impact, tailored intelligence that will inform and shape decision making. Implementation of the joint customer services team is an ongoing process that is phased over four years.

Capability development

The GCSB made significant progress with capability development throughout 2020/21, despite a high operational tempo and COVID-19 related disruptions. These capabilities ensure that the New Zealand Intelligence Community can undertake their functions in an effective way that is compliant with the Intelligence and Security Act 2017.

The GCSB delivers high grade cryptographic infrastructure for government communications higher than RESTRICTED. The Cryptographic Products Management Infrastructure (CPMI) project was a multi year project that replaced the existing infrastructure, and was completed in 2020/21.

Throughout 2020/21 the GCSB, along with the NZSIS, established a programme of work focused on highest priority investments, from funding received in Budget 2020. This work will develop new capabilities and build capacity to respond to the GCSB's operational environment, particularly as the world recovers from COVID-19.

Organisational Health

Rainbow Excellence Awards

In October 2020 the GCSB and the NZSIS won two categories at the Rainbow Excellence Awards – the Partners Life Emerging Award and the Rainbow Tick Training and Development Award – as well as being named the Supreme Award winner.

These awards recognise our work towards creating an inclusive workplace, and reflect the work that has gone in to our Diversity and Inclusion strategy. This is an ongoing area of focus for the GCSB and the NZSIS as we strive to reflect the communities we serve.

Diversity

In 2020/21 the GCSB made significant progress towards its ethnic diversity goals. We have increased the percentage of staff from ethnically diverse groups from 10.85 per cent in June 2017 to 18.34 percent. While this exceeds our goal of 13.6 percent, we acknowledge that this requires ongoing effort and our refreshed Diversity and Inclusion Strategy, which has been developed throughout 2020/21, will continue this important work.

Gender diversity is a key part of the GCSB's Diversity and Inclusion Strategy. The GCSB has exceeded its target of no less than 50 percent of our senior management group being made up of women, reaching 52.2 per cent as at 30 June 2021.

The gender pay gap

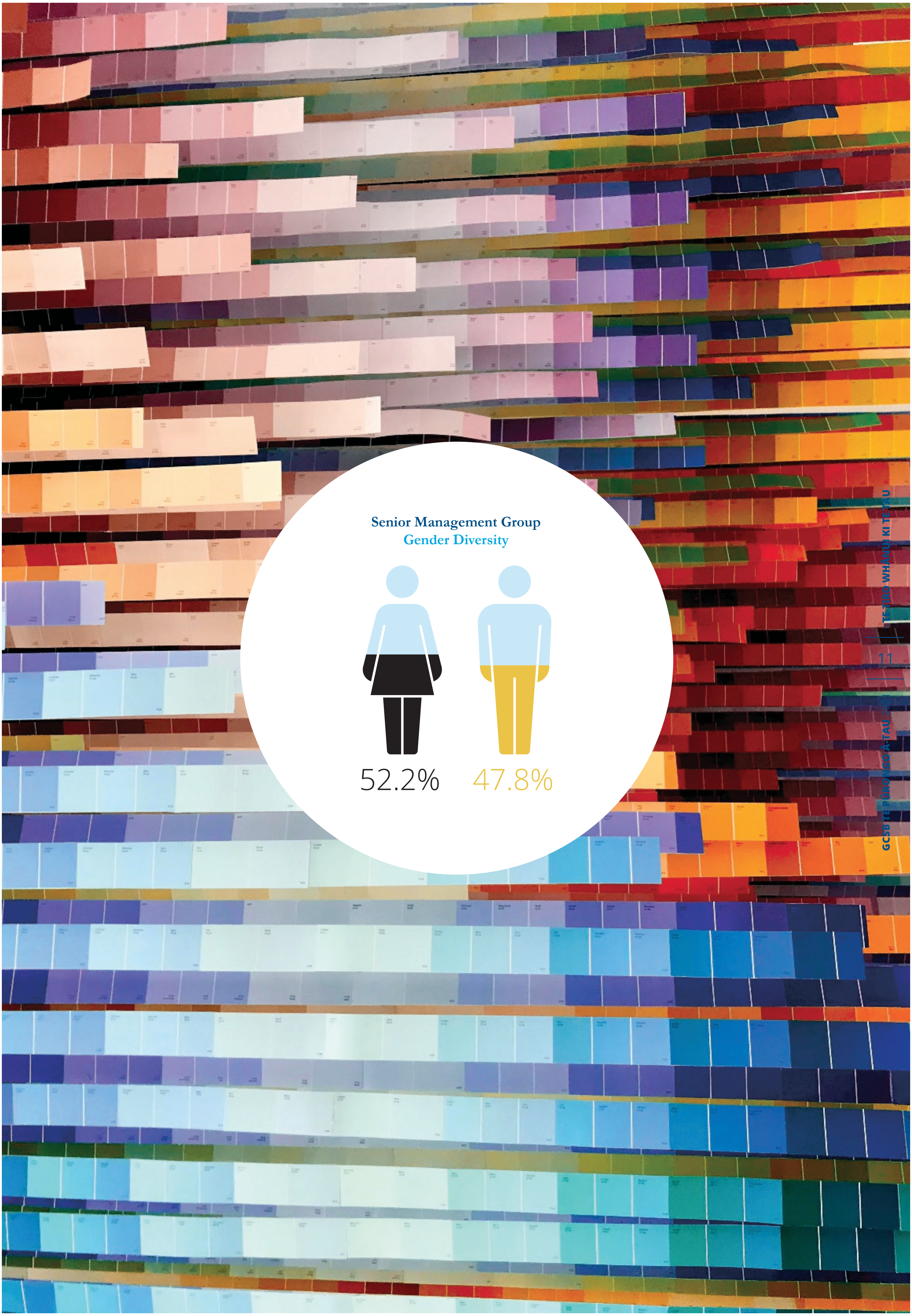
The GCSB continues to work towards its current goal of closing the gender pay gap. In 2017 when our gender pay gap was 8.7 per cent the GCSB set an initial goal of reducing the average pay gap to a maximum of 5 per cent by 2021. Throughout the 2020/21 year the GCSB achieved its goal, reaching a gender pay gap of 4.9 per cent, however due to the small size of our organisation that figure can fluctuate with small staffing changes.

At the end of the 2020/21 financial year the GCSB gender pay gap was 5.4 per cent, close to our goal of no more than five percent.

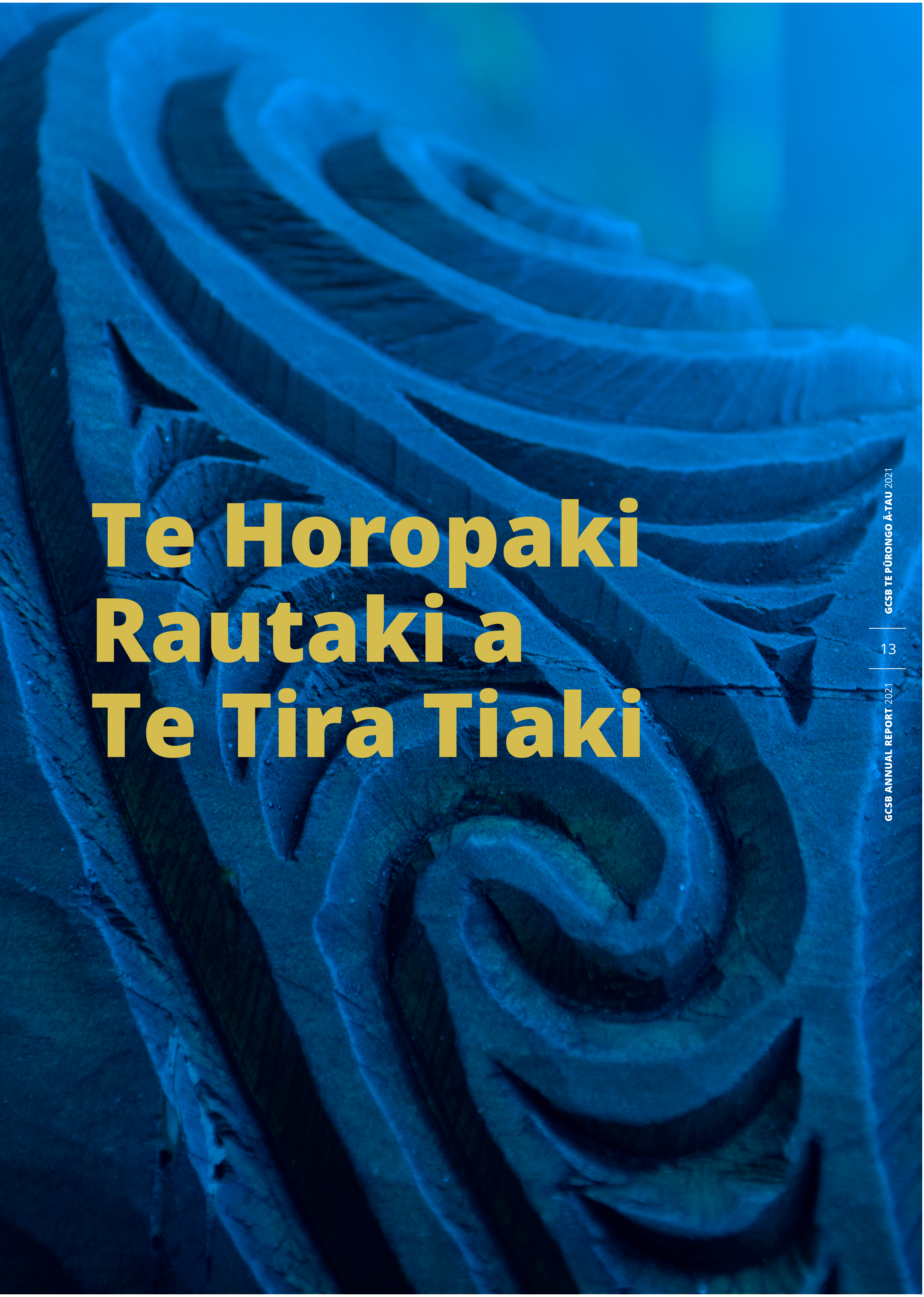
Women in STEM

Our women in STEM (science, technology, engineering and mathematics) scholarship programme is aimed at second-year and above tertiary students who are undertaking STEM disciplines at New Zealand tertiary institutions.

This year we received 126 applications, and awarded three scholarships. These scholarships can also feed into our graduate programme. In our latest graduate recruitment for the 2022 intake, three scholarship finalists, including two winners, have been appointed.


Senior Management Group
Gender Diversity

GCSB Strategic Context



Te Horopaki Rautaki a Te Tira Tiaki

THE NEW ZEALAND INTELLIGENCE COMMUNITY

The GCSB, along with the NZSIS and the National Security Group within the DPMC make up the New Zealand Intelligence Community (NZIC). The NZIC works alongside other agencies, such as New Zealand Police, New Zealand Customs Service and Immigration New Zealand to contribute to New Zealand's national security and the wellbeing of New Zealanders.

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

The NZIC strives to advance New Zealand's international reputation and interests.

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

New Zealand Intelligence Community
Te Rōpū Pārongo Tārehu o Aotearoa

The core NZIC agencies are:

Government Communications Security Bureau

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

New Zealand Security Intelligence Service

The NZSIS investigates threats to New Zealand's national security, and provides a range of protective security advice and services to the New Zealand Government.

Department of the Prime Minister and Cabinet: National Security Group

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

NATIONAL SECURITY AND INTELLIGENCE PRIORITIES

The Government's National Security and Intelligence Priorities (NSIPs) outline key areas of national security interest to the New Zealand Government. The NSIPs direct the GCSB's intelligence collection and analysis. The priorities assist agencies that have a national security role to make informed, joined-up decisions, and define key areas of focus.

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

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

The current priorities were approved in December 2018. They are listed in alphabetical order:

- *Biosecurity and human health* – Threats to New Zealand's biosecurity and human health arising from human activity.
- *Environment, climate change and natural resources* – International environment, climate change and natural resources challenges that may impact New Zealand's interests and national security.
- *Foreign influence, interference and espionage* – Acts of interference, influence and espionage in and against New Zealand that would erode New Zealand's sovereignty, national security or economic advantage.
- *Global economy, trade and investment* – Developments in international trade governance, and New Zealand's bilateral, plurilateral and multilateral trading relationships.
- *Implications of emerging technology* – The implications of emerging technology and innovation trends for New Zealand's national security, international relations and economic wellbeing.
- *International governance, geopolitics and global security* – Developments in international governance, geopolitics and global security that may impact New Zealand's interests.
- *Malicious cyber activity* – Cyber threats to New Zealand from state-sponsored and other malicious actors.
- *Middle East regional security* – The implication of events in the Middle East region on New Zealand's national security, international relations and economic wellbeing.
- *New Zealand's strategic interests in the Asia region* – The implications of events in the Asia region on New Zealand's national security, international relations and economic wellbeing.
- *Pacific regional stability* – Protecting and promoting stability, security and resilience in the Pacific region.
- *Proliferation of weapons of mass destruction and conventional weapons* – Non-proliferation and counter-proliferation of weapons of mass destruction and conventional weapons.

