



New Zealand  
Security Intelligence  
Service  
Te Pā Whakamarumarū

# ANNUAL REPORT 2021 TE PŪRONGO Ā-TAU 2021

**Keeping New Zealand  
and New Zealanders  
safe and secure.**

**Te tiaki i a Aotearoa me  
ngā tāngata o Aotearoa  
kia haumaruru ai.**

#### **PREFACE**

This is the Annual Report of the New Zealand Security Intelligence Service (NZSIS) for the year ended 30 June 2021, presented for consideration and scrutiny to the Intelligence and Security Committee (ISC).

Presented to the House of Representatives pursuant to section 221(4) of the Intelligence and Security Act 2017.

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



# Contents

<b>DIRECTOR-GENERAL'S OVERVIEW</b> <b>TE TIRO WHĀNUI A TE TUMUAKI AHUREI</b>	<b>4</b>
<b>OUR WORK IN DETAIL</b> <b>HE TIROHANGA HŌMIROMIRO KI Ā MĀTAU MAHI</b>	<b>7</b>
New Zealand Intelligence Community	8
An Introduction to the NZSIS	10
The Strategic Environment	15
The Year in Review	17
<b>NATIONAL SECURITY INVESTIGATIONS AND ASSESSMENT</b> <b>NGĀ WHAKATEWHATEWHANGA ME TE AROMATAWAI</b> <b>I NGĀ ĀHUATANGA WHAKAHAUMARU Ā-MOTU</b>	<b>21</b>
Countering the Threat of Terrorism	22
Investigating Violent Extremism Threats	23
The Combined Threat Assessment Group	30
Espionage and Foreign Interference	32
Investigating Espionage and Foreign Interference	35
<b>PROTECTIVE SECURITY SERVICES</b> <b>NGĀ RATONGA TAUTIAKI WHAKAHAUMARU</b>	<b>37</b>
Protecting People, Information, and Assets	38
Protective Security Requirements	39
National Security Clearances	41
<b>NATIONAL SECURITY RISK ADVICE</b> <b>NGĀ TOHUTOHU TŪRARU WHAKAHAUMARU Ā-MOTU</b>	<b>47</b>
Security Screening	48
Overseas Investment Assessments	49
Countering the Proliferation of Weapons of Mass Destruction Technology	50
Space and High-altitude Activity Assessments	50
<b>PROTECTING REGIONAL SECURITY</b> <b>TE TAUTIAKI WHAKAHAUMARU Ā-ROHE</b>	<b>51</b>
Contributions to Pacific Regional Security	52
Contributions to International Security	53
International Liaison	53
<b>ORGANISATIONAL CAPABILITY   NGĀ ĀHEITANGA WHAKAHAERE</b>	<b>55</b>
<b>OUR PEOPLE   Ō MĀTAU TĀNGATA</b>	<b>57</b>
Our People	58
Diversity in the Workforce	60
Progress Against Public Service Commission Papa Pounamu Commitments	65
Supporting Inclusion in the NZSIS	67
Talent Outreach and Engagement	68
<b>ACCOUNTABILITY AND TRANSPARENCY</b> <b>TE NOHO HERE ME TE PŪATAATA</b>	<b>69</b>
Engagement and Transparency	70
Oversight	72
Statement on Warrants	73
<b>FINANCIAL STATEMENTS   NGĀ TAUĀKĪ PŪTEA</b>	<b>75</b>

# Director-General's Overview

## Te Tiro Whānui a te Tumuaki Ahurei

### The past year has seen more information about the New Zealand Security Intelligence Service (NZSIS) made publicly available than ever before.

The NZSIS has fully supported this shift. We worked hard to declassify information so that it could be included in the December 2020 release of the *Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019* ("the Report"). We understood that the scale of the attack meant that greatest possible public transparency was vital. The result was that an unprecedented level of detail was put into the public domain about the NZSIS's processes and capabilities.

The release of the Report was a very significant event for the year. The Report found no failures within any government agencies that would have allowed the terrorist's planning and preparation to have been detected. The Report also found, however, that there should have been an informed, system-wide assessment to understand whether counter-terrorism resources were appropriately allocated in the years leading up to the attack.

The Royal Commission recognised the enormous amount of change and improvement that has taken place within the NZSIS over recent years. While there were no recommendations for the NZSIS, the Report identified many lessons to be learnt and areas needing change within the overall national security system.

The NZSIS is absolutely committed to contributing to and supporting those changes. We are also committed to continuing our own evolution in line with the direction of travel identified by the Royal Commission; in particular to increase our ability to discover unknown threats through our Discover Strategy. The 51 shuhada, the survivors, their families, and their communities are front of mind for us as we strive to achieve better national security outcomes for New Zealanders.

The Royal Commission also emphasised the importance of a more active public conversation about national security – which the NZSIS welcomes. The NZSIS can help by making more information public, and by sharing intelligence with customers at the lowest possible levels of classification. There is – unfortunately – a necessary limit on how much the NZSIS can reveal publicly about our work. Those who seek to harm New Zealand and New Zealanders are constantly learning and adapting their activities to avoid our attention. We must not help them by disclosing information about our specific areas of focus, our sources, or our most secret capabilities. Having said that, we do continually debate and discuss how much information we can make public without compromising our mission of keeping New Zealand safe.



We demonstrated our drive for increased transparency by releasing a declassified version of the internal review into our practices and decision-making in the lead up to the terrorist attack (“the Arotake Report”). In addition, anonymised case studies of some key investigations were published in last year’s annual report, to demonstrate both the scope and complexity of our work, and the value of our intelligence for New Zealand. Further case studies have been included in this year’s annual report. And more NZSIS officers have been authorised to openly engage with the public and communities about our work, including declaring where they work. That might not sound like a big deal for most New Zealanders but it represents a significant change at the NZSIS, where traditionally only the Director-General has been authorised to speak on the agency’s behalf.

The trend towards greater openness and transparency will help more New Zealanders understand the threats we face as a nation. The Royal Commission emphasised that good national security outcomes cannot be achieved by law enforcement and intelligence agencies alone. If we are to enlist the support of the New Zealand public in the national security effort then we need to help them

understand the nature of the threats we face. It’s important we do this in a way that inspires confidence that as a country we can unite against national security threats. An inclusive approach is also vital so everyone feels they have a role to play, and so that we don’t unfairly associate entire communities with a perceived threat.

In line with this approach, the NZSIS has changed its counter-terrorism terminology to avoid stereotyping and to be more specific about the violent extremist ideologies we are investigating. I am pleased to say that our language is being increasingly adopted across government agencies.

In addition, NZSIS is in the process of completing a set of terrorism indicators, which will outline behaviours that everyone should be aware of and know to report. These indicators will be publicly released in the next reporting period.

Greater and more open engagement is also informing our approach to countering espionage and foreign interference. We are reaching out to those that are most at risk of being targeted by foreign states and their proxies for the purposes of foreign interference or espionage. Our outreach, using guidance developed by our Protective

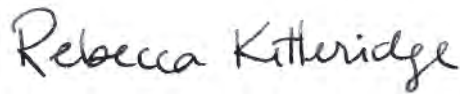
Security Requirements team, has included local government, academia, and politicians — all of whom we have found to be highly engaged on the topic.

At the same time as engaging more openly, NZSIS must continue to develop its own capabilities to counter constantly evolving threats. The Royal Commission identified a critical challenge faced by all security agencies such as ours: how to join dots and identify weak signals to reveal and understand would-be terrorists or other security threats.

Joining these dots is hugely assisted by having access to and analysing the right data at the right time. NZSIS, like other 21st century organisations, is increasingly data-led. We understand that the public will want to have input about how we collect data, and how we hold it, use it, and protect it. I would welcome a measured and informed public discussion about how to achieve positive national security objectives while safeguarding privacy, leading to a broad consensus about the best balance.

In the meantime, the people of the NZSIS will continue to learn and evolve, and will strive to do everything they can to keep New Zealand safe and secure.

New Zealanders cannot always see the difference my staff make, but I do. I am immensely proud to lead such a committed group of public servants, a group which exemplifies the spirit of service to New Zealand.



**Rebecca Kitteridge**

Director-General of Security

Te Tumu Whakarae mō Te Pā Whakamarumarū

22 November 2021

# 01

## **Our Work in Detail**

He Tirohanga Hōmiromiro  
ki ā mātau Mahi



# New Zealand's Intelligence Community

## **The NZSIS, the Government Communications Security Bureau (GCSB), and the National Security Group within Department of the Prime Minister and Cabinet (DPMC) perform the national intelligence and assessment functions within the New Zealand Intelligence Community (NZIC).**

These agencies work with the specialist intelligence functions of other agencies such as New Zealand Police, the New Zealand Customs Service, the New Zealand Defence Force, and Immigration New Zealand. The NZIC exists to protect New Zealand as a free, open, and democratic society. The intelligence-based insights and advice provided by the NZIC contribute to decisions that sustain and enhance New Zealand's security and wellbeing.

The work of the NZIC is a key contributor to the national security of New Zealand, and by extension, to the current and future wellbeing

of New Zealand and New Zealanders. The NZIC has a crucial role to play in understanding the threats New Zealand faces and how to guard against those threats.