- *Space security* – The implications of the exploitation of space and space-based technology on New Zealand's national security, international relations and economic wellbeing.
- *Territorial security and sovereignty* – Threats to New Zealand's territorial security and sovereign rights arising from illegal, unregulated, negligent, harmful (or potentially harmful) human activity.
- *Terrorism* – Threats to New Zealand, New Zealanders and New Zealand's interests from terrorism (ideology, politically or religiously motivated violence) at home and abroad.
- *Threats to New Zealanders overseas* – Threat to the safety and success of New Zealand people, platforms and missions (military, police, diplomatic and civilian) overseas.
- *Transnational organised crime* – Threats to New Zealanders and New Zealand's interests from transnational organised crime, including trafficking, irregular migration, financial crime, fraud and corruption.

THE ROLE OF THE GCSB

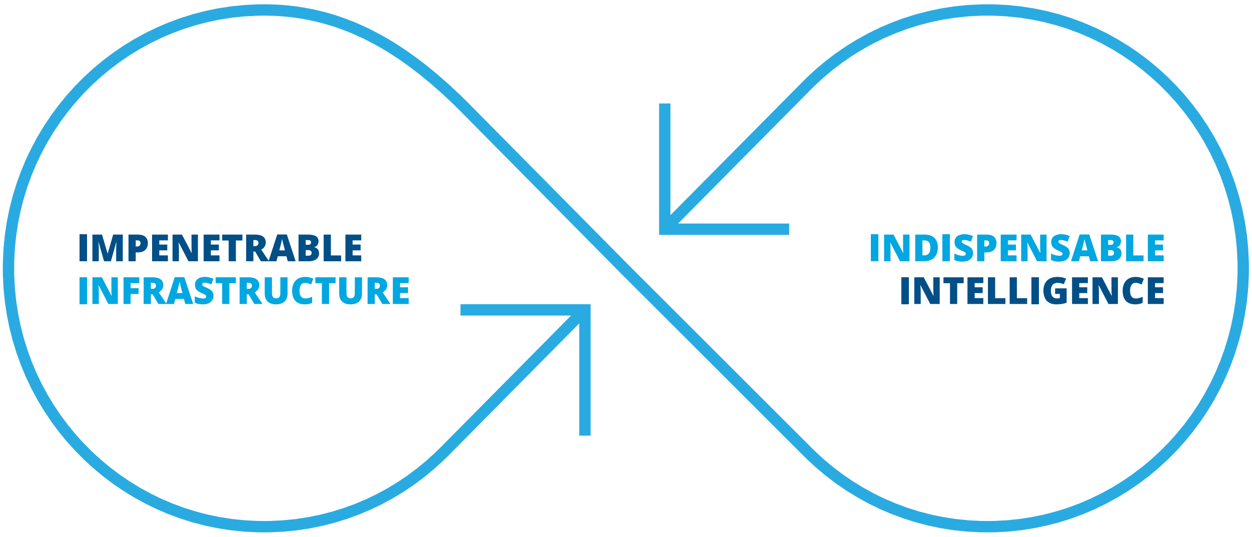
The GCSB is New Zealand's lead organisation for signals intelligence (SIGINT). We use our intelligence collection capabilities, supplemented by intelligence received from partners, to support government agencies in their operations and decision making, and to carry out their legislatively mandated functions.

Our work is driven by the priorities of Government and we provide SIGINT for all of the National Security Intelligence Priorities, either through our own or partner reporting.

We also have a statutory role to provide cyber security and information assurance services to organisations of national significance.

The GCSB is a crucial part of how New Zealand makes sense of the world and manages national security threats and in doing so contributes to the wellbeing of the nation and its citizens. The GCSB Strategy 2018 – 2022 focuses on two primary outcomes; Impenetrable Infrastructure and Indispensable Intelligence. These areas of focus contribute to New Zealand's national security by:

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



INVESTING IN OUR FUTURE

In Budgets 2019 and 2020 the NZIC received $196 million of new funding, over four years. Of this funding, the GCSB received $139 million. The GCSB received a higher proportion of the funding because it houses services shared with the NZSIS.

Throughout 2020/21 the GCSB established a programme of work focusing on highest priority investments based on their alignment and expected benefit towards Government priorities, and their ability to meet the challenges facing the NZIC.

This programme of work will develop new capabilities and build capacity to respond to an ever changing strategic environment, particularly as the world recovers from COVID-19.

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

STRATEGIC OPERATING ENVIRONMENT

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

Cyber security

New Zealand's nationally significant organisations continue to be frequently targeted by malicious cyber actors of all types. Throughout the 2020/21 year, state-sponsored and non-state actors targeted public and private sector organisations to steal information, generate revenue, or disrupt networks and services.

The NCSC recorded 404 incidents in the 12 months to 30 June 2021, compared with 353 incidents in the previous year.

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

New Zealand organisations remain the target of persistent malicious cyber activity linked to state-sponsored actors. This type of activity poses a more serious cyber security threat, as it is typically conducted for geopolitical or economic purposes and is more likely to affect organisations of national significance.

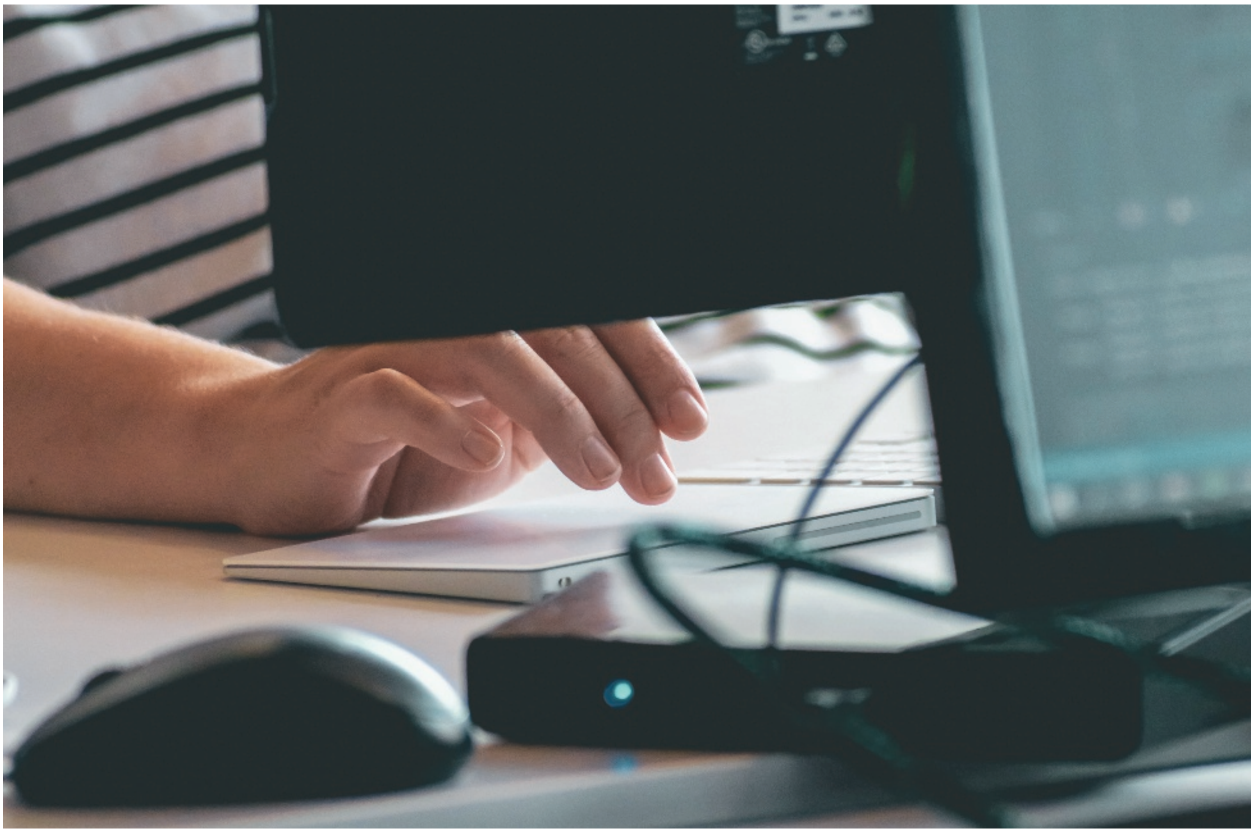
The NCSC was able to identify indicators linking state-sponsored cyber actors to 28.4 per cent of total incidents recorded in 2020/21. We have continued to see a blurring of the distinction between state and non-state actors, with well resourced and motivated criminal organisations increasingly having access to capabilities that were previously the preserve of state actors.

The GCSB is seeing changes in the way malicious actors operate, with updated tactics, techniques and procedures.

The 2020/21 year has also seen a shift to establishing more strategic access, through the compromise of critical supply chains. Increasingly, newly disclosed vulnerabilities in products and services, alongside the adoption of new services and working arrangements, are rapidly exploited by state-sponsored actors and cyber criminals alike. Changing tactics mean that every device and organisation that is potentially vulnerable to exploitation is being targeted to establish a foothold in networks. Once a foothold is established actors then selectively target further compromise.

The targeting of the Microsoft Exchange vulnerabilities, which was publicly attributed by the New Zealand Government and international partners to the Chinese state in 2020/21, is an example of this type of supply chain attack. The SolarWinds Orion attack, which involved compromising a legitimate security update prior to it being distributed by the software provider, is a similar example. The SolarWinds Orion attack was attributed by the New Zealand Government and international partners to Russia.

Greater use of 'malware as a service' has also been a trend seen throughout 2020/21. This model reduces technical barriers for actors to carry out increasingly complex and impactful campaigns, with much lower technical skill. Similarly, the blurring of the lines between state sponsored and criminally motivated actors is becoming more pronounced.



The use of ransomware, typically by financially motivated criminal actors has also been a prominent trend of 2020/21. This activity has seen a change in strategy, with broad-based campaigns targeting individuals declining and targeting of high-profile organisations increasing. These organisations are potentially more vulnerable to extortion of because the critical services they provide.

In 2020/21 there was a significant number of high profile ransomware attacks globally. These included the attack on the Colonial pipeline in the United States of America and the attack on the Waikato District Health Board here in New Zealand.

A hybrid of these tactics is Distributed Denial of Service (DDoS) attacks. These attacks do not involve encryption – the actors overload internet-facing systems with significant amounts of traffic. These actions place pressure on the targets to pay a ransom. In 2020/21 the New Zealand Stock Exchange (NZX), as well as other organisations, were the target of DDoS attacks.

The pandemic accelerated the adoption of technologies and greatly increased New Zealand's reliance on an open, secure and trusted cyberspace.

Good cyber security practices are increasingly important to safeguarding New Zealand's national security. The increased uptake and reliance on digital platforms by the private and public sectors increases the potential attack surface for malicious cyber actors, potentially increasing the likelihood and impact of a security breach.

Changes in technology

Technological acceleration represents a significant challenge for the GCSB and as new technologies emerge we must be able to react quickly. This includes the increasing use of Artificial Intelligence and satellite technology in our daily lives. These technologies can have significant benefits, improving the lives of New Zealanders, and contributing to the economy. The GCSB plays a role in ensuring they do not pose risks to New Zealand's security and wellbeing.

Digital transformation continues to evolve internationally, with ever more devices connected to the internet, and organisations increasingly reliant on technology for everyday activities.

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

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

Large-scale public breaches of personal information have promoted the issue of data privacy amongst the public consciousness, and developing technologies continue to increase the attack surface available to cyber actors.

Encryption

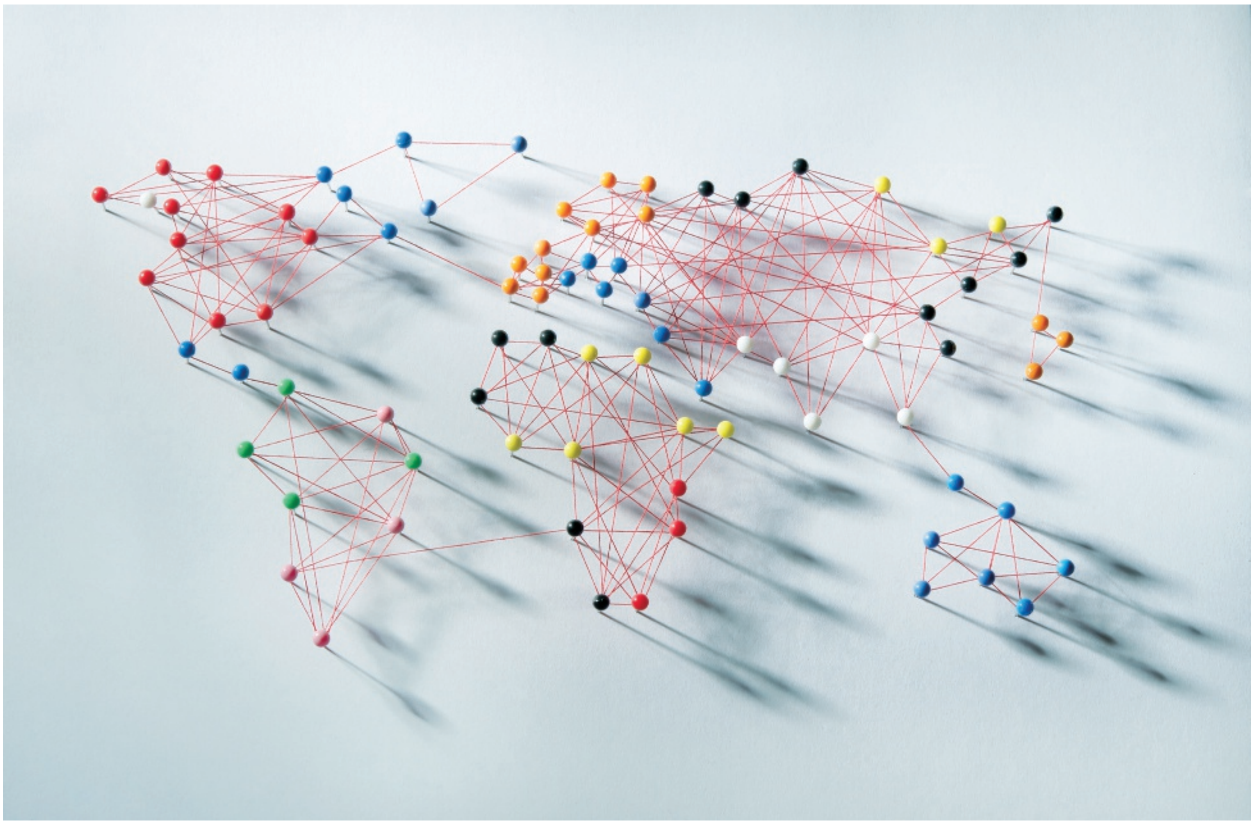
Encryption is the process of encoding data so that it can only be read by the intended audience. Encryption is a fundamental element of good information security, which is increasingly critical to New Zealand's national security and economic prosperity. The GCSB supports New Zealand's use of encryption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

Encryption can, however, be an impediment to law enforcement and intelligence and security agencies, as it can be used to protect unlawful activity such as terrorism or organised crime. Developments in encryption technology and improved security challenges continue to present new and unique challenges to the GCSB's lawful intelligence collection activities.

Regional security and geostrategic competition

The security of the South Pacific is a continuing focus area for New Zealand. As competition between states increases, so do the efforts of those states to project influence and power into the Pacific region. These actions have the potential to impact New Zealand's national and regional security.

The GCSB continues to support the National Security Intelligence Priority 'Pacific Regional Security' by ensuring that the intelligence products provided to customers meet their needs. Key customers in this area of work are the Ministry of Foreign Affairs and Trade (MFAT) and the Department of the Prime Minister and Cabinet (DPMC).



Counter-terrorism

The threat of harm from all types of violent extremism continues to be a security issue both internationally and for New Zealand. The GCSB's primary focus is to contribute to global efforts to counter violent extremism in its various forms. Throughout 2020/21 the GCSB has continued to make unique contributions to the global counter-terrorism effort, including contributing to the disruption of terrorist attack planning.

The spread of extremist content and ideologies online remains a threat to New Zealand's safety and security. The GCSB's role in domestic counter-terrorism is more limited in that we provide technical expertise and intelligence to support other agencies. The GCSB has continued to support the work of partners in countering domestic violent extremism.

Foreign Interference

All states engage in foreign influence activity in seeking to shape perceptions and decision making in another country. This activity becomes foreign interference when it is purposely misleading, deceptive, covert or clandestine.

Foreign interference is a growing threat globally and domestically, with potentially wide-ranging impacts on New Zealand's economic wellbeing and democratic norms and values. The scale and aggressive nature of this activity is on the rise around the world.

WARRANTS AND AUTHORISATIONS

Intelligence and Security Act 2017

Under the Intelligence and Security Act 2017 (ISA), the GCSB's warranted operational activity is covered by two types of intelligence warrants. A Type 1 warrant is issued for the purpose of collecting information about or to do any other thing directly in relation to New Zealanders. A Type 2 warrant is for activities done for other purposes. In each case, warrants may only be issued if the activities authorised by the warrant:

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

A total of 47 intelligence warrants were applied for and approved in 2020/21, of which 20 were Type 1 intelligence warrants and 27 were Type 2 intelligence warrants. No warrant applications were declined.

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

No applications for a joint intelligence warrant with the NZSIS were made under section 56. Joint intelligence warrants authorise the Directors-General of the GCSB and NZSIS to carry out the activities authorised by the warrant, and to exercise all of the powers of either agency to give effect to the warrant. While no occasion arose where the GCSB and NZSIS considered it necessary to seek such authority, the GCSB and NZSIS closely co-operate on operational matters.

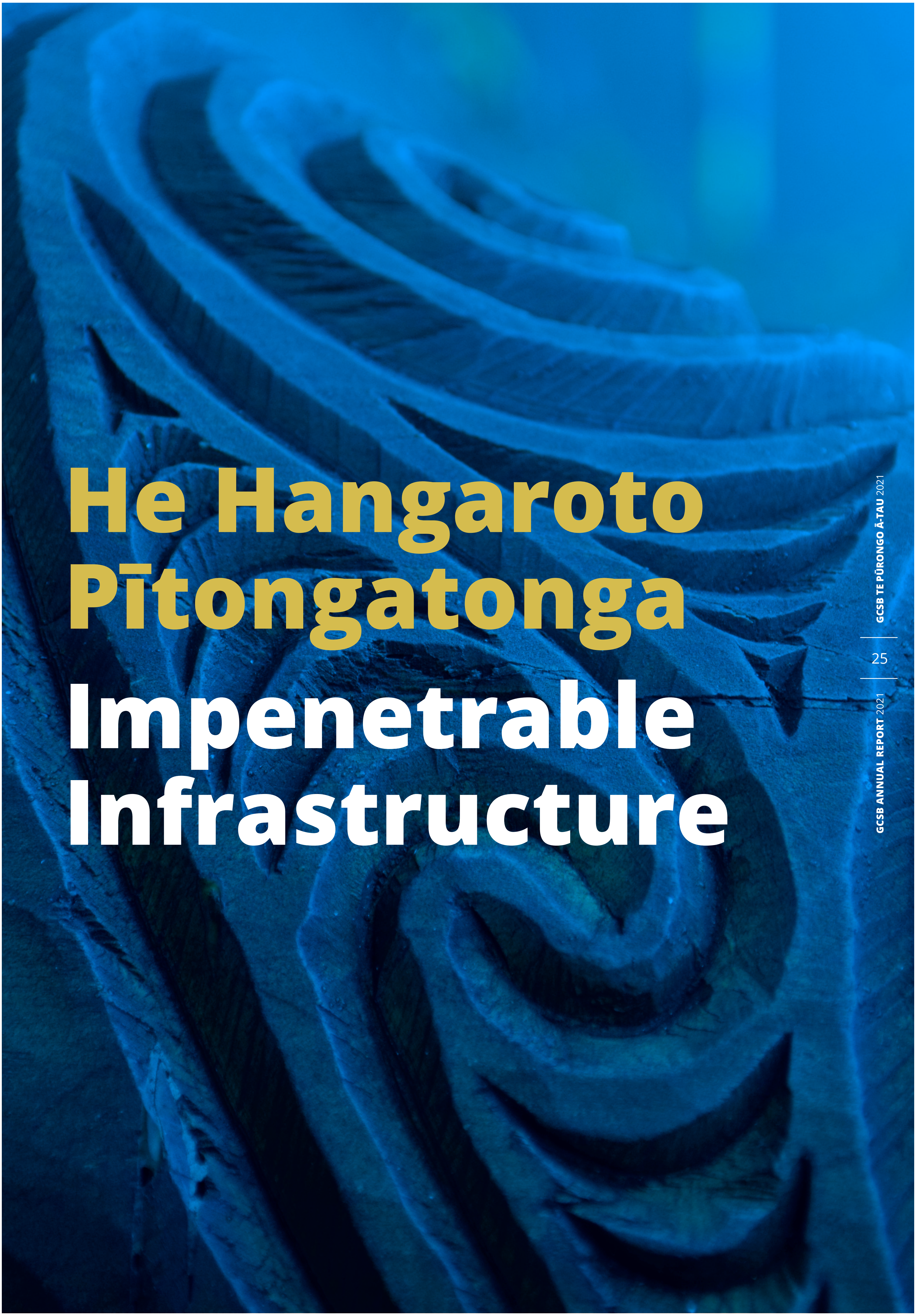
There were no occasions on which the GCSB provided assistance under section 14.

One very urgent authorisation was 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. It is automatically revoked 24 hours after the authorisation is given. In accordance with section 79, the GCSB made an application to the Chief Commissioner of Intelligence Warrants and the Minister for a Type 1 intelligence warrant, which was approved. In this case the very urgent warrant was in support of a Police operation.

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

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

The GCSB did not provide any advice and assistance to the New Zealand Defence Force or the New Zealand Police for the purpose of exercising those agencies' functions under section 13(1)(b). However, the GCSB co-operated with both agencies on a wide range of matters as part of performing the GCSB's intelligence collection and analysis and protective security services, advice, and assistance (including information assurance and cyber security activities) functions.



He Hangaroto Pītongatonga

Impenetrable Infrastructure

STRATEGIC FOCUS

Our Information Assurance and Cyber Security Directorate (IACD) has completed a strategic review to ensure it is best placed to address the increasingly complex security environment.

The review enabled a realignment of functions to absorb new responsibilities, refocus support to nationally significant organisations and achieve the directorate's strategic purpose to 'create a safer digital world for New Zealand to prosper'.

The IACD strategy established five objectives for the directorate's work over the next three years to 2024. These are:

- Defend national security,
- Raise cyber resilience,
- Support economic recovery,
- Facilitate digital transformation, and
- Improve New Zealand's wellbeing

The directorate provides an array of specialised services to support these objectives, fulfilling functions to detect, disrupt, advise and deter.

Who we work with

Throughout 2020/21 IACD partnered with government agencies such as the Ministry of Business, Innovation and Employment and the Department of Internal Affairs on cross-government projects on digital transformation.

The IACD also works with the Department of the Prime Minister and Cabinet (DPMC) and the Ministry of Foreign Affairs and Trade (MFAT) to support the Government's decision to call out malicious cyber activity. The IACD's role in this process is to conduct detailed technical investigations of malicious cyber activity, and where possible, attribute that activity to a specific actor.

The IACD also works with a range of customers, including organisations of national significance, key economic generators, niche exporters and research institutions to counter cyber threats.

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

The varying nature and impact of cyber incidents means the NCSC, New Zealand's Computer Emergency Response Team (CERT NZ), and the New Zealand Police work to ensure the New Zealand Government's response to cyber events is effective and comprehensive.

The Police are responsible for responding to crimes occurring online and CERT NZ works to support businesses, organisations and individuals who are affected by cyber security incidents. The NCSC responds to cyber incidents involving organisations of national significance or where the security and/or economic prosperity of New Zealand may be impacted.

SUPPORT TO MAJOR EVENTS

Throughout 2020/21 the GCSB contributed to several major events. These events provide opportunities to proactively provide advice, assessments and other services to the entities involved.

General Election 2020

In 2020 the GCSB, along with the NZSIS, provided a range of support for the General Election and referendums, including as part of a multi-agency effort led by the Electoral Commission.