The NZIC contributes to building a safer and more prosperous New Zealand. NZIC agencies work to ensure that New Zealand is protected from harm and that New Zealand policy makers have intelligence to support good decision-making. The NZIC strives to advance New Zealand's international reputation and interests.



## Agencies

The core NZIC agencies are:



### New Zealand Security Intelligence Service

Te Pā Whakamarumarū

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.



### GOVERNMENT COMMUNICATIONS SECURITY BUREAU

TE TIRA TIAKI

The GCSB provides information assurance and cyber security to the New Zealand Government and critical infrastructure organisations, collects and analyses intelligence in accordance with the Government's priorities, and provides cooperation and assistance to other New Zealand government agencies.



### DEPARTMENT OF THE PRIME MINISTER AND CABINET

TE TARI O TE PIRIMIA ME TE KOMITI MATUA

#### NATIONAL SECURITY GROUP

The National Security Group helps inform government decision-making by providing intelligence assessments on events and developments that are relevant to New Zealand's interests.

The National Security Group is also responsible for promoting excellence in intelligence analysis across the New Zealand Government.

# An Introduction to the NZSIS

## **The NZSIS is New Zealand’s domestic security intelligence agency, with a mission to keep New Zealand and New Zealanders safe and secure. The NZSIS is New Zealand’s lead organisation for human intelligence (HUMINT).**

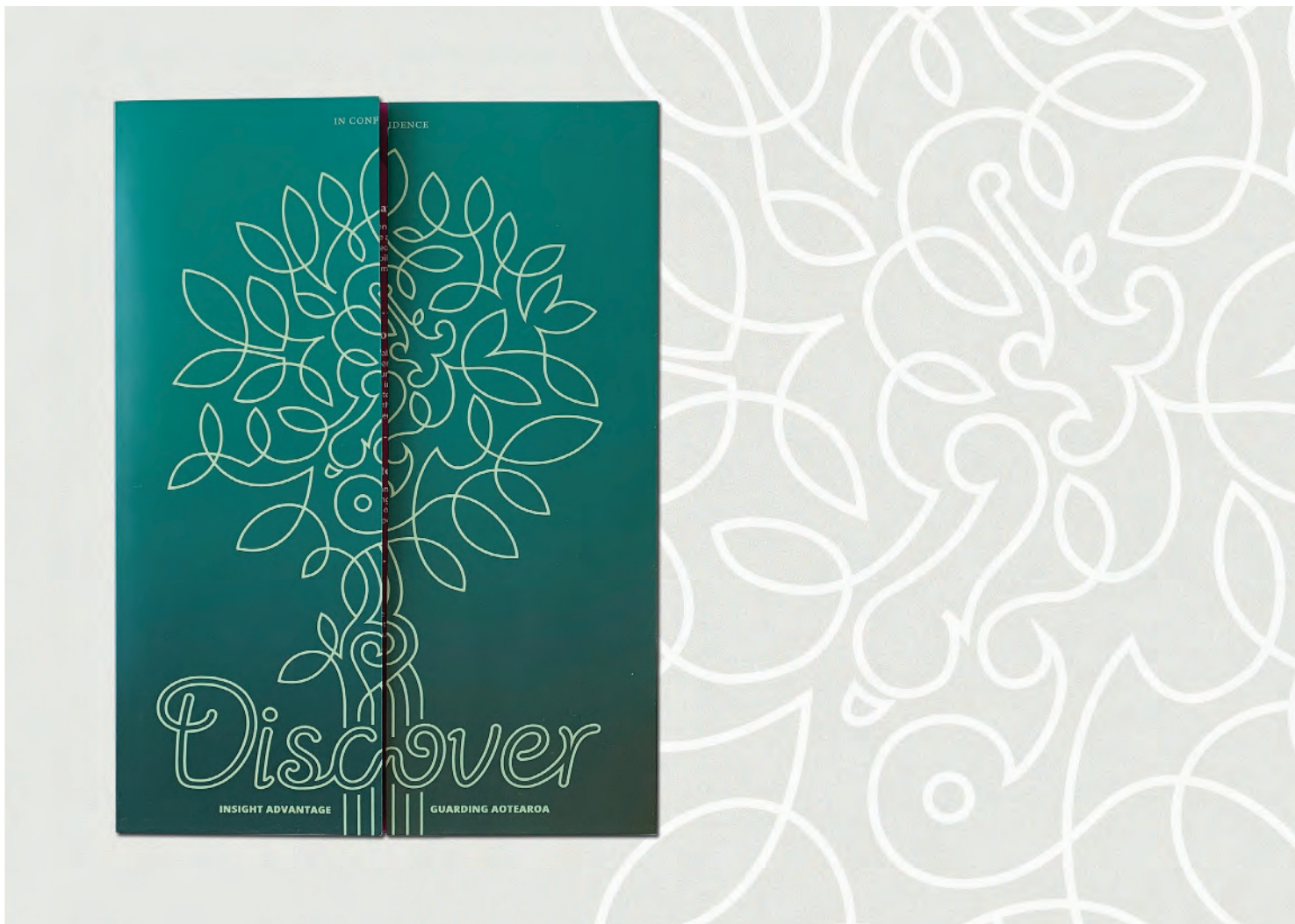
The NZSIS head office is based in Pipitea House on Pipitea Street in Wellington. The NZSIS has regional offices in Auckland, Christchurch, and overseas liaison offices. As of 30 June 2021, the NZSIS had 397.15<sup>1</sup> full-time equivalent staff.

On its fiftieth anniversary (2006), the Māori name for the NZSIS, Te Pā Whakamarumarū, which translates to The Sheltering Citadel, was adopted as part of its official emblem.

The NZSIS undertakes a range of functions relevant to New Zealand’s security. These include:

- Collecting, analysing and reporting on intelligence relevant to New Zealand’s security.
- Providing protective security services, including advice about personnel security, information security, physical security, and national security risks.
- Cooperating with a variety of other government agencies in the performance of their functions. These agencies include the GCSB, the New Zealand Defence Force, New Zealand Police, the Department of Corrections, the New Zealand Customs Service, the Ministry of Foreign Affairs and Trade, and the Ministry of Business, Innovation, and Employment.

<sup>1</sup> This FTE count is consistent with Public Service Commission methodology, counting all current employees of the NZSIS excluding those on leave without pay or parental leave.



## NZSIS Strategy: Discover

In 2019, the NZSIS undertook a strategic refresh and replaced STERLING with the Discover Strategy. STERLING was designed in 2015/16 as “version 0.1”, with the intention that future iterations would need to evolve in response to environmental changes. Much of what we learned from STERLING and many of its initiatives continue to be represented in the new strategy.

The refreshed NZSIS Strategy is focused on six key themes that collectively contribute to the following outcomes:

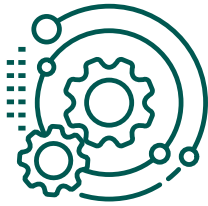
- New Zealand institutions are protected
- New Zealanders are safe
- New Zealand’s national advantage is promoted

The first of these six themes and current organisational priority is Discover. The Discover Strategy provides a pathway to unlock the NZSIS’s ability to discover, connect, and use information. As key Discover objectives are delivered, subsequent themes will include Investigate, Impact, Respond, System, and Future.

The Discover Strategy is intended to improve the way that the NZSIS accesses and analyses information sources. This includes information sources that are already used, as well as future requirements. Through this Discover theme, the NZSIS will gain a better understanding of known adversaries, and increase opportunities to find emerging or unknown threats. Discover is about:

- Finding the right information at the right time
- Knowing adversaries and understanding where threats, risks, and vulnerabilities may appear
- Generating enriched security intelligence insights for customers
- Strengthening foundations, leveraging trusted information and knowledge for decision-making
- Understanding the skills and experience staff need and the factors to attract and retain our workforce
- Being open and exploring different ways to do our business

Five Strategic Objectives have been developed to deliver the Discover Strategy:



### Optimising use of data and information

Accessing the right data when needed, by people with the skills, experience and tools needed to analyse data and information to generate insights that matter. Effectively managing and sharing data and information in a trusted way, producing consistent and reliable outputs. Inefficiencies are removed, policies and processes improved or automated in an innovative culture.



### Creating a discover environment

The authorising environment enables the NZSIS to discover those who intend to harm New Zealand or New Zealanders by fostering fast access and information use. The NZSIS knows the threat, risk, and vulnerability indicators and has ways of identifying future threats. Strong relationships with the right people and organisations allow timely, evidence-based insights and services that customers value.



### Strengthening customers

Customers have the knowledge and abilities they need to prevent and manage their security risks and vulnerabilities. They feel supported by NZSIS services and proactively find and report suspicious activities.



### Advancing our workforce

The NZSIS is a desirable place to work, attracting the right people with the right skills and experience. The NZSIS anticipates future workforce needs and is agile to changes in the environment.



### Enhancing regional security understanding

The NZSIS understands our regional context and its role. It knows what is normal and can see shifts in behaviours and actions that could indicate areas of interest, risk, and vulnerabilities to New Zealand's regional priorities.



## National Security and Intelligence Priorities

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

New Zealand takes an 'all hazards, all risks' approach to national security. This means the priorities cover a large range of risks to New Zealand's security and wellbeing.