Part of this work included updating principles and protocols for the GCSB and the NZSIS in managing foreign interference and cyber security threats to the 2020 General Election. These protocols helped to establish a threshold for escalating incidents for a broader national security system response. The principles and protocols were not triggered.

In the lead up to the 2020 election the GCSB, through the IACD, engaged directly with the Electoral Commission to provide cyber security advice and support to reinforce their cyber security resilience.

APEC 2021

The GCSB, through the IACD, has provided ongoing support to the Ministry of Foreign Affairs and Trade's hosting of APEC21. This has included the provision of cyber security advice and guidance for delivery of the APEC21 virtual meetings.

COVID-19 Immunisation Programme

The GCSB worked closely with the Ministry of Health on the development of the COVID-19 scanning app, and continues to support the immunisation programme.

CYBER SECURITY

Improving cyber security is a key for New Zealand to thrive in the digital age. As New Zealanders become more reliant on technologies and more connected to the world, we face a greater number of technological vulnerabilities.

The GCSB's NCSC plays a vital role in protecting government agencies and nationally significant institutions from cyber threats that have the potential to affect New Zealand's national security and the economy. The NCSC does this by detecting and disrupting cyber threats, providing cyber threat analysis to customers and partners and issuing cyber security advice. It is our mission to ensure that New Zealand's most important information infrastructures are impenetrable to technology-borne compromise.

Without fit-for-purpose cyber security, New Zealand will be unable to protect its intellectual property, maintain its reputation as a stable and secure place to do business, and ensure governmental and democratic processes remain free from interference.

The NCSC operates a suite of cyber defence capabilities and provides incident response support to help nationally significant organisations address potentially high impact cyber events.

The NCSC's incident response capabilities include coordination, communication, forensics, detection, disruption and intelligence.

Cyber Security Incident Response

Throughout the 2020/21 year the NCSC has responded to several high profile cyber security incidents, including Distributed Denial of Service (DDoS) and Ransomware attacks.

The DDoS attack on the New Zealand Stock Exchange (NZX) and other organisations, particularly the financial sector, is an example of the increasing sophistication and capability of criminal actors. The NCSC response to this incident highlighted our effective working relationships with internet service providers, who played a significant role in response to the DDoS attack.

The Waikato District Health Board (DHB) was the target of a ransomware attack in 2021. This attack had significant impact on the DHB and the GCSB worked with domestic partners to support the response.

The NCSC also responded to activity against the Reserve Bank, involving a vulnerability in Accellion, a type of file transfer software. This vulnerability was effectively unknown to security experts at the time malicious actors exploited it. There are many examples of the creation and exploitation of vulnerabilities in widely used systems and hardware. This has been an area of focus for the NCSC over the 2020/21 year and will continue to be a focus in the coming months.

In 2020/21 the NCSC and Computer Emergency Response Team (CERT NZ) engaged with international cyber security partners on the SolarWinds compromise. This compromise is an example of malicious actors shifting to establish more strategic access to systems through the compromise of critical supply chains. The SolarWinds Orion attack involved compromising a legitimate security update prior to it being distributed by the software provider.

While a significant number of New Zealand organisations downloaded the trojanised software update containing the malicious code, the NCSC did not see evidence of it being exploited here.

The GCSB, through the NCSC, continues to work with New Zealand's nationally significant organisations to build cyber resilience and respond to incidents. This includes supporting organisations to ensure cyber security systems are in place. Mitigating the risk, and impact of incidents, relies on organisations investing in and governing cyber security.

CORTEX

Our cyber defence capabilities developed as part of the CORTEX initiative continue to be a key tool to support nationally significant organisations to protect their networks from malicious, advanced, persistent, and sophisticated cyber security threats.

Analysis undertaken by the GCSB shows that in 2020/21, the operation of our cyber defence capabilities has prevented $119 million in harm to New Zealand's nationally significant organisations. This means that, over the last six years, these capabilities have reduced harm from hostile cyber activity by around $284.2 million.

The NCSC has continued to use its cyber defence capabilities to identify vulnerabilities being exploited by malicious cyber actors. In cases where known vulnerabilities are being exploited, the NCSC was able to provide mitigation advice directly to affected customers and potentially affected organisations, or as security advisories on the NCSC website.

In the past year, the NCSC has continued work to improve the use of CORTEX data and tools to more effectively defend New Zealand's organisations of national significance.

The NCSC has adopted a continual service-improvement approach to help mitigate risks associated with customers' evolving use of technology.

Malware-Free Networks

Malware Free Networks (MFN) provides a cyber threat intelligence feed that enables the GCSB to significantly scale our cyber defence efforts across a broad range of New Zealand organisations.

(U)Through MFN, the GCSB's NCSC partners with network operators and cyber security service providers to detect and disrupt threats to nationally significant organisations.

MFN delivers an active disruption capability that is scalable, through the provision of a threat intelligence feed that can be consumed by organisations either directly, via a cyber security service provider, or through their internet service provider.

The MFN threat intelligence feed contains indicators of malicious activity generated from a range of sources including the operation of our CORTEX capabilities and specialist information from domestic and international partnerships.

Throughout the 2020/2021 reporting year, the NCSC has worked with a range of network operators and commercial security service providers to expand the range of organisations able to be protected by the MFN threat intelligence feed. This new capability went live in June 2021.

Customer Engagements

The NCSC works with more than 250 of New Zealand's nationally significant organisations (NSOs) to understand their cyber resilience and vulnerability to attack, providing advice, support and cyber threat alerts to help organisations lift their overall cyber security resilience.

During the reporting period, the NCSC recorded 1872 engagements with customers across the broad spectrum of public and private sector organisations, geographically disbursed across all regions.

The NCSC also facilitates security information exchanges (SIEs) where participants can share information in a confidential and trusted environment. The SIEs are organised on a sector-by-sector basis, and membership is restricted to nationally significant organisations. We currently support the operation of sector-based security information exchanges covering the energy, finance, government, network, transport and logistics, and university sectors. The SIEs generally meet

quarterly to share information on cyber security risk management and resilience building. As these exchanges mature, the participants are focusing more on the uplift of their specific sectors as opposed to just their own organisations. Two more SIEs are currently in the planning phase.

In the 2020/21 reporting period, the NCSC facilitated 22 security information exchanges, which enhanced collaboration on cyber security challenges and opportunities across all sectors.

The NCSC also published 47 reports for specific NSO customers, and some for general consumption via the NCSC website. These identify specific cyber security vulnerabilities, providing cyber threat mitigation advice and reinforcing cyber security best practice to assist raise overall cyber security resilience.

Cyber Resilience Campaigns

In 2017/18, the NCSC gathered data from 250 NSOs and produced the NCSC Cyber Security Resilience Assessment, which identified four areas of good practice where organisations can focus their efforts for the greatest effect. The key areas we identified were: governance, incident management, investment, and supply chain security. Over the past few years we have developed resources to help organisations increase their cyber resilience in these areas.

In 2020/21, two more campaigns in this series of resources were released to help organisations address the focus areas published in the original report. The campaigns focused on incident management and supply chain cyber security. The steps outlined in both these campaigns define the principles for building resilience and help to focus engagement between senior leadership and security practitioners.

INFORMATION ASSURANCE

One of the GCSB's key functions is to provide protective security advice and information assurance services to the New Zealand Government. This includes providing technical expertise, specialised technology and regulatory oversight to protect New Zealand's most important information and infrastructures. It also protects the Government's most sensitive information.

Government Chief Information Security Officer

Through the Director-General's role as Government Chief Information Security Officer (GCISO), the GCSB takes a functional leadership role in protecting New Zealand's digital interests.

As government agencies take advantage of the opportunities presented by changes in technology, increased remote working and video conferencing, the associated risks also need to be managed. Working closely with other digital functional leads, the Government Chief Digital Officer, and the Government Chief Data Steward, the GCISO supports the secure digital transformation of the public service.

The GCSB's approach in supporting the GCISO is both strategic and practical and seeks to identify systemic risks and to strengthen assurance.

In 2020/21, the GCISO contributed to the All-of-Government Cloud Programme. This programme saw the GCISO working in partnership with major cloud service providers (Microsoft and Amazon) to develop baseline security templates for their cloud services. These templates are based on the New Zealand Information Security Manual controls. This will enable any public sector organisation to adopt cloud technologies securely and safely.

The GCSB continues to support improved information security across the public service as a whole. This includes research and policy development to address strategic risks associated with adoption of new technologies across Government and release of significant updates to the New Zealand Information Security Manual (version 3.4).

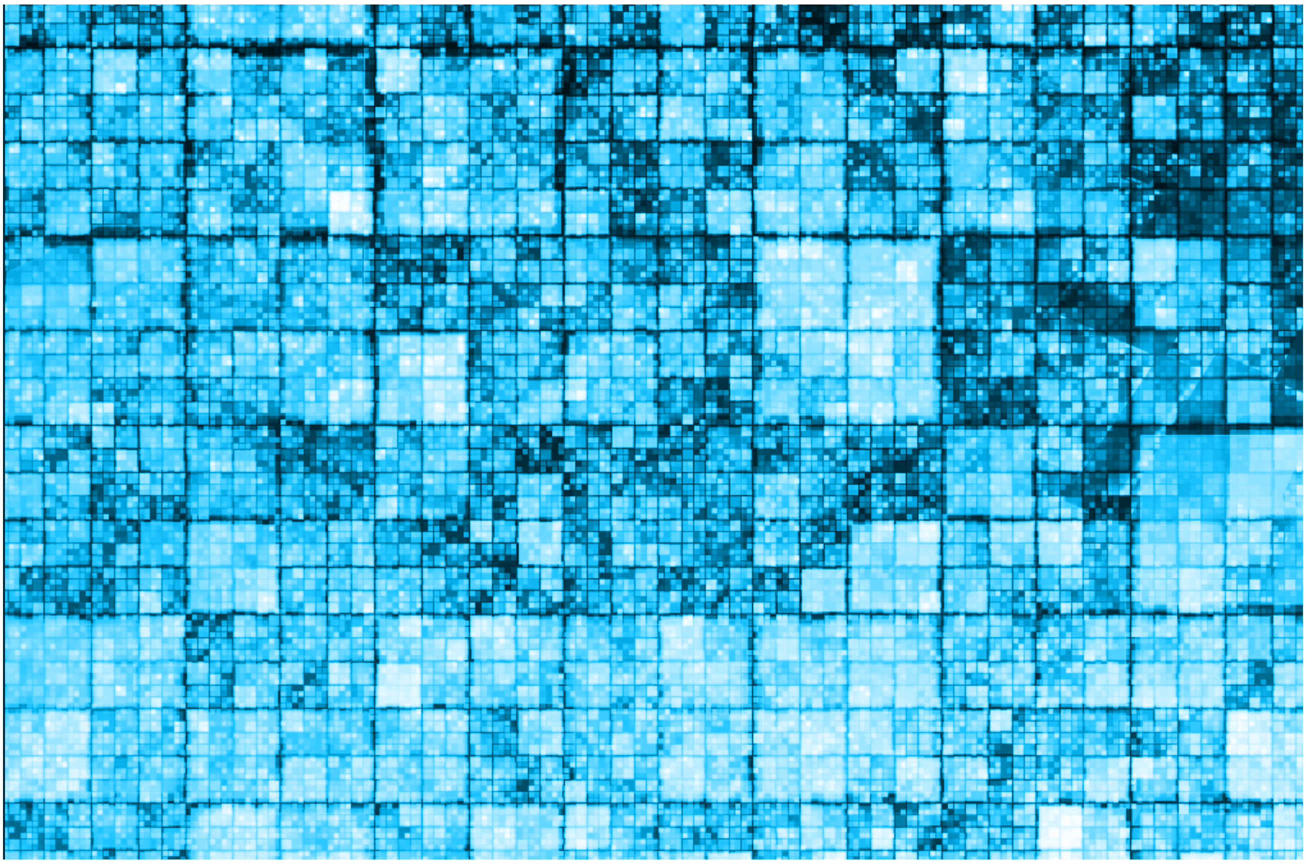
High Assurance Services

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

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

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

HAS provides a number of services to government, including technical surveillance counter-measure inspections, emanations testing and inspections, as well as advice on the standards required for SCI site and system accreditation. The GCSB provides technical inspection services and advice, and seeks to ensure that these facilities are free from vulnerabilities that would allow unauthorised access to information. The HAS team also has a mobile capability to inspect existing facilities for signs of technological efforts to compromise security.



Regulatory functions

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

Telecommunications (Interception Capability and Security) Act 2013

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

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

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

In the 2020/21 reporting period, the GCSB received 141 notifications, comparable to the 145 notifications in 2019/20. Many of these involved changes related to the rollout of 5G or full-fibre networks.

Outer Space and High-altitude Activities Act 2017

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

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

During the 2020/21 reporting period, the GCSB conducted 29 assessments of regulated space activities, down from 31 in the last reporting period.

Overseas Investment (Urgent Measures) Amendment Act 2020

The Overseas Investment (Urgent Measures) Amendment Act 2020 (OIAA), which came into force on 16 June 2020, made changes to the Overseas Investment Act 2005. The amended Overseas Investment Act includes a national interest test and a new emergency notification regime to manage risks associated with overseas investments that are contrary to New Zealand's national interest (including national security). The emergency notification regime is a temporary measure to address risks associated with overseas investment while the New Zealand economy is affected by and recovering from COVID-19.

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

During the 2020/21 reporting period, the GCSB conducted 69 assessments under the emergency notification regime.

The IACD also responded to a number of ad hoc requests for technical security assessments throughout the 2020/21 year.

SECURE TECHNOLOGY

The GCSB delivers secure information technology for the NZIC, and the wider national security sector. This role is vital as this sector handles some of the Government's most sensitive information. It requires specialist technology, expertise and ongoing effort to ensure the information remains protected.

The GCSB is New Zealand's national authority on communications security. As part of this role the GCSB provides the technology, processes and key material used to protect the country's most sensitive information.

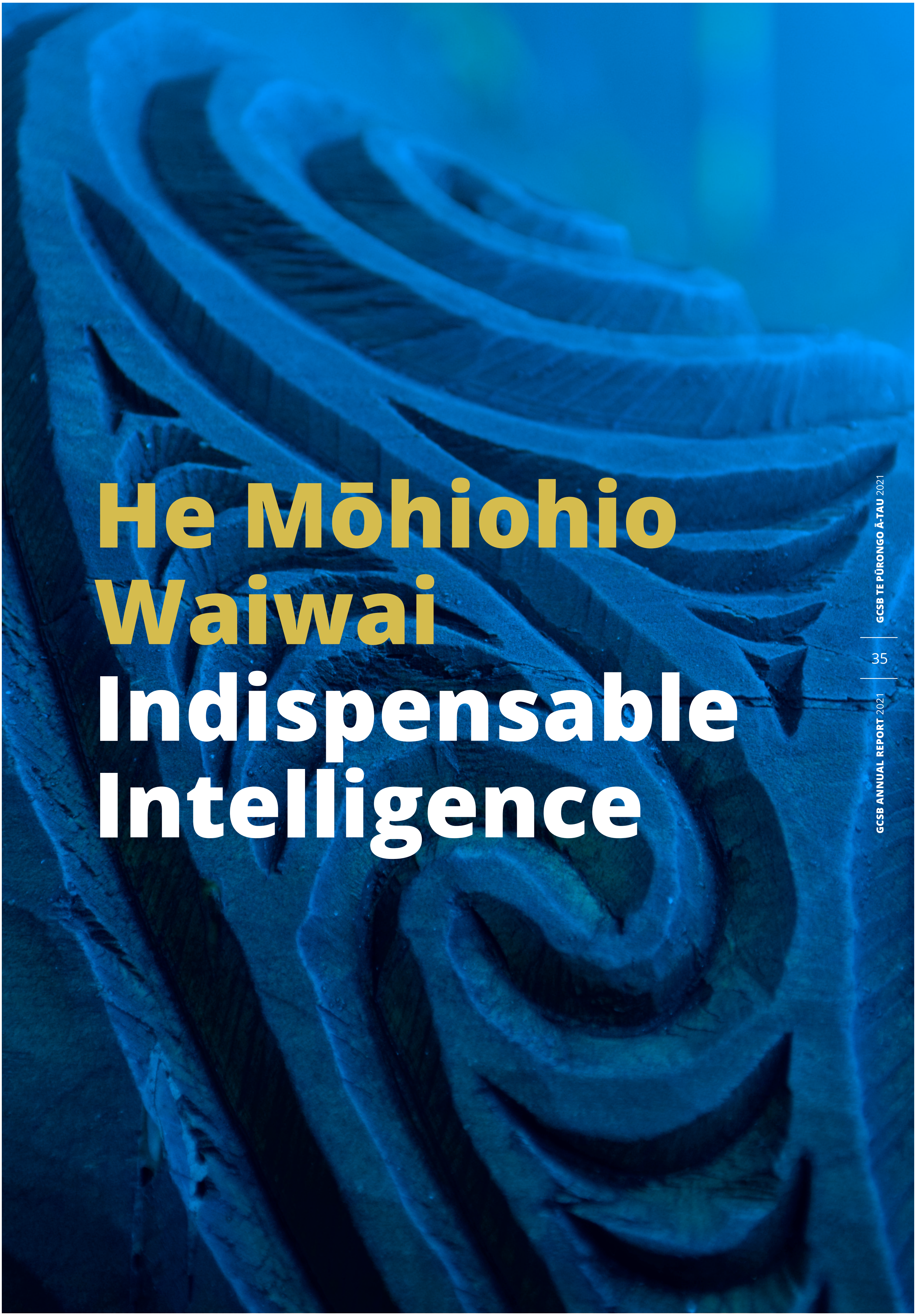
The GCSB has several significant projects underway in this area.

High-Grade Cryptographic Infrastructure

The reporting year has seen the achievement of a major milestone for the provision of the high-grade cryptographic product which is used to protect New Zealand's most sensitive communications. This was the completion of the multi-year project to upgrade our cryptographic product management infrastructure (CPMI). The CPMI system supports the Keying Management Infrastructure for New Zealand communications security (COMSEC), accounting for key production and dissemination used to protect the New Zealand Government's highly classified communications.

New Zealand Top Secret Network (NZTSN)

The New Zealand Top Secret Network (NZTSN) is a GCSB-led programme to deliver a set of technology capabilities for New Zealand's national security sector.



He Mōhiohio Waiwai

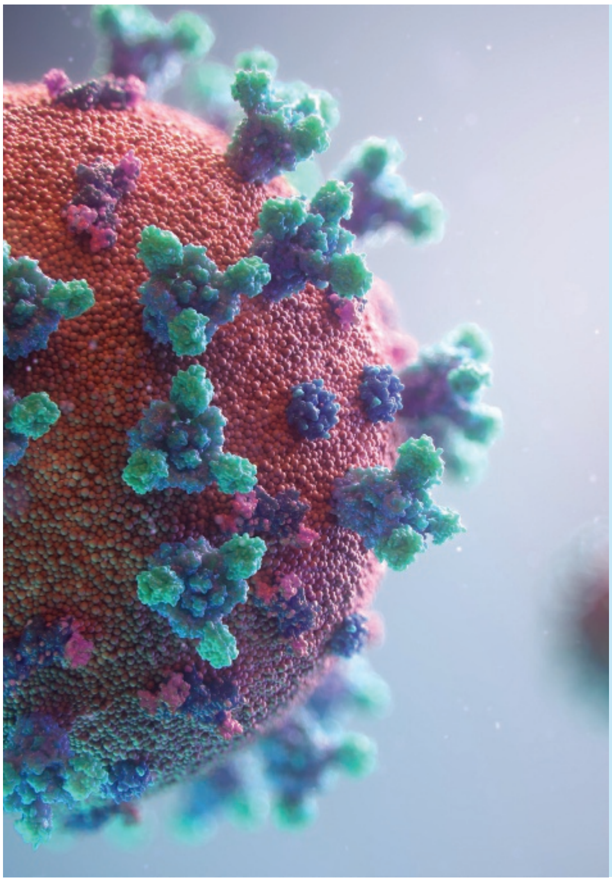
Indispensable Intelligence

INTELLIGENCE COLLECTION

The GCSB primarily collects signals intelligence, or SIGINT. This means that the GCSB collects and analyses electronic communications to produce intelligence. Through its role in collecting and analysing intelligence, the GCSB contributes to the protection of New Zealand's national security, international relationships, economic wellbeing, and the safety and security of New Zealanders.

The GCSB collects and analyses intelligence in accordance with the policy and priorities set by the New Zealand Government. The GCSB may provide intelligence to the Minister Responsible for the GCSB, the Chief Executive of the DPMC, and any person or class of person the Minister authorises to receive it. This includes other government agencies and international partners.

Throughout 2020/21 the GCSB continued to supply intelligence to various government agencies, Ministers and decision makers, across all of the National Security Intelligence Priorities. This intelligence was obtained through the GCSB's own capabilities, and from international partner agencies. The provision of this intelligence is one way that the GCSB contributes to the safety and security of New Zealand and our interests.



COVID-19

In the 2020/21 period, the GCSB has continued to provide a significant amount of intelligence to New Zealand Government customers in relation to New Zealand's response and recovery from the COVID-19 pandemic.

Throughout lockdowns the GCSB continued to deliver critical intelligence relating to the pandemic and other national security matters; and maintained its 24/7 watch and warn service.

REGIONAL SECURITY AND GEOSTRATEGIC COMPETITION

Security and resilience in the Pacific region has long been an important area of focus for New Zealand. The Pacific is increasingly becoming an area of strategic competition for great powers, with various states seeking to project influence and power into the region. This competition has the potential to have a detrimental effect on regional security.

Alongside the increase in strategic competition, transnational organised crime affects the security of the Pacific, and can easily spread to the surrounding region, including New Zealand.

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

COUNTER-TERRORISM

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

Throughout 2020/21 the GCSB has continued this role, supporting counter-terrorism efforts globally.

The GCSB's role in domestic counter-terrorism is to assist the NZSIS and Police in their investigations. This assistance is primarily the provision of technical capabilities and intelligence.

Domestically, the GCSB has continued to respond to recommendations made by the Royal Commission of Inquiry into the terrorist attacks on Christchurch masjidain and has worked closely with both NZSIS and Police partners on a number of domestic terrorism related investigations.

TRANSNATIONAL ORGANISED CRIME

Contributing to the protection of New Zealand's national security and wellbeing and supporting the safety and security of New Zealanders at home and abroad, are key objectives of the GCSB.

One way of achieving these objectives is by supporting other government agencies, through provision of relevant intelligence, so they can carry out their work.

The GCSB responds to requests for intelligence from, and provides technical assistance to, the NZSIS and New Zealand Police. The GCSB has contributed to development of the Police-led Transnational Organised Crime Strategy and has worked closely with New Zealand Customs Service (Customs) throughout 2020/21 to contribute to the prevention and detection of transnational organised crime. Our focus is on providing intelligence leads that will assist Customs to prevent large scale drug importation.

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

SUPPORTING NEW ZEALAND DEFENCE FORCE

In 2020/21 the GCSB continued to provide support to the New Zealand Defence Force (NZDF) for the purposes of its operations. The GCSB contributes to NZDF efforts to detect and counter threats to New Zealand military personnel deployed overseas.

CUSTOMER ENGAGEMENT

In 2020/21, the NZIC established the joint Intelligence Customer Centre (ICC). The purpose of the ICC is to engage and lead the provision of products and services to customers on behalf of the GCSB, DPMC (NAB) and NZSIS. The ICC creates an integrated 'one-stop-shop' for intelligence products and services from our three agencies. This means more coordination between the agencies and more capacity for us to tailor to customer needs. The ICC is currently in the establishment phase, is in the process of building the core team of 12 and developing underpinning processes and ways of working. The ICC will grow in capacity over time, subject to future funding.

INTERNATIONAL PARTNERSHIPS

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

Any cooperation and intelligence sharing with international partners is subject to New Zealand's laws, including human rights obligations, and to the laws of partner countries that share information or other support with us.

Five Eyes

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

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

The Five Eyes partnership is fundamental to the GCSB's work to support New Zealand's national security and interests, and ensure the wellbeing of New Zealanders both at home and abroad. We could not deliver our current level of intelligence and security activity alone.

The Five Eyes partnership has been an instrumental part of New Zealand's intelligence and security activities since World War Two. The partnership began as a cryptographic venture to share efforts and results in code breaking (and code making) during the war. Following that work, a wider partnership was established, involving all aspects of security and intelligence, which continues today.

Other international partners

In addition to our Five Eyes partnership, the GCSB collaborates with a range of other nations. Cooperation extends to the sharing of intelligence, best practice, knowledge and expertise. These efforts are undertaken to help the states involved, including New Zealand, counter threats like hostile cyber activities, transnational organised crime and violent extremism.