The NSIPs are coordinated by the Department of the Prime Minister and Cabinet (DPMC) and a range of agencies, including the NZSIS, work toward achieving them. The priorities include counter-terrorism, foreign interference, global economy, emerging technology, malicious cyber activity, regional stability, and space.

The current priorities were approved in December 2018 and are listed below 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 (ideologically, politically, or religiously motivated violence) at home and abroad.
- **Threats to New Zealanders overseas** – Threats 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 Strategic Environment

## Terrorism and Violent Extremism

New Zealand's national terrorism threat level is currently set at 'Medium'. This means a terrorist attack is assessed as 'feasible and could well occur'.

New Zealand's terrorism threat environment remains dynamic due to the ongoing influence of the 2019 Christchurch attack, the COVID-19 pandemic, and global trends in extremism and terrorism. It is possible that COVID-19-related personal grievances, and increased time spent online during lockdowns around the world, will result in online rhetoric that will continue to accelerate some drivers of violent extremism in New Zealand. However, the extent of this radicalisation, how it has manifested to date, and how it will present in the medium to long-term, remains unclear.

The Christchurch attack continues to influence the domestic terrorism threat environment, although we believe this has gradually diminished over time. The Christchurch attack will continue to influence New Zealand's terrorism threat environment in the long-term, including through online propaganda. New Zealand-based individuals continue to display support for the Islamic State in Iraq and the Levant (ISIL), and continue to consume its propaganda and espouse extremist rhetoric online. Despite this, ISIL's overall loss of influence has diminished its ability to radicalise new followers in New Zealand.





## Espionage and Foreign Interference

Foreign political and economic espionage remains a significant threat to New Zealand's interests. Foreign intelligence services exist to obtain useful information for their governments. Intelligence can be collected in a number of ways, including through cyber activity, by professional intelligence officers utilising operational cover, or by individuals who have been co-opted to act on behalf of a foreign intelligence agency. In the latter two scenarios, information is collected by either the intelligence officer or the co-optee by developing personal and professional relationships with government officials, academics, business people, and politically-connected individuals to elicit information.

Foreign intelligence services continue to target New Zealand interests through the use of human intelligence collection and cyber espionage. Foreign states have also targeted New Zealand universities and organisations to steal personal data, research data, and intellectual property.

A foreign state actor may:

- Seek opportunities to develop a research and innovation base that increases its economic, military, and technological advantages over other countries.
- Prioritise the stability of its regime by suppressing dissent, political opposition, or media freedoms in countries other than its own.

Foreign interference should be understood as an effect against a state's politics, governance, or society that is facilitated by covert operational activity. Interference refers to acts by a state or its proxies that are intended to influence, disrupt, or subvert another state's interests through deceptive, corruptive, or coercive means. Normal diplomatic activity, lobbying, and other genuine and overt efforts to gain influence are not interference.

## Security in the Pacific

Geopolitical competition in the Pacific has continued over the past year. An increased number of countries compete for influence in the region through development funding, infrastructure builds, and proposals for military and security cooperation. This increased competition for influence and dominance in the Pacific is eroding some of the security benefits of New Zealand's geographic isolation.



# The Year in Review

## Royal Commission of Inquiry into the Christchurch Terrorist Attack

On 8 December 2020, the findings of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019 were made public. The 51 shuhada of the attack, their loved ones, and the wider community have remained front of mind in the NZSIS response to the Royal Commission's report.

The NZSIS was already going through a significant transformation at the time of the attack. That transformation has continued, and will go even further with the insights provided by the Royal Commission. The NZSIS is absolutely committed to addressing the recommendations of the Royal Commission, and some changes that the NZSIS has already made include:

- Enhancing how the NZSIS works with its key partner agencies, particularly New Zealand Police, to improve coordination of the detection and investigation of counter-terrorism threats. This change includes further developing a joint leads process and strengthening inter-agency governance.
- A significantly increased focus on ensuring the NZSIS is connected with a range of communities to identify and discuss shared national security concerns, including being an active participant in the Royal Commission implementation and engagement programme.
- Designing and running a recruitment campaign aimed at increasing the diversity of the workforce within the intelligence agencies.
- Strengthening existing training measures already in place at the NZSIS to help our people understand unconscious bias, and how to remove bias from their decision-making.

The NZSIS released a declassified version of the Arotake report in March 2021. Arotake was an internal review into our processes and decision-making in the lead up to the 15 March 2019 terrorist attack in Christchurch. While Arotake remains useful internally for the NZSIS, its findings are superseded by the findings and recommendations of the Royal Commission.



## 2020 General Election

New Zealand, like many other countries in the world, is the target of foreign interference. States may be motivated for a range of tactical and strategic reasons to attempt political interference against New Zealand, and this could take the form of interference in our elections and our democratic institutions.

In the period surrounding the 2020 General Election, the NZSIS focused on monitoring and collating insights about the activities of foreign states against New Zealand's democratic system and electoral processes. Due to the prevalence of interference in elections globally, this issue remains a key area of focus for us. The NZSIS did not identify systemic, state-sponsored interference activity against the 2020 New Zealand General Election.

## Trusted Research Guidance

New Zealand's thriving research and innovation sector attracts funding and investment from across the world. New Zealand has an open and collaborative research and innovation system, and values academic freedom and research conducted independently by individuals and organisations. Still, there are risks with international engagement that should be identified and managed to prevent any harm to New Zealand's national interests.

In 2021, Trusted Research guidance for institutions and researchers was launched. This guidance was produced through collaboration between New Zealand's research and university communities and our Protective Security Requirements team.

Trusted Research guidance aims to help New Zealand's research and innovation sector get the most out of international scientific collaboration while protecting their intellectual property, sensitive research, and personal information. Trusted Research guidance:

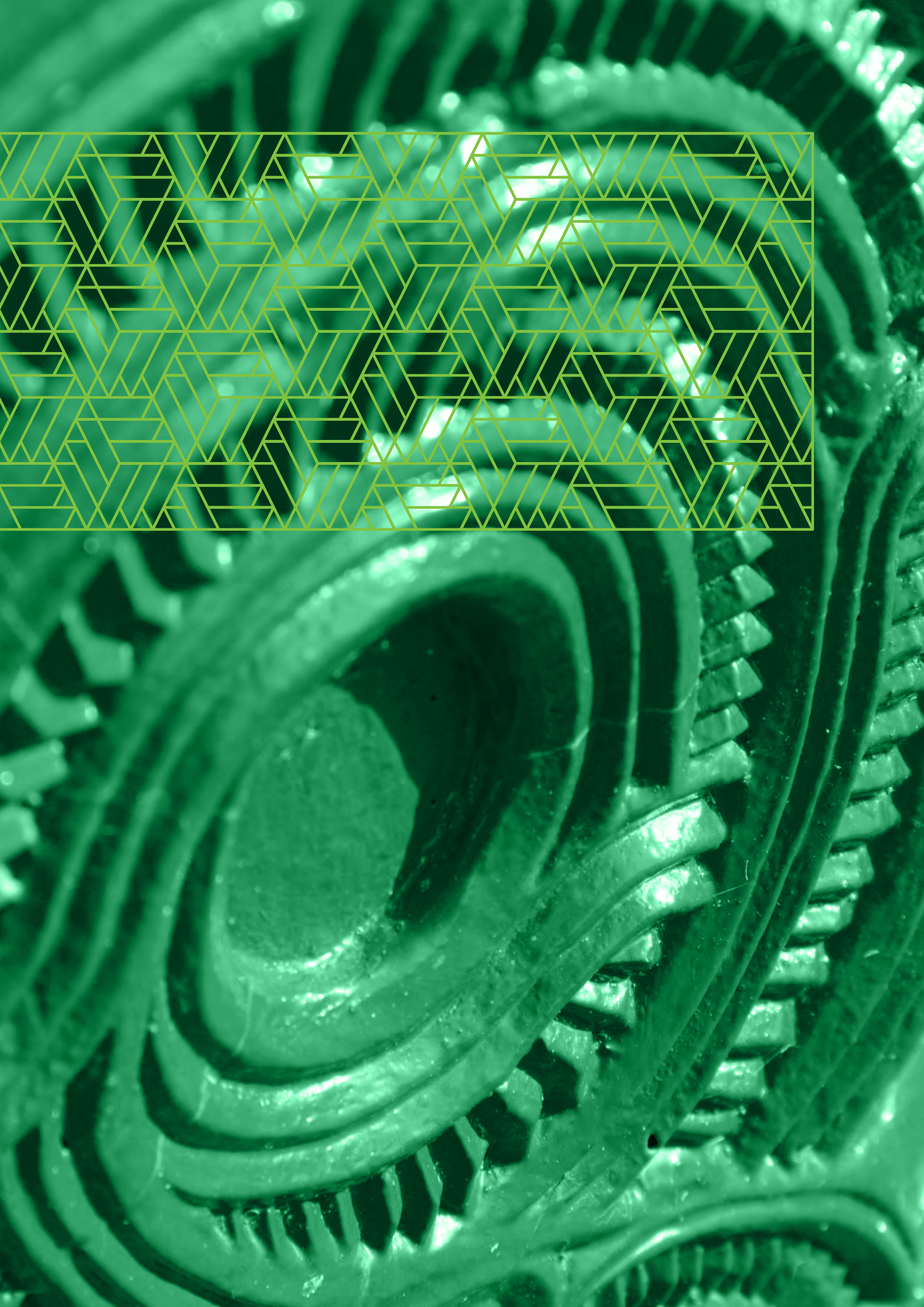
- Outlines the potential risks to New Zealand research and innovation;
- Helps researchers, New Zealand universities, research organisations, and industry partners have confidence in international collaboration, and make informed decisions about potential risks; and
- Explains how to protect research and staff from potential theft, misuse, or exploitation.