COVID-19 impact on international partnerships

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

Our People

Ō Mātau Tāngata

OUR VALUES

Respect

We respect the role that each individual plays in the organisation. We value diversity in thought and approach. We treat each other with dignity.

Integrity

We act lawfully and ethically. We are accountable for our actions – both personally and organisationally. We act professionally and with respect.

Commitment

We are committed to our purpose. We are committed to excellence – recognising the contribution of our tradecraft to national security. We are committed to our customers – recognising that our success is measured in their terms. We are committed to our stakeholders – the government and people of New Zealand.

Courage

We face facts, tell it how it is and are prepared to test our assumptions. We have the courage to make the right decisions at the right time even in the face of adversity. We are prepared to try new things while managing the risk of failure. We perform at pace and are flexible and responsive to change.

LEADERSHIP

Director-General of the Government Communications Security Bureau

Andrew Hampton began his term as Director-General (formerly the Director) of the Government Communications Security Bureau (GCSB) in April 2016.

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

- Stewardship of the GCSB, including its medium and long-term sustainability, organisational health and capability, and capacity to offer free and frank advice to successive governments;
- Ensuring the performance of the functions and duties and the exercise of the powers of the Director-General of the GCSB;
- The tendering of free and frank advice to Ministers, as well as the integrity and conduct of the employees for whom the Director-General is responsible; and
- The efficient and economical delivery of the GCSB's services and the effective provision of those services, ensuring they contribute to intended outcomes.

In 2018 the Director-General became the Government Chief Information Security Officer, or GCISO.

The Director-General is accountable to the Minister Responsible for the GCSB.

Senior Leadership Team

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

The SLT meets regularly to focus on the GCSB's strategic direction, risk, opportunities, overall work programme, significant organisation-wide policies, major projects, departmental budget and workforce capability and capacity.

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

- Director, Strategy, Governance and Performance;
- Director, Intelligence;
- Director, Information Assurance and Cyber Security;
- Director, Technology;
- Chief Legal Adviser;
- Chief Financial Officer, Intelligence Community Shared Services; and
- Chief People Officer, Intelligence Community Shared Services.

The roles of Director Technology, Chief Financial Officer and Chief People Officer lead functions that are shared with the New Zealand Security Intelligence Service (NZSIS).

Leadership Development

Equipping and developing leaders as the organisation grows and evolves remains a priority. The NZIC leadership competency framework aligns with the Public Service Commission framework and the core competencies expected of leaders are included in all people managers' performance and development reviews.

Our newest Leadership Development programme, Te Ara o Tātāriki – The Path of Kākā/Leadership, launched in July 2020 with topics that include Leadership, Strategic Execution, Leading Change and Resilience, Teamwork and Collaboration, Decision Making in Complexity and Ambiguity. As the programme is implemented the content will be further refined based on participant feedback.

In total our leaders have access to over 15 centrally managed, core leadership development offerings. As at 30 June 2021 more than 70 per cent of our leaders have completed one or more of these core programmes.

RETAIN, DEVELOP AND RECRUIT THE BEST PEOPLE

The GCSB is a public service department with 543.9[1] full-time equivalent staff, as at 30 June 2021.

The GCSB is able to deliver on its mission to protect and enhance New Zealand's security and wellbeing because of the unique skills and innovation of our people.

Throughout 2020/21 the GCSB has continued its focus on retaining the existing workforce and providing opportunities for growth and development.

Recruiting the best people remained a priority throughout 2020/21. The GCSB employs people from a wide range of disciplines, including foreign language experts, communications and cryptography specialists, engineers, and technicians and support staff. Over the past year efforts have been focused on ensuring that recruitment resources reflect that we want a more diverse workforce.

In October 2020 we launched a recruitment campaign to raise awareness of who we are, the career opportunities available at the GCSB and NZSIS, and the benefits of working for us. One of the key drivers for the recruitment campaign was the findings of 2019 research, conducted by an external agency, into the perceptions of Māori, Pasifika, other ethnic groups, and women in New Zealand. This research found there was limited awareness of who we were. As a result we developed a recruitment campaign to better promote the work we do, the range of career opportunities available, and our strong focus on creating a diverse and inclusive work environment.

The recruitment campaign saw a significant increase in traffic to our Beyond Ordinary website, an increase in the number of applications for vacancies, and we successfully filled the majority of vacancies advertised throughout the campaign. As part of the campaign the GCSB and NZSIS also established our first social media presence with the Facebook page 'Beyond Ordinary'.

Alongside our October 2020 recruitment campaign, we have updated our job advertisements and Beyond Ordinary website to include more information about our work environment, how much we value diversity and inclusion, and our employment package offerings.

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

Staff Retention

Staff retention is critical for the GCSB, particularly given the unique and demanding environment staff operate in, and the time involved in recruiting, vetting and training suitable people.

In July we implemented a new Retention Strategy 2020-2024 that outlines the areas we need to focus on in order to attract, develop, and retain a workforce that is diverse, highly capable, and engaged. The strategy builds on existing initiatives and provides a holistic approach to retention at an organisational and directorate level. It told us where we were in 2020, where we aspire to be in 2024, and sets out a plan for how to get there.

U) The GCSB supports staff retention by providing learning and development opportunities and a clear view of career pathways where appropriate. We also recognise, reward, and retain our talented staff through our Long Service Recognition programme and the Exceptional Achievement Awards, which were established this year.

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

Overall we have seen a significant drop in turnover this year, with a 5.6 percent decrease from 2019/20. This reduction moved us under the wider public service rate. Turnover in previous years is attributed to the demand for our staff's skill set in both the public and private sector. We are attributing the lower turnover of staff to the impact of COVID-19.

TABLE 1: GCSB CORE UNPLANNED STAFF TURNOVER (2015 TO 2021)

	2015/16	2016/17	2017/18	2018/19	2019/20	2020/21
Staff Turnover	9.3%	6.9%	7.1%	12.0%	13.7%	8.1%
Public Service	11.1%	11.5%	12.1%	11.8%	10.1%	Figure not yet available

DIVERSITY IN THE WORKFORCE

To achieve our mission of keeping New Zealand safe we need people who can think differently, people with different skills and experiences, and people who embrace diversity of thought to solve the problems we face. This means we need people from a wide range of backgrounds.

When we launched our first Diversity and Inclusion (D&I) Strategy 2017-2020 with the NZSIS in March 2018, we focused on two priority areas – increasing representation of women, and ethnic diversity at all levels of our workforce.

Gender Diversity

At 30 June 2021 women made up half of the GCSB's senior management group. We have successfully met our diversity and inclusion aspiration of women forming not less than 50 per cent of our senior leadership group.

TABLE 2: THE GCSB'S GENDER REPRESENTATION (2015 TO 2021)

	2015/16	2016/17	2017/18	2018/19	2019/20	2020/21
Senior Management (Tier 2 and 3)						
Men	47.0%	40.0%	42.9%	48.0%	54.5%	**47.8%**
Women	53.0%	60.0%	57.1%	52.0%	45.5%	**52.2%**
All staff						
Men	63.1%	63.6%	62.4%	63.8%	64.4%	**64.5%**
Women	36.9%	36.4%	37.6%	36.2%	35.6%	**34.9%**
Another Gender	-	-	-	-	-	**0.2%**
Undisclosed	-	-	-	-	-	**0.4%**

This is the first year that we have had staff with undisclosed and other genders, and as such have included them into our reporting.

While it is encouraging to see gender diversity in the senior management group, we have yet to meet and exceed our target of 39.4 per cent representation of women across the workforce as a whole.

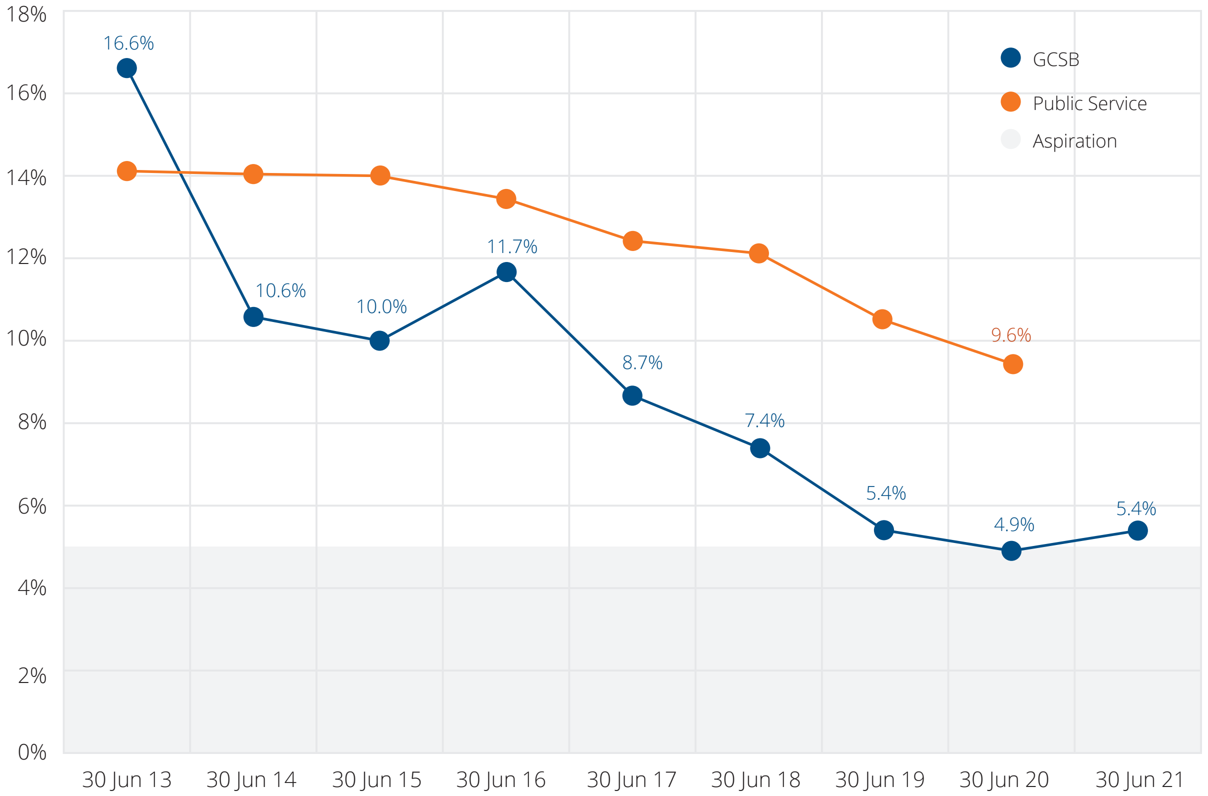
The GCSB has a range of initiatives in place to recruit women, and we are seeing encouraging trends such as appointing women at a higher percentage (39.7 per cent) than the total percentage of women applicants (33.9 per cent) in 2020/21.

Additionally, the GCSB is actively fostering external connections to support the development of technical capabilities our agency, and New Zealand, needs for the future. This includes initiatives such as our Women in STEM scholarship, graduate programme, and our 2021/22 Talent Outreach and Engagement Strategy, which are all key to our efforts in improving the representation of women in the GCSB.

Closing the Gender Pay Gap

Closing the gender pay gap has been a focus for the GCSB with a target of reducing the average gap to a maximum of five percent by 2021. At the end of the 2020/21 financial year, the gender pay gap in the GCSB was 5.4 percent. Despite this increasing by 0.5 per cent from last year, we remain close to our goal, and are significantly lower than the public service benchmark of 9.6 percent (at 30 June 2020).

Work to reduce the gender pay gap is being undertaken in collaboration with staff associations and network groups throughout the NZIC. The gender pay gap work feeds into the wider programme established by the Public Service Commission seeking to resolve the gender pay gap across the public service.



Gender Pay Gap Action Plan

Our Gender Pay Gap Action Plan incorporates four core milestones:

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

We have made, and continue to make, steady progress towards these goals. The GCSB has established a new Flexible Working Policy (and associated online training), and we continue to work on identifying and mitigating bias and discrimination in all practices.

Ethnic Diversity

The GCSB is working to improve the ethnic representation of its workforce, and has achieved improvement in some areas. In 2020/21 the GCSB continued to implement the Diversity and Inclusion strategy. The strategy ensures we have diverse talents, views and thinking, which is critical to achieve our mission. It will take time for new recruitment strategies to be reflected in workforce statistics; however the GCSB is committed to this work.