Trusted Research guidance aims to help New Zealand’s research and innovation sector get the most out of international scientific collaboration while protecting their intellectual property, sensitive research, and personal information.







# 02

## **National Security Investigations and Assessment**

Ngā Whakatewhatewhanga me  
te Aromatawai i ngā Āhuatanga  
Whakahaumarū ā-Motu

The NZSIS works to protect New Zealanders by detecting, investigating and providing advice about threats to their wellbeing. We provide advice to Government, other agencies and our international partners to enable them to make informed decisions.

# Countering the Threat of Terrorism

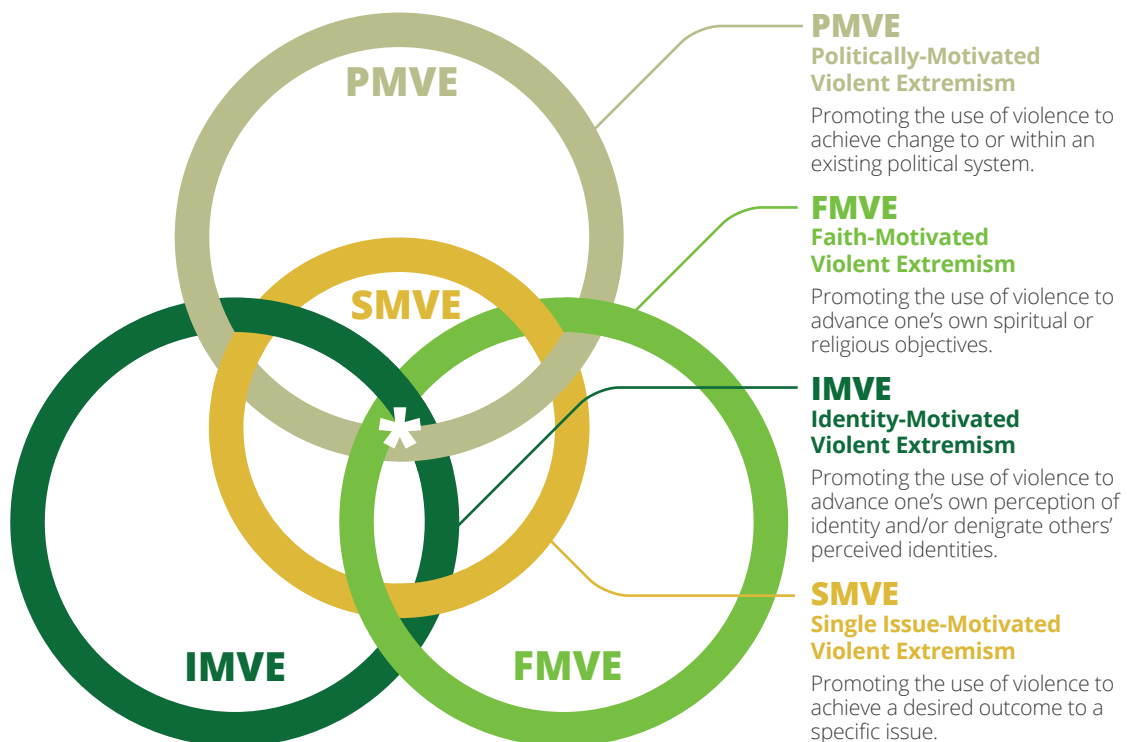
## The NZSIS investigates violent extremism threats against New Zealand interests and works with other agencies to prevent these threats from escalating into acts of terrorism.

The NZSIS looks at global and domestic events and developments relating to violent extremism in order to understand the possible impact on violent extremist activity in New Zealand. This enables the NZSIS to assess whether existing threats are increasing or diminishing, and to understand new or emerging threats.

We provide the Government and government agencies with intelligence, threat assessments, and advice to inform their response to specific terrorist threats and to broader trends in violent extremism.

### Extremism Terminology

The NZSIS uses terminology consistent with the CTAG framework when referring to extremist ideology.



# Investigating Violent Extremism Threats

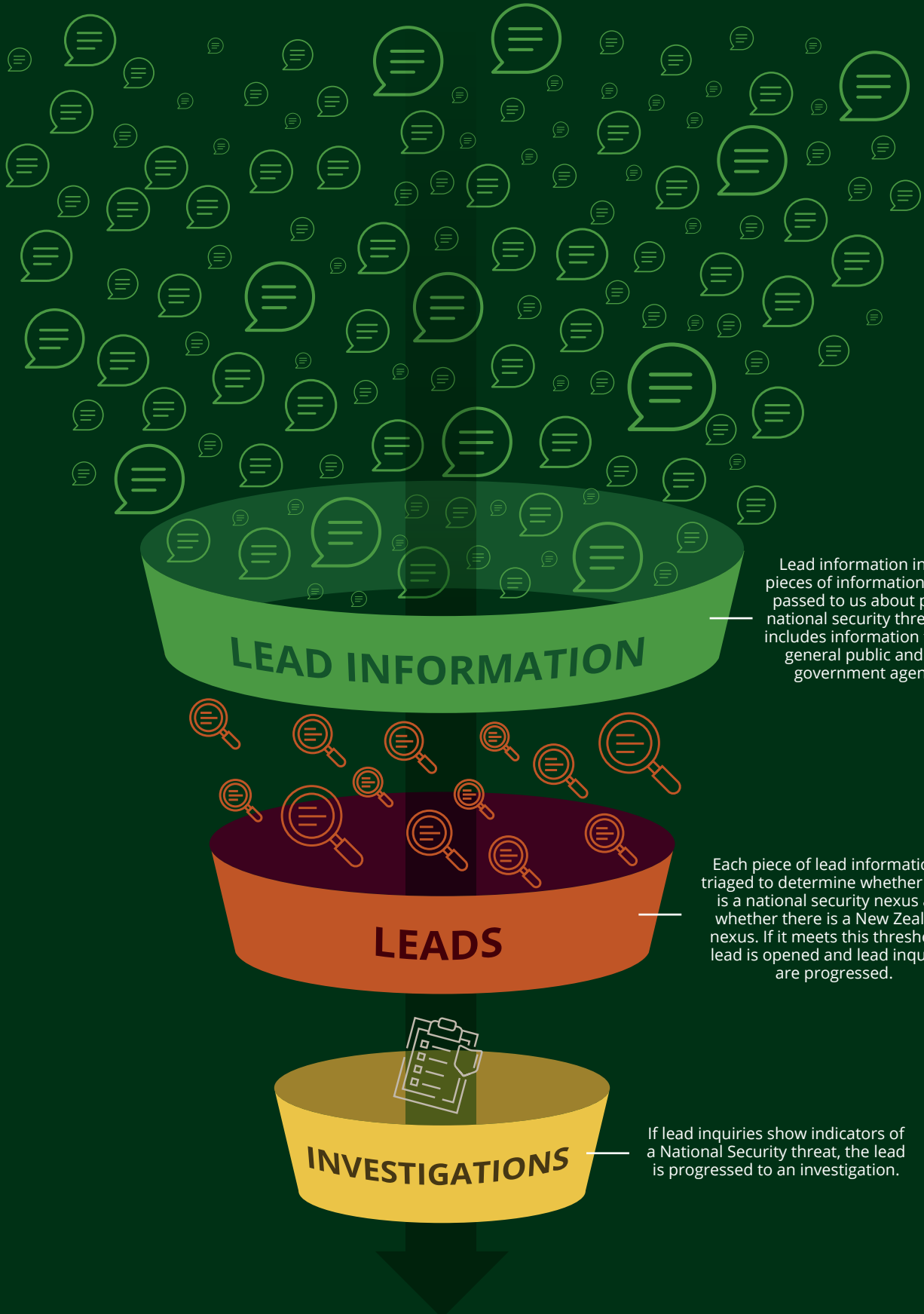
**The NZSIS investigates threats to the public's safety posed by violent extremism at home and abroad. We investigate individuals and groups that support violent extremist organisations, or promote violent extremist ideologies, or may be planning to undertake a terrorist attack. We investigate threats to New Zealand and New Zealanders.**

The NZSIS's counter-terrorism investigations rely on information about potential threats and extremist activities. We call this lead information. The lead information comes from a wide range of sources, including the public, international and domestic partner agencies and groups, and from other NZSIS investigations and enquiries.

A range of powers and information collection tools are used to evaluate lead information to assess the extent to which a national security threat exists. For each piece of lead information received, the NZSIS considers whether the lead information meets the threshold to initiate further enquiries to determine the nature of the threat.