TABLE 3: THE GCSB'S STAFF ETHNICITY (2015 TO 2021)

	2015/16	2016/17	2017/18	2018/19	2019/20	2020/21
NZ European & European	69%	68.7%	67.6%	67.8%	71.2%	76.0%
New Zealander	N/A	N/A	27.5%	29.4%	26.8%	22.8%
New Zealand Māori	6.5%	7.2%	7.8%	7.2%	7.3%	7.2%
Asian	5.8%	5.4%	4.9%	5.4%	5.5%	7.2%
Pacific Peoples	1.6%	1.8%	2.8%	2.3%	1.6%	2.6%
MELAA	0.3%	0.3%	0.3%	0.9%	1.1%	1.2%
Other	–	–	–	–	–	0.2%

These metrics cover the number of employees who identify themselves as having a certain ethnicity. They are calculated by taking the number of people who identify as being a certain ethnic group, divided by the number who have provided an ethnic group. Metrics are taken 'as at 30 June' of the relevant year. This is the first year was have included 'other' ethnicity in our reporting, so we have updated our statistics to include this.

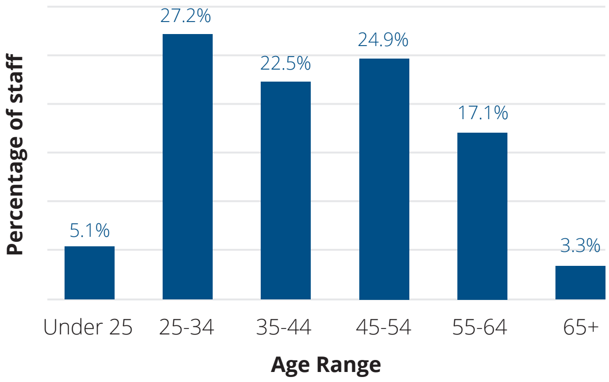
Diversity and inclusion embedded in our performance framework

To further cement our commitment to building a diverse and inclusive workplace the GCSB has introduced a new 'Community Contribution' performance objective for all staff. This objective encapsulates elements of diversity and inclusion, wellbeing, and other factors that contribute to a positive workplace culture. Embedding the new objective into our performance framework enables the GCSB to recognise the contribution individuals make to develop a diverse, inclusive, and healthy workplace culture.

Age Demographics

The majority of our workforce are between 25 and 54, which is reflective of our average tenure and age (6.4 years and 43). Of our staff under 35, 73 per cent have started in the last four years. As the age of our staff increases, so does our average tenure of these age groups. Most of our ethnically diverse staff are over the age of 45 (68 per cent).

AGE DEMOGRAPHICS AS AT 30 JUNE 2021



Progress against Public Service Commission Papa Pounamu Commitments

In October 2020 we established a formal programme of essential and recommended D&I learning for leaders and staff across the NZIC. The purpose of these activities is to support our people in developing the understanding and capabilities required to build and sustain a diverse and inclusive workplace. Key topics within this programme are outlined within the following sections.

Addressing bias

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

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

Our Understanding & Managing Unconscious Bias learning is now available online. 69 per cent of our leaders have either completed this learning in a face-to-face workshop or online. In alignment with increased emphasis on all staff contributing to our D&I objectives a December 2021 completion target has been established for those yet to complete this training.

In addition, online learning is being developed to support the requirement for hiring managers and panel members to undertake removing bias from recruitment practice training before serving on recruitment panels.

Cultural competence

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

In February a group of 20-30 volunteers from across the GCSB and NZSIS undertook a series of workshops to assess our current level of maturity against Te Arawhiti's Māori Crown Relations Framework. As a result, we have developed a programme of work to mature our capability over the next six years. While we already have some great work underway, we have chosen four dedicated priority areas for the next 12 months – leadership, cultural expertise, learning experiences and measures.

Inclusive leadership

The GCSB offers a range of leadership development opportunities targeted at helping our leaders recognise and mitigate bias, value diversity and foster inclusivity in the workplace. These include in-house learning activities, the range of Leadership Development Centre (LDC) programmes and other externally provided offerings.

Employee-led networks

We have established more staff networks to support the breadth of diversity across the workplace. At present we have eight networks. Each network is assigned their own budget, giving them the autonomy to drive their own initiatives. Staff networks contribute to, and deliver many initiatives including policy development, D&I events, internal celebrations, guest speakers, D&I training, networking functions, and conferences.

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

Rainbow inclusion

In early 2019 Standing Out @ the NZIC – our Rainbow network – was established. In July 2019 we were accredited with the Rainbow Tick.

We entered multiple categories at the 2020 Rainbow Excellence Awards. We were extremely proud when won the Partners Life Emerging Award, the Rainbow Tick Training and Development Award, and the overall Westpac Supreme Award. To win the Supreme award for LGBTTQIA+ staff shows we have made some great progress in creating a safe and inclusive workplace.

In 2020 we created a set of Transitioning Guidelines for staff and managers, and a brochure which captured key pieces of information. These resources have now been widely shared with a number of external organisations and have been used as a template by a number of workplaces throughout New Zealand.

GCSB Graduate Programme

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

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

For the 2020/21 graduate recruitment intake, the GCSB received 95 applications, of which 30 (32 per cent) were female and 39 (41 per cent) were ethnically diverse. Six offers were made to successful applicants – three (50 per cent) were female, two (33 per cent) were ethnically diverse, and one (17 per cent) identified as another gender.

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

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

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

Winners have come from a range of disciplines including cyber security, mathematics, physics, data science, computer science, and engineering. Since 2017 we have awarded 14 scholarships to women throughout New Zealand, and hosted four STEM Scholarship events in-house. The in-house event is an opportunity for the top scholarship finalists (10-12 students, including the winners) to learn more about the GCSB, and the wide range of STEM-related career opportunities we can offer.

This year we received a total of 126 applications from across all of New Zealand's universities. The calibre of applicants was extraordinary, and three scholarships were awarded. Two of our winners identify as New Zealand European and Māori, and the other identifies as New Zealand European.

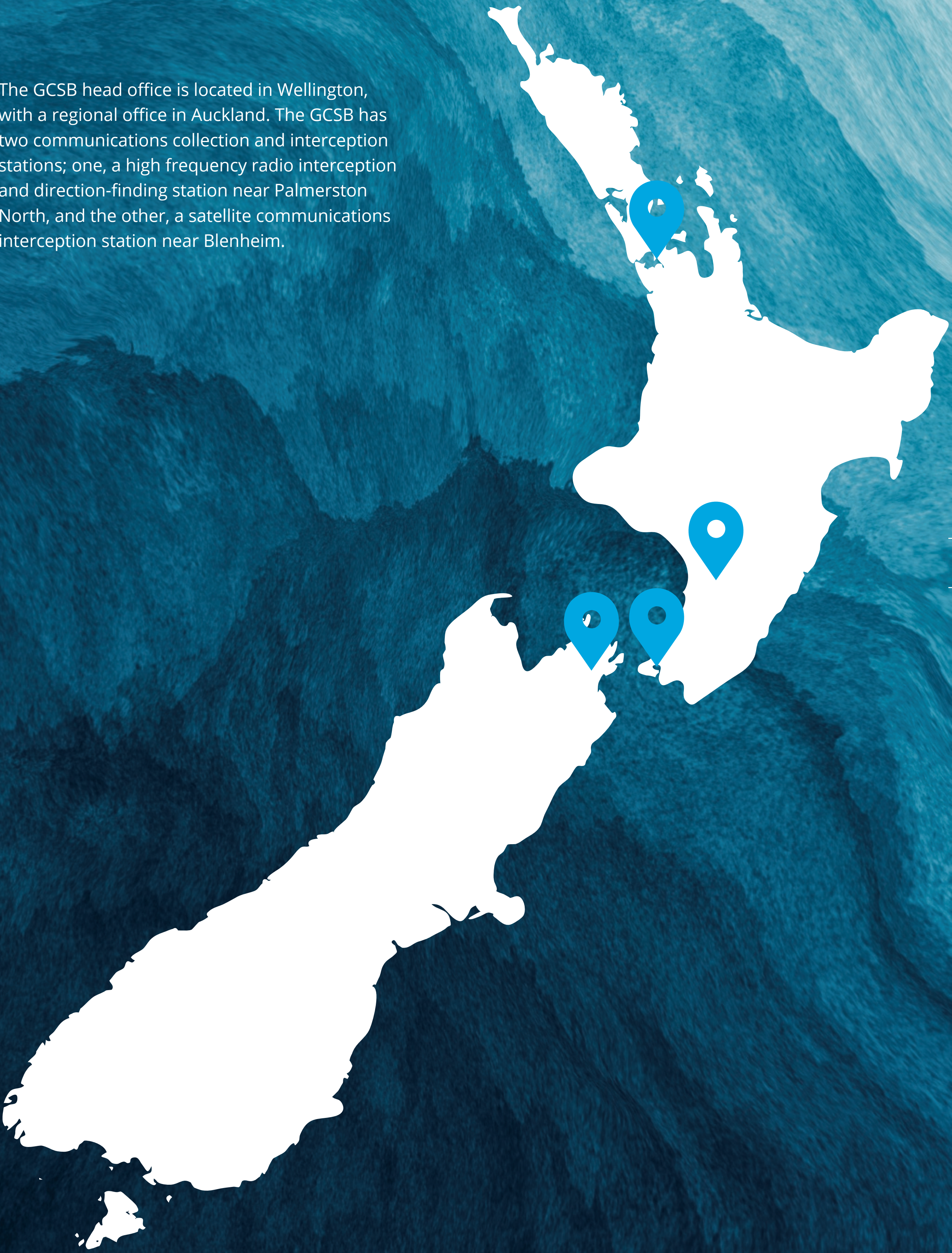
Talent Outreach and Engagement

Over the next year the GCSB will be implementing our Talent Outreach and Engagement strategy focused on connecting our community to a pipeline of potential talent with the capabilities critical to our mission, within demographics that are harder to recruit.

The Talent Outreach and Engagement strategy will include increasing promotion of our existing Graduate Programme, Women in STEM scholarship, and participating in the Department of Internal Affairs' Ethnic Community Graduate Programme.

LOCATIONS

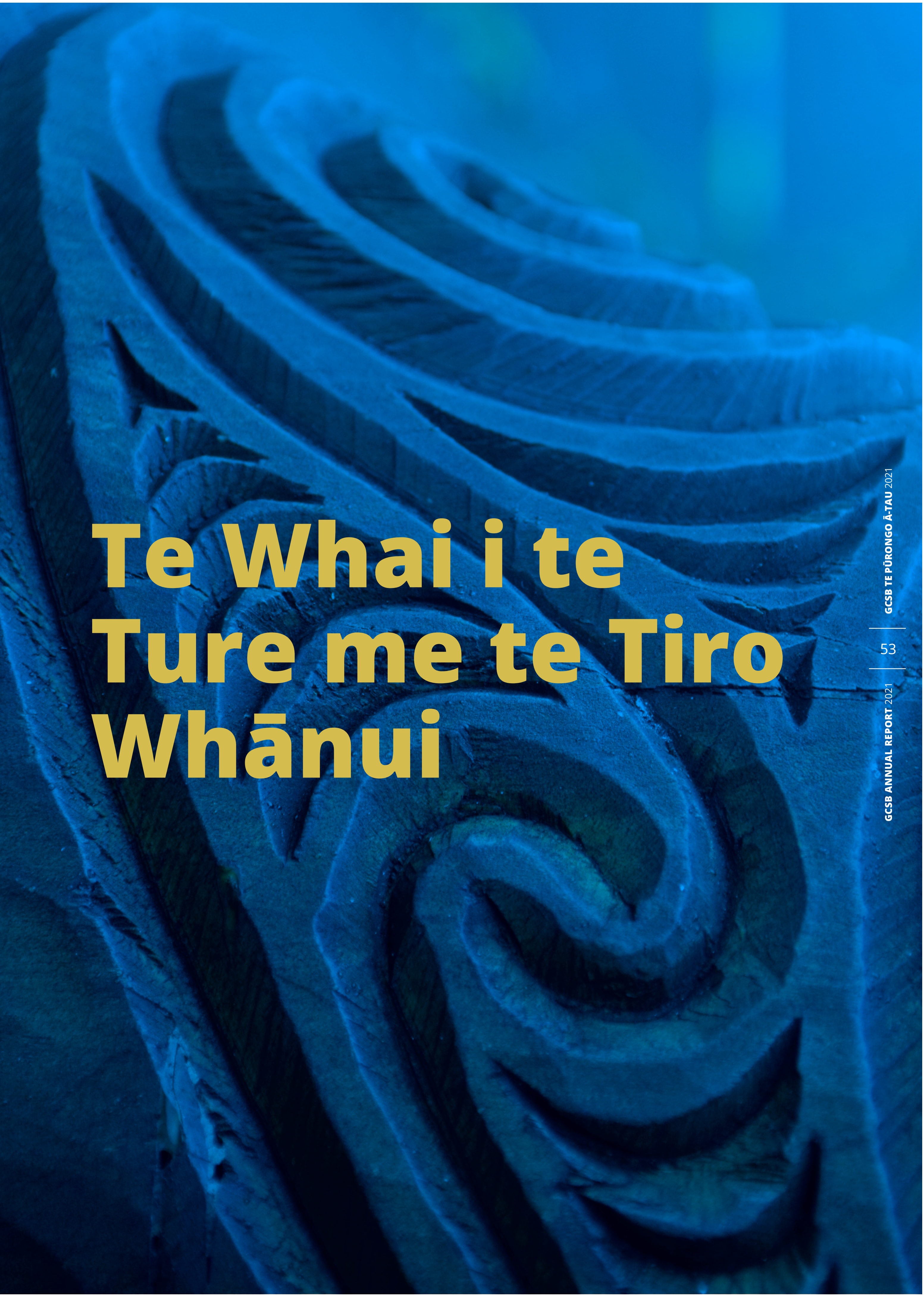
The GCSB head office is located in Wellington, with a regional office in Auckland. The GCSB has two communications collection and interception stations; one, a high frequency radio interception and direction-finding station near Palmerston North, and the other, a satellite communications interception station near Blenheim.