The NZSIS works closely with other agencies – notably the New Zealand Police – to investigate threats that pose a risk to the public.

# HOW THE NZSIS INVESTIGATES COUNTER-TERRORISM



Lead information includes pieces of information that are passed to us about possible national security threats. This includes information from the general public and other government agencies.

Each piece of lead information is triaged to determine whether there is a national security nexus and whether there is a New Zealand nexus. If it meets this threshold a lead is opened and lead inquiries are progressed.

If lead inquiries show indicators of a National Security threat, the lead is progressed to an investigation.



## Investigating terrorist threats in 2020/21

### LEADS

During the 2020/21 year, the NZSIS received a range of lead information relating to a broad spectrum of extremist ideologies and support for extremist groups.

Harmful online activity, including individuals consuming extremist material and expressing violent rhetoric, was a consistent feature of many leads, with one third of all leads relating to online threats or support for violent extremism. Information from online platforms presents a real challenge to counter-terrorism investigations, often due to the anonymity provided by some forums, and the proliferation of non-genuine or hoax threats.

### VIOLENT EXTREMIST IDEOLOGIES

The 2020/21 period has seen an increased range of extremist ideologies and sentiment manifesting in New Zealand, with international trends continuing to influence the real-world and online activities of individuals in this country.

Increasingly we have seen crossovers and combinations of different ideologies, with co-mingling of political, identity, faith, and single-issue agendas, sometimes combined with or exacerbated by trending topical issues and conspiracy theories.

### INVESTIGATIONS

During the past year, between 40 and 50 individuals have been under active investigation by the NZSIS in relation to violent extremism at any one time.

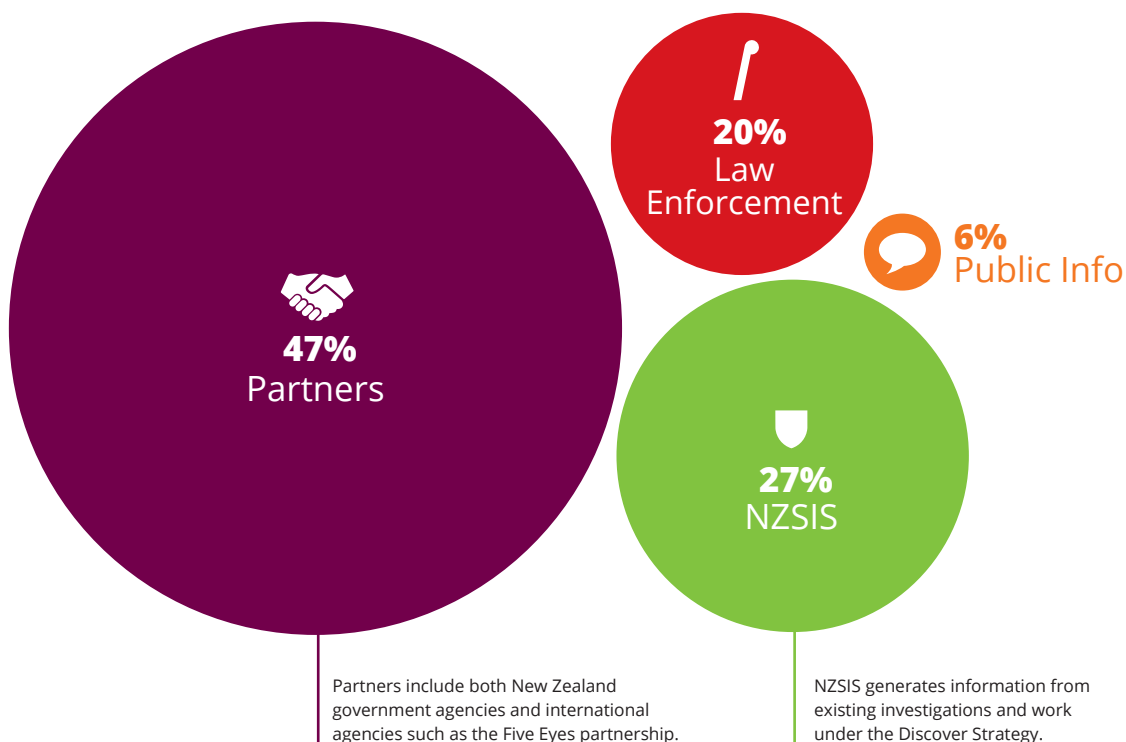
Terrorist violence in New Zealand is most likely to come from extremists who choose to undertake an act of ideologically motivated violence without communicating their plans to others. They may mobilise to violence rapidly, with little or no warning.

The investigations the NZSIS undertook throughout 2020/21 reflect those of previous years, with the majority having an identity-based or faith-based violent extremist ideology. As of June 2021 there was approximately a 50/50 split between identity-based and faith-based investigations as part of the overall caseload.

Public awareness and reporting of suspicious and extreme ideological behaviour or violent rhetoric continues to be an important and valuable source of information. In 2020/21, approximately 15% of counter-terrorism investigations originated from public information.

Our active investigations include a small number of New Zealanders who are believed to remain offshore linked to Islamic State in Iraq and the Levant (ISIL) or other extremist groups.

## SOURCES OF COUNTER-TERRORISM OPENED IN 2020/2021



### ONLINE EXTREMISM

The sheer quantity of extremist content and extremist ideologies of various kinds online continues to be a security challenge in New Zealand and around the world.

Individuals can be exposed to graphic content and extremist ideologies in their own homes with little, if any, moderating influence. The consumption of extremist material may radicalise an individual and, in some cases, lead ideologically-motivated extremists to attempt real-world actions in support of their beliefs.

Internationally, elements of COVID-19 pandemic-related grievances and various conspiracy theories continue to contribute to the beliefs and discourse of some extremist entities. In line with international trends, this was seen to escalate to a peak during and following global political events, but has since diminished as some of the claims and predictions of online groups and entities have not eventuated.

It is likely that the ongoing online trends of pandemic and conspiracy-related sentiment will continue to influence and impact on the New Zealand security environment.

The NZSIS is aware that offensive, racist, and hateful views are spread in our communities every day. The online environment makes this easier than ever before. Anonymous internet forums have enabled threats to be posted online that do not represent the genuine intent of the individual posting the threat. Such threats, while easily made, are difficult to attribute to a user and to determine whether it constitutes a genuine threat to national security. When the NZSIS is alerted to an online threat, whether that be through our own enquiries or through public reporting, we work to identify whether the individual has the intent and capability to carry out the threat.

## **IDENTIFYING UNKNOWN THREATS**

The NZSIS has dedicated resources to discover unknown terrorism threats to New Zealand. In 2020/21, we have focused on collaborating with various New Zealand government agencies and international partners to expand this programme of work. In doing so, the NZSIS aims to provide assurance and insight to partner agencies on emerging terrorism threats to New Zealand.

The NZSIS is actively working to enhance our outreach activities, and to equip partner agencies, organisations, and the people of New Zealand with knowledge and tools to assist in identifying violent extremism. To support this work, in early 2021 the NZSIS developed and shared a classified Terrorism Indicators Framework. The framework focuses on identifying pathways to terrorism by illustrating behaviours and activities that may indicate someone is mobilising in support of an extremist ideology or cause. The NZSIS is currently working to produce an unclassified Terrorism Indicators Framework to equip the people of New Zealand with the knowledge and tools to assist in identifying violent extremism.

The NZSIS continues to engage with a range of groups and communities around New Zealand to provide guidance and understanding around violent extremism. This engagement is vital in building a relationship of trust and understanding between the NZSIS and communities within New Zealand.

## **YOUNG PEOPLE ENGAGED WITH EXTREMIST IDEOLOGIES**

In 2020/21 the NZSIS has seen an increasing number of young people exposed to violent and extremist material, predominantly online, with some who have subsequently expressed support for violent extremist ideologies.

In New Zealand, the goal of New Zealand government agencies is to encourage young people to disengage from violent extremism, including through social support opportunities. The NZSIS is part of a multi-agency working group, He Aranga Ake, which aims to empower frontline agencies to engage with at-risk young people to support their disengagement from violent extremism.

## Case studies

### CASE STUDY 1

In 2020/21, the NZSIS investigated an individual who expressed support for identity-motivated violent extremism, and claimed he planned to undertake a domestic terrorist attack in the future. The individual was also actively involved in extremist forums online. The NZSIS worked closely with other government agencies to identify and mitigate the potential threat posed by this person.