Legal Compliance and Oversight

Due to the nature of the GCSB's work, a significant amount of our activities are classified. This means that the agency is unable to talk about much of our work in public.

Oversight is of fundamental importance to the GCSB and is something that we value highly. Strong oversight, comprehensive legal frameworks and good governance all contribute to New Zealanders' trust and confidence in their intelligence agencies.



Te Whai i te Ture me te Tiro Whānui

The Intelligence and Security Act 2017

The Intelligence and Security Act 2017 (ISA) provides the legal framework for GCSB and NZSIS activities.

The ISA sets out objectives and functions of the GCSB and NZSIS, and provides the mechanism for the agencies to carry out otherwise unlawful activities. There are 11 Ministerial Policy Statements that set out Ministerial expectations and provide guidance for the agencies on how certain lawful activities should be conducted.

Compliance systems

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

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

Independent oversight

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

The Intelligence and Security Committee

The Intelligence and Security Committee (ISC) is the Parliamentary oversight committee for the GCSB and NZSIS. The ISC's role is to examine the policy, administration and expenditure of both agencies.

The ISC is currently made up of the Prime Minister, three Members of Parliament nominated by the Prime Minister, the Leader of the Opposition, and two Members of Parliament nominated by the Leader of the Opposition.

Office of the Inspector-General of Intelligence and Security

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

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

Review of GCSB and NZSIS activity and assessments under the Outer Space and High-Altitude Activities Act 2017.

In 2020/21 the IGIS undertook a baseline review of GCSB and NZSIS activities under the Outer Space and High Altitude-Activities Act (OSHAA) 2017. The purpose of a baseline review is to provide the IGIS with an understanding of a particular area of agency activity and, when appropriate, comment on issues identified in agency policy and procedure.

The review sought to improve the IGIS's understanding of the agencies' role under OSHAA, the way the agencies' conduct assessments/provide advice to the Minister and to better understand the agencies' internal compliance system in relation to these regulatory activities.

The review found that the compliance systems within the GCSB and NZSIS that apply to our activities under OSHAA are generally well developed. The report made recommendations on how policy and procedure can be further strengthened. The GCSB and NZSIS are working through how those recommendations could be implemented throughout 2021/22.

Royal Commission of Inquiry into the terrorist attacks on Christchurch masjidain

In December 2020 the Royal Commission of Inquiry into the terrorist attacks on Christchurch masjidain report was released.

While the report made no specific recommendations in relation to the GCSB it did fairly reflect our role. The report also noted that the GCSB should play a more active role in domestic counter terrorism and suggested we take a more proactive approach to better understand customer requirements and how our capabilities can complement their work.

The report also observed that other agencies within the counter terrorism system did not always have sufficient understanding of the GCSB's capabilities to know how to maximise its contribution. We are committed to making our role and capabilities more widely understood and utilised. Work in this space is already underway.

The Justice Select Committee Inquiry into 2020 General Election and Referendums

In May 2021, the Directors-General of the GCSB and NZSIS appeared before the Justice Select Committee inquiry into the 2020 General Election and Referendums. The two agencies were invited to appear before the inquiry to answer questions pertaining to decision-making about security investigations into New Zealand citizens, and mechanisms to address foreign interference risks.

The GCSB continues to work with the Justice Committee, Ministers, Members of Parliament and the Electoral Commission to mitigate foreign interference risks to the next General Election.

Official Information and Privacy Act Requests

The GCSB is subject to the Official Information Act 1982 (OIA) and the Privacy Act 2020 (previously the Privacy Act 1993). In responding to requests for information under these Acts, the organisation aims to be as transparent as possible. Each request is assessed on a case-by-case basis, and national security concerns are considered against the public interest using the guiding statutory principles.

For the period from 1 July 2020 to 30 June 2021, the GCSB:

- Completed 49 OIA requests, with two requests not completed within the legislated timeframe; and
- Completed 27 Privacy Act requests within the legislated timeframe.

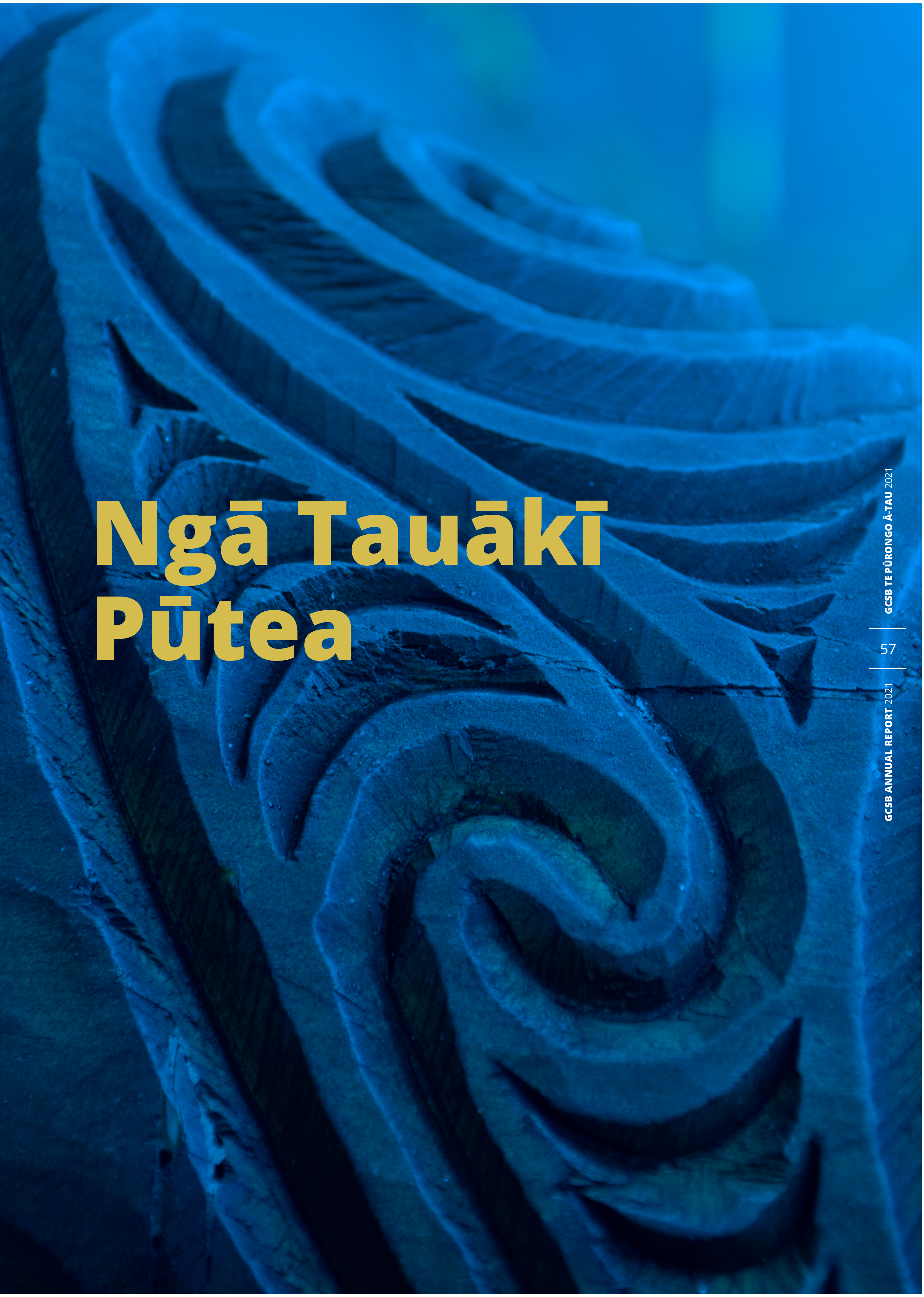
The GCSB aims to complete all information requests within the legislated timeframe. Administrative errors caused delays to two OIA requests in the reporting period. Processes have been improved to prevent this happening in the future.

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

One complaint was raised with the Office of the Ombudsman during the 1 July 2020 – 30 June 2021 period. A final decision has not yet been made on this complaint.

One complaint was raised with the Office of the Privacy Commissioner during the period. As at 30 June 2021, the GCSB is working with the Office of the Privacy Commissioner to achieve a resolution to this complaint.

Financial Statements



Ngā Tauākī Pūtea

STATEMENT OF RESPONSIBILITY

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

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

In my opinion:

- The financial statements fairly reflect the financial position of the GCSB as at 30 June 2021 and its operations for the year ended on that date.

Andrew Hampton

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

22 November 2021

INDEPENDENT AUDITOR'S REPORT

To the readers of the Government Communications Security Bureau's statement of expenses and capital expenditure against appropriation for the year ended 30 June 2021

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 2021 on page 62.

Opinion

In our opinion the statement of expenses and capital expenditure against appropriation of the GCSB for the year ended 30 June 2021 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 22 November 2021. This is the date at which our opinion is expressed.

The basis for our opinion is explained below, and we draw your attention to a breach of legislation. 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.

Emphasis of matter – Breach of statutory reporting deadline

Without modifying our opinion, we draw your attention to the note on page 62 which outlines that the GCSB did not meet the requirement of section 45D of the Public Finance Act 1989. Due to the impact of Covid-19, the required information was not made available to us within two months after the end of the financial year. We could therefore not meet the requirement to issue the audit report within three months after the end of the financial year.

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 2020/21 for Vote Communications Security and Intelligence.

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

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

- We identify and assess the risks of material misstatement of the information we audited, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for our opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.

- We obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the GCSB's internal control.
- We evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by the Director-General of the GCSB.
- We conclude on the appropriateness of the use of the going concern basis of accounting by the Director-General of the GCSB and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the GCSB's ability to continue as a going concern. If we conclude that a material uncertainty exists, we are required to draw attention in our auditor's report to the related disclosures in the information we audited or, if such disclosures are inadequate, to modify our opinion. Our conclusions are based on the audit evidence obtained up to the date of our auditor's report. However, future events or conditions may cause the GCSB to cease to continue as a going concern.
- We evaluate the overall presentation, structure and content of the information we audited, including the disclosures, and whether the information we audited represents the underlying transactions and events in a manner that achieves fair presentation in accordance with the requirements of the Intelligence and Security Act 2017.

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

Our responsibilities arise from the Public Audit Act 2001.

Other information

The Director-General of the GCSB is responsible for the other information. The other information comprises the information included on pages 3 to 58, 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 issued by the New Zealand Auditing and Assurance Standards Board.

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

S B Lucy

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

Audit New Zealand
Mana Arotake Aotearoa

STATEMENT OF EXPENSES AND CAPITAL EXPENDITURE AGAINST APPROPRIATION

FOR THE YEAR ENDED 30 JUNE 2021

	$000
Total appropriation	$206,220
Total expenditure	$162,807

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.

Due to the impact of COVID-19, the Government Communications Security Bureau was unable to meet the statutory obligation under the Public Finance Act 1989 (section 45D) to provide the annual report to the Auditor-General to audit within two months after the end of the financial year. This meant that the Auditor-General was unable to provide an audit report within the three months after the end of the financial year.

GOVERNMENT COMMUNICATIONS SECURITY BUREAU

TE TIRA TIAKI

New Zealand Government