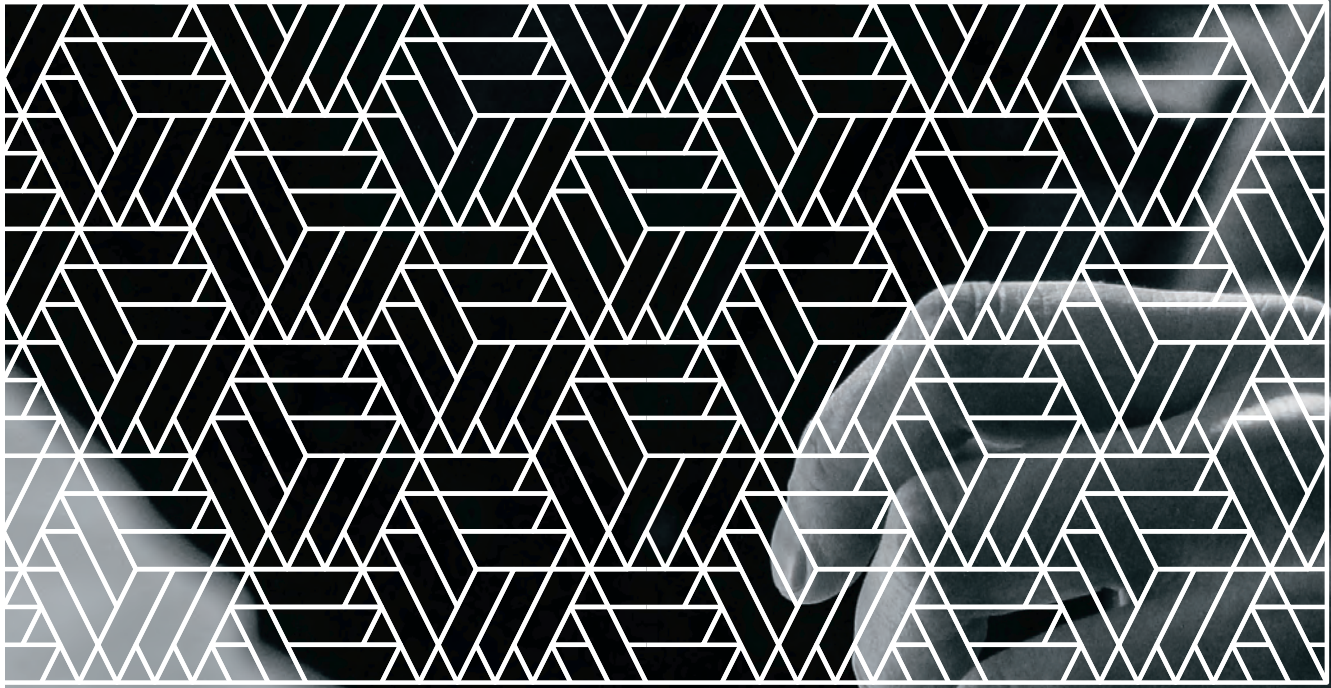
### CASE STUDY 2

In late 2020, the NZSIS received information from a partner agency identifying an online account which espoused a faith-motivated violent extremist ideology. The user made comments indicating they were located in New Zealand. Analysis of the individual's online activities has identified the user, and enquiries are underway to understand whether they pose a national security threat.

### CASE STUDY 3

In mid-2020, a member of the public provided information on a New Zealand-based individual who had expressed support for identity-motivated violent extremism and had made comments supportive of violence against non-European communities. The NZSIS worked closely with New Zealand Police to identify the individual, determine the national security threat they posed, and mitigate the threat. The individual has been charged with offences related to their online activities.







# The Combined Threat Assessment Group

**The NZSIS works to understand domestic and global trends relating to violent extremism. A wide range of intelligence is examined – drawn from our own investigations, other New Zealand government agencies, and international counterparts – to provide an assessment of the impact of violent extremism on New Zealand’s strategic environment.**

## **The Combined Threat Assessment Group**

The Combined Threat Assessment Group (CTAG) is an interagency group hosted by the NZSIS that provides independent assessments to inform the National Security System and wider government agencies of the physical threat posed by terrorism to New Zealanders and New Zealand interests domestically and overseas.

CTAG includes representatives from NZSIS, GCSB, New Zealand Defence Force, New Zealand Police, Department of Corrections and the Civil Aviation Authority, funding contributions from the Ministry of Foreign Affairs and Trade and the New Zealand Customs Service, and benefits from analytical coordination and cooperation with the National Assessments Bureau.

CTAG works closely with other government agencies to ensure that the national terrorism threat level is set appropriately. The national terrorism threat level informs national security risk management and decision-making processes. CTAG also prepares threat assessments on a wide range of domestic and global terrorism threat issues.

## The National Terrorism Threat Level

CTAG uses a five-tier framework to determine the threat of terrorist activity, which ranges from 'Very Low' to 'Extreme'. The national terrorism threat level is used by government agencies to ensure they consistently manage risks associated with terrorism. A formal review of New Zealand's terrorism threat environment and threat level takes place annually, but does not prevent a change in threat level at any time in response to emerging threats.

In the immediate aftermath of the Christchurch attack, the national terrorism threat level was raised from 'Low' to 'High'. This reflected the impact the attack had on the New Zealand threat environment and the likelihood of a copycat or revenge attack against New Zealand interests offshore. Based on subsequent intelligence assessments, the threat level was lowered to 'Medium' in April 2019.

The routine annual review of the domestic threat level was conducted in February 2021. The national terrorism threat level remains set at 'Medium', which means a terrorist attack is assessed as feasible and could well occur.

### NEW ZEALAND TERRORISM THREAT LEVEL DEFINITIONS

#### LIKELIHOOD ASSESSMENT

#### THREAT LEVEL

Expected .....	<b>EXTREME</b>
Highly likely .....	<b>HIGH</b>
Feasible and could well occur .....	<b>MEDIUM</b>
Realistic possibility .....	<b>LOW</b>
Unlikely .....	<b>VERY LOW</b>

# Espionage and Foreign Interference

**The NZSIS investigates and provides advice on possible espionage and foreign interference threats taking place in or against New Zealand. We seek to understand and assess the threats and provide timely advice and intelligence reporting to other agencies to help counter these activities.**

The NZSIS investigates specific instances of espionage and foreign interference activity, as well as working to monitor and understand the overall threat posed by different states to New Zealand. We provide analysis on emerging threats and evolving patterns in espionage and foreign interference. A particular focus is on identifying and understanding the covert activities of foreign state actors operating in, or seeking to influence, New Zealand democratic institutions, decision-making, and processes.

Our work enables us to provide comprehensive advice to government partners about the threats to New Zealand's interests in the dynamic geopolitical environment. We work closely with the GCSB and NZSIS Protective Security teams to inform their advice and assistance to a wide range of individuals and entities both inside and outside government. We also work with our international intelligence partners to share information and understand emerging international threats.

## Espionage

Espionage poses an enduring threat to New Zealand's interests. Espionage refers to the clandestine activities that states undertake to collect information, materials, or capability for the purpose of obtaining an advantage over their rivals. The NZSIS divides espionage into two major categories:

- **State espionage** targets New Zealand government entities for sensitive and protected information and capabilities, both in New Zealand and against our official presence abroad.
- **Economic espionage** targets New Zealand's commercial, research, and industrial entities for proprietary technology, research, and commercial information.

Over the past year we have seen New Zealand's border restrictions limit some human espionage. Despite this, current settings do not restrict either the activities of intelligence assets already in New Zealand or those that use cyber means. Espionage threats to New Zealand's interests are also present offshore, and target our official and commercial presence in certain countries.

# EXTERNAL THEMATIC/ EMERGING THREATS TO NEW ZEALAND'S INTERESTS

## COERCIVE STATECRAFT & ECONOMIC ESPIONAGE

Theft of intellectual  
property and technology

Technical  
surveillance

## TECHNOLOGICAL CHANGE

Disruptions in  
international  
commerce and  
supply chains

Encrypted means  
of spreading  
misinformation

Cyber-enabled coercion and espionage  
Inter-connectivity and proliferation  
of personal networked technology  
Data complexities

## OUR NEIGHBOURHOOD

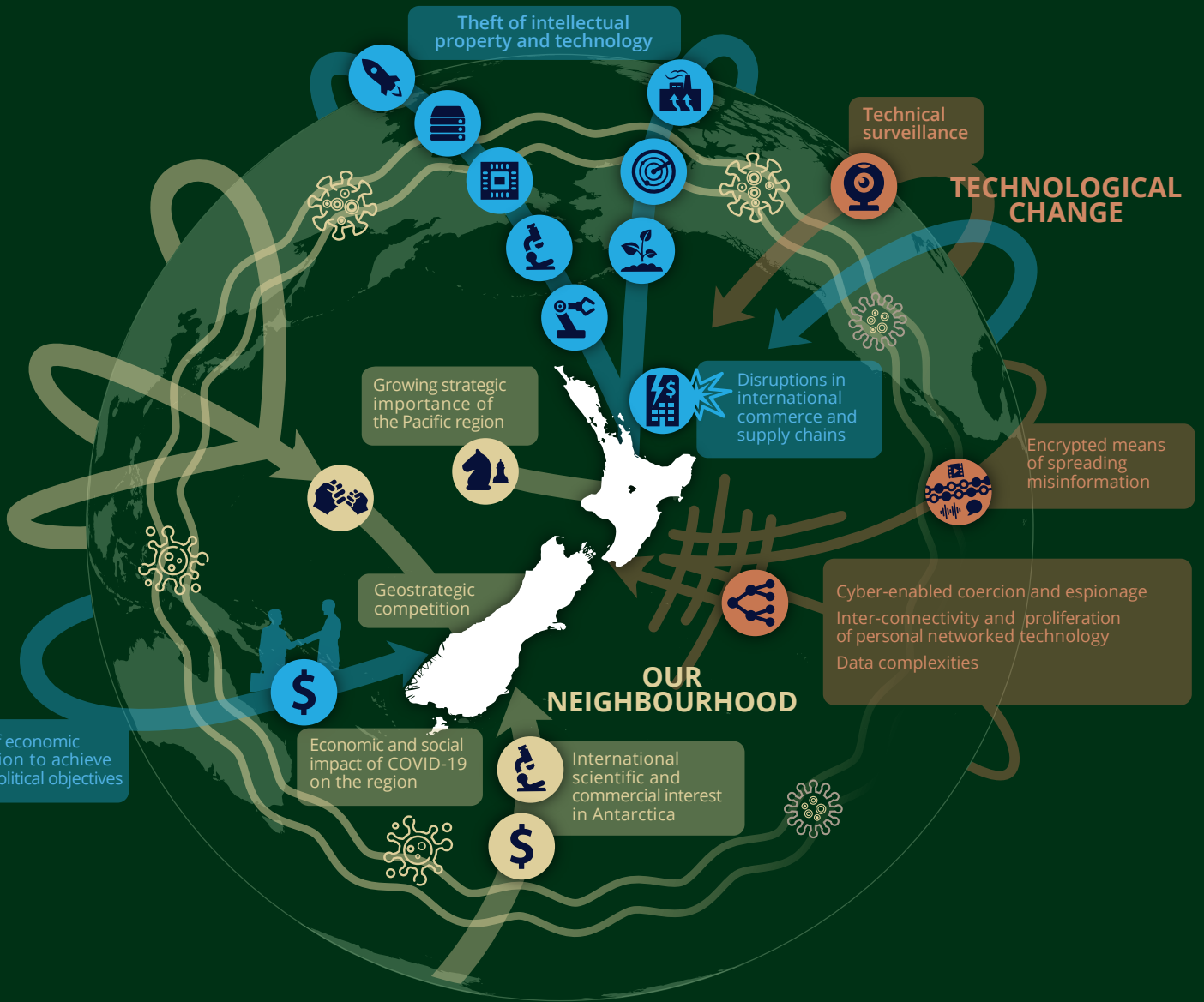
Growing strategic  
importance of  
the Pacific region

Geostrategic  
competition

International  
scientific and  
commercial interest  
in Antarctica

Economic and social  
impact of COVID-19  
on the region

Use of economic  
coercion to achieve  
geo-political objectives



## Foreign Interference

Interference by foreign states poses a threat to New Zealand's interests, including our sovereignty, democratic integrity, and social cohesion. Interference refers to acts by a state or its proxies that are intended to influence, disrupt, or subvert a New Zealand interest by covert, corruptive, deceptive, or threatening means. Normal diplomatic activity, lobbying, and other genuine, overt efforts to gain influence are not interference.

A small number of states engage in interference activities against New Zealand national interests. The NZSIS has observed indications of interference efforts targeting our political, academic, media and private sectors, and several of our ethnic communities.





# Investigating Espionage and Foreign Interference

## **The NZSIS works to detect, defend against and counter the threats posed by foreign intelligence services to New Zealand.**

This work includes understanding, investigating, and assessing the espionage and interference activities of foreign states, and the people working on their behalf, at home and abroad.

Our investigations and analysis seek to understand what particular actors are doing and to provide intelligence about those actors to decision-makers who can take action against the threat. NZSIS reporting has improved awareness and understanding across the New Zealand government, particularly on foreign interference, and provided valuable insights to inform decision-making.

Over the last 12 months the NZSIS has investigated and analysed the activities of individuals linked to a number of states that target New Zealand for espionage and interference. Investigative work is informed by a wide variety of sources, including strategic analysis of emerging trends and specific leads from NZSIS investigations, partner reporting, and community engagement.

### **How we understand and identify espionage and foreign interference threats**

In the last year, the NZSIS has been led by the Discover Strategy to detect and mitigate the wide array of methods foreign intelligence services use to target New Zealand's interests. This strategy allows us to focus on finding the right information at the right time, knowing our adversaries, and understanding where threats, risks, and vulnerabilities may appear.

The NZSIS produces an annual National Counter-intelligence Assessment. This assessment examines current and emerging threats to

New Zealand's national security, international relations, and economic wellbeing from the intelligence and security services of other states. The report contains assessments of how these threats may develop over the next 12 months, and is intended to provide decision-makers with the strategic insights necessary for planning and prioritising discovery efforts and other counter-intelligence responses.

The NZSIS works with New Zealand government partners and other stakeholders to make it harder for our adversaries to operate in New Zealand. Our aim is to disrupt their ability to interfere in our democracy, the academic and commercial sectors, and in New Zealand's communities.

Some state actors are skilled at finding weaknesses or "grey areas", which they exploit to covertly build and project influence. New Zealand's public, communities, media, and decision-makers play an important security awareness role by increasing public scrutiny and transparency over foreign state interference activities.

Societal interference is probably the most common form of interference in New Zealand, and the NZSIS continues to provide reporting on foreign states targeting members of New Zealand's ethnic communities. These activities include actors associated with foreign states monitoring individuals considered to be dissidents, and preventing communities from developing views deemed subversive by the foreign state. Foreign state interference activities cause some members of New Zealand's ethnic communities to feel less safe, secure, and free, thereby impacting their ability to exercise their freedom of speech and freedom of association.

## Case studies

### CASE STUDY 1:

The NZSIS has been conducting an investigation into a New Zealand-based individual who sought to facilitate the transfer of sensitive New Zealand technologies and intellectual property to a foreign state. The New Zealander, who had long-term relationships with individuals linked to a foreign state's military and intelligence services, facilitated access to New Zealand persons and information through legitimate business dealings. The industries and technologies involved would highly likely benefit the foreign state's military capabilities.

The NZSIS is currently satisfied that the activity has been disrupted and is working with New Zealand government agencies to mitigate remaining national security risks.

### CASE STUDY 2:

The NZSIS has been conducting an investigation into a New Zealand citizen who is assessed to be closely affiliated with a foreign state's intelligence services. The New Zealander is almost certainly collecting intelligence about New Zealand-based people for the purpose of monitoring members of communities whose views do not align with that of the foreign state. The individual uses various public and covert means to collect information on individuals, some of which is likely passed back to the foreign state's intelligence agency. The NZSIS is seeking to understand the nature of these activities and the interference threat posed by the individual against New Zealand.

The NZSIS has been working closely with New Zealand government agencies to manage and, where appropriate, mitigate the threat posed by this individual.

# 03

## **Protective Security Services**

Ngā Ratonga Tautiaki  
Whakahaumarū

The NZSIS delivers a full range of protective security functions to the NZIC and New Zealand. We are focussed on ensuring that New Zealand's institutions have the tools they need to manage their security and address any threats they may encounter.

This is achieved through effective security clearance management across the public sector, the provision of shared security services for the NZIC, the administration of the Protective Security Requirements (PSR) programme and counter-intelligence activities.

# Protecting People, Information, and Assets

## **Given the NZSIS's Protective Security Requirements and Government Protective Security Lead responsibilities, we strive to be protective security exemplars.**

Alongside the GCSB, we seek to continuously improve our protective security practices and ensure they remain up-to-date and fit-for-purpose. These efforts ensure New Zealand's most sensitive information, facilities, and assets are protected.

The NZSIS hosts the NZIC's Security Services Group (SSG), which provides protective security services to the NZSIS, the GCSB, and the National Security Group and National Assessments Bureau in the Department of the Prime Minister and Cabinet. The SSG's work includes undertaking internal security investigations, providing personnel, IT security and physical security advice across the NZIC, and ensuring internal security practices are fit-for-purpose.

### **Addressing the Risk of Insider Threats**

The NZSIS, via the SSG, has a specific responsibility to provide leadership on countering insider threats and personnel security functions across government.

An insider threat is any person who exploits, or intends to exploit, their legitimate access to an organisation's assets to harm the security of their organisation or New Zealand. This harm could be done either knowingly or unknowingly, through espionage, terrorism, unauthorised disclosure of information, or loss/degradation of a resource or capability.

Our work in this area includes establishing best practice for identifying and mitigating insider threats, and working with government agencies to prevent, mitigate, and respond to actual or potential insider threats.

### **NZIC Psychology Services**

The SSG also includes the NZIC Psychology Services team. This function was established to support the wellbeing of NZIC employees, and to ensure that those joining the intelligence community can manage the particular challenges of working in this unique environment.

The NZIC Psychology Services team also works to support the NZIC to help identify, manage the risks associated with, and achieve better outcomes for those people whose actions indicate they may be or could become an insider threat to the NZIC.

The NZIC Psychology Services team has a multi-disciplinary approach. The team provides NZIC agencies with access to expert advice, in-house psychometric screening, psychological interviews, wellbeing support services and psychological health risk assessment capabilities. Holding this range of expertise "in-house" ensures the NZIC leads in using psychological expertise to both support staff and to protect New Zealand's national security.

# Protective Security Requirements

**The PSR outlines 20 mandatory requirements, which provide a foundation for strong security practice. These requirements are divided into four areas: security governance, personnel security, information security, and physical security.**

The PSR team is continually reviewing and updating the framework and support mechanisms to ensure it remains best practice.

Since the PSR programme began in 2014, there has been a measurable increase in the mandated agencies' capabilities, and a positive shift in their risk understanding and security culture. The PSR framework continues to be adopted by agencies in the wider state sector as well as the private sector. It is a business enabler in an environment where there are increased needs for improved protective security practices.

In the coming year we will continue to deliver a number of security awareness campaigns through the PSR website at [www.protectivesecurity.govt.nz](http://www.protectivesecurity.govt.nz) that will be available for any organisation to use.

## Improving New Zealand's Foreign Interference Awareness

NZSIS investigations have directly informed public outreach with a variety of sectors about the threat of foreign interference and espionage. In the previous year, the NZSIS has focused on increasing engagement with political parties, members of Parliament, some mayors, and local government officials as we increase public awareness of the threat posed by hostile foreign states targeting New Zealand's democracy.

During the 2020/21 year, we have developed specific guidance to support the work of those elected to represent New Zealanders in democratic institutions. *The Espionage and Foreign Interference Threats – Security advice for members of the New Zealand Parliament and Locally Elected Representatives* guidance was launched and has been used across central and local government to help increase security awareness and to support increased security capability and resilience in our democracy and democratic institutions.

We have also extended our engagement with academic and research institutions, particularly universities and Crown Research Institutes. We have developed and launched *Trusted Research – Guidance for Institutions and Researchers* in collaboration with Science New Zealand and Universities New Zealand. The PSR framework has complemented this and has been used to support broader foreign interference awareness and capability building in this area. Our PSR advisors work closely with the sector's research leaders and security teams to provide support, according to their needs and risk profiles.

The Trusted Research work will continue in the coming year and we will develop more security risk management tools and advice to support institutions, organisations, and individuals working in these areas.



## COVID-19 and Foreign Interference

During 2020/21, in collaboration with the GCSB's National Cyber Security Centre (NCSC), we have provided protective security advice to the Ministry of Health and have supported them through workshops and other engagements to ensure that the COVID-19 vaccine programme incorporated protective security into its design and delivery.



# National Security Clearances

**The NZSIS has a statutory responsibility for administering the national security clearance vetting process. This role enables the NZSIS to support effective security across the public sector, by ensuring only those people who are suitable for handling sensitive information are in a position to do so.**

The NZSIS provides advice on whether or not a person is suitable for the clearance, or whether any risks need to be managed in order for them to hold a national security clearance. The process can include a deep look into a candidate's background, lifestyle, and any other relevant information. The chief executive of the requesting agency makes the final determination about granting a staff member a national security clearance.

## Total inventory levels of security clearances

There has been a 67% reduction in the total number of security clearance applications held by the NZSIS Vetting Team over the past two years. During this time, considerable business improvement activities have taken place in the Security Vetting Unit to enhance the way Confidential and Secret clearance applications are processed. The benefits of these business improvement activities have now been realised, with a dramatic reduction in the total number of applications, or 'inventory'<sup>2</sup>, for these two clearance levels.

The business improvement activity on Top Secret and Top Secret Special applications has more recently been completed, and the benefits of these improvements are starting to show. Further reductions in the Top Secret and Top Secret Special inventory are expected over 2021/22.

**TABLE 1: TOTAL INVENTORY OF NATIONAL SECURITY CLEARANCE APPLICATIONS**

	18/19	19/20	20/21
<b>Total inventory</b>	<b>3065</b>	<b>3264</b>	<b>1030</b>
Confidential	501	394	102
Secret	1623	1605	115
Top Secret	852	955	665
Top Secret Special	89	310	148

<sup>2</sup> Total inventory is the total number of security clearance applications held by the NZSIS Vetting Team. This number includes cases currently being worked on by Analysts and Officers, as well as applications waiting to be worked on.

## Total application time<sup>3</sup>

In 2020/21, the total application time for all four security clearance levels decreased significantly compared to the previous year. In June 2021, all standard<sup>4</sup> Confidential and Secret applications were received, processed, and completed in less than two weeks. This is a considerable reduction in total application time compared to 2019/20, during which a Secret application would take over six months to complete. The total application time for both Top Secret and Top Secret Special applications has also decreased by more than 50% in 2020/21.

**TABLE 2: TOTAL AVERAGE APPLICATION TIME**

	JULY 2020	JUNE 2021	% REDUCTION	TARGET TOTAL APPLICATION TIME
Confidential	34	6	82%	15 working days
Secret	115	5	96%	15 working days
Top Secret	183	74	60%	50 working days
Top Secret Special	113	54	52%	60 workings days

## Key Performance Indicator (KPI) – Timeliness

**TABLE 3: TIMELINESS TARGETS**

	TIMELINESS KPI TARGET
Confidential	80% of applications completed in 15 working days
Secret	80% of applications completed in 15 working days
Top Secret	80% of applications completed in 50 working days
Top Secret Special	80% of applications completed in 60 workings days

To achieve our timeliness KPI targets, the total application time must be below the targets outlined in Table 3. Although the targets for Confidential, Secret, and Top Secret Special were achieved in June 2021 (see Table 2), the improvements were made over the course of the performance year and so the average timeliness across the full performance year was not achieved.

Despite not achieving our timeliness KPI targets across all four clearance levels, there has been an increase in the percentage of applications that met the KPI (see Table 4).

3 Total Application Time is the total time taken to complete an application from when it is received to when a recommendation is issued. This includes the time a case is unassigned and the processing time. This is measured in the average number of working days.

4 'Standard' applications make up between 85-90% of all CV and SVs received. The remaining 10-15% of applications are escalated for more in-depth enquiries and therefore fall outside of the Government KPI, which only measures the 'standard' applications processed.

**TABLE 4: COMPARISON OF TIMELINESS KPI RESULTS**

	2017/18	2018/19	2019/20	2020/21
Confidential	12%	7%	9%	66%
Secret	17%	11%	1%	46%
Top Secret	20%	24%	11%	23%
Top Secret Special	39%	54%	37%	65%

The timeliness results for Confidential and Secret clearances dramatically improved in the last quarter of the 2020/21 year, when the total application time reduced below the timeliness targets (see Table 2) and the number of unassigned applications also reduced significantly (see Table 7).

The timeliness KPI for Confidential applications has been consistently exceeded since February 2021, and Secret applications since March 2021(see Table 5). This trend provides assurance that in 2021/22 our timeliness KPI targets will be achieved in the Confidential and Secret clearance level.

**TABLE 5: TIMELINESS RESULTS FOR CONFIDENTIAL AND SECRET APPLICATIONS OVER 2020/21**

	JUL 2020	AUG 2020	SEPT 2020	OCT 2020	NOV 2020	DEC 2020
Confidential	80%	3%	7%	19%	60%	78%
Secret	100%	20%	0%	0%	12%	3%
	JAN 2021	FEB 2021	MAR 2021	APR 2021	MAY 2021	JUN 2021
Confidential	67%	91%	99%	100%	100%	100%
Secret	1%	7%	87%	99%	100%	100%

Although the timeliness results for Top Secret and Top Secret Special continue to be below the expected targets, there is a strong indication that the timeliness target for Top Secret Special will be achieved early in the 2021/22 year (see Table 2), and the timeliness target for Top Secret will be achieved by late 2021/22.

## Key Performance Indicator – Unassigned application queue

In 2020/21, the Security Vetting Unit was able to achieve three out of four of the unassigned queue targets. The numbers of unassigned Confidential, Secret, and Top Secret Special applications were all lower than the KPI targets. This marks the first time that any KPIs have been met by the Security Vetting Unit and is a major milestone. Top Secret is the only remaining unassigned queue, and we will eliminate this in the next 12 months.

**TABLE 6: COMPARISON OF UNASSIGNED APPLICATIONS TARGET TO ACTUAL NUMBER**

	UNASSIGNED APPLICATION TARGET – JUNE 2021	UNASSIGNED APPLICATIONS ACTUAL NUMBER – JUNE 2021
Confidential	150	30
Secret	350	21
Top Secret	250	441
Top Secret Special	110	85

A key highlight for this year has been the reduction in the unassigned Secret applications. In July 2020 there were 713 unassigned Secret clearance applications. By June 2021 this number reduced by 692 to only 21 unassigned Secret applications, a reduction of 97%.

**TABLE 7: COMPARISON OF THE NUMBER OF UNASSIGNED APPLICATIONS FROM JULY 2020 TO JUNE 2021**

	JUL 2020	JUN 2021	% REDUCTION
Confidential	284	30	89%
Secret	713	21	97%
Top Secret	713	441	38%
Top Secret Special	287	85	70%



## Age of the oldest unassigned case

Throughout 2020/21, the age of applications in the unassigned queue<sup>5</sup> has reduced significantly. In July 2020, the age of the oldest unassigned application in three of the clearance levels was over 100 working days, two of these being over 220 working days (this equals more than one calendar year).

In June 2021, the oldest Confidential and Secret clearance application has an unassigned age of less than two weeks. Although the oldest unassigned Top Secret and Top Secret Special application is still higher than desired, both levels have decreased by 100 working days in 2020/21.

**TABLE 8: COMPARISON OF THE AGE OF THE OLDEST UNASSIGNED APPLICATION FROM JULY 2020 TO JUNE 2021**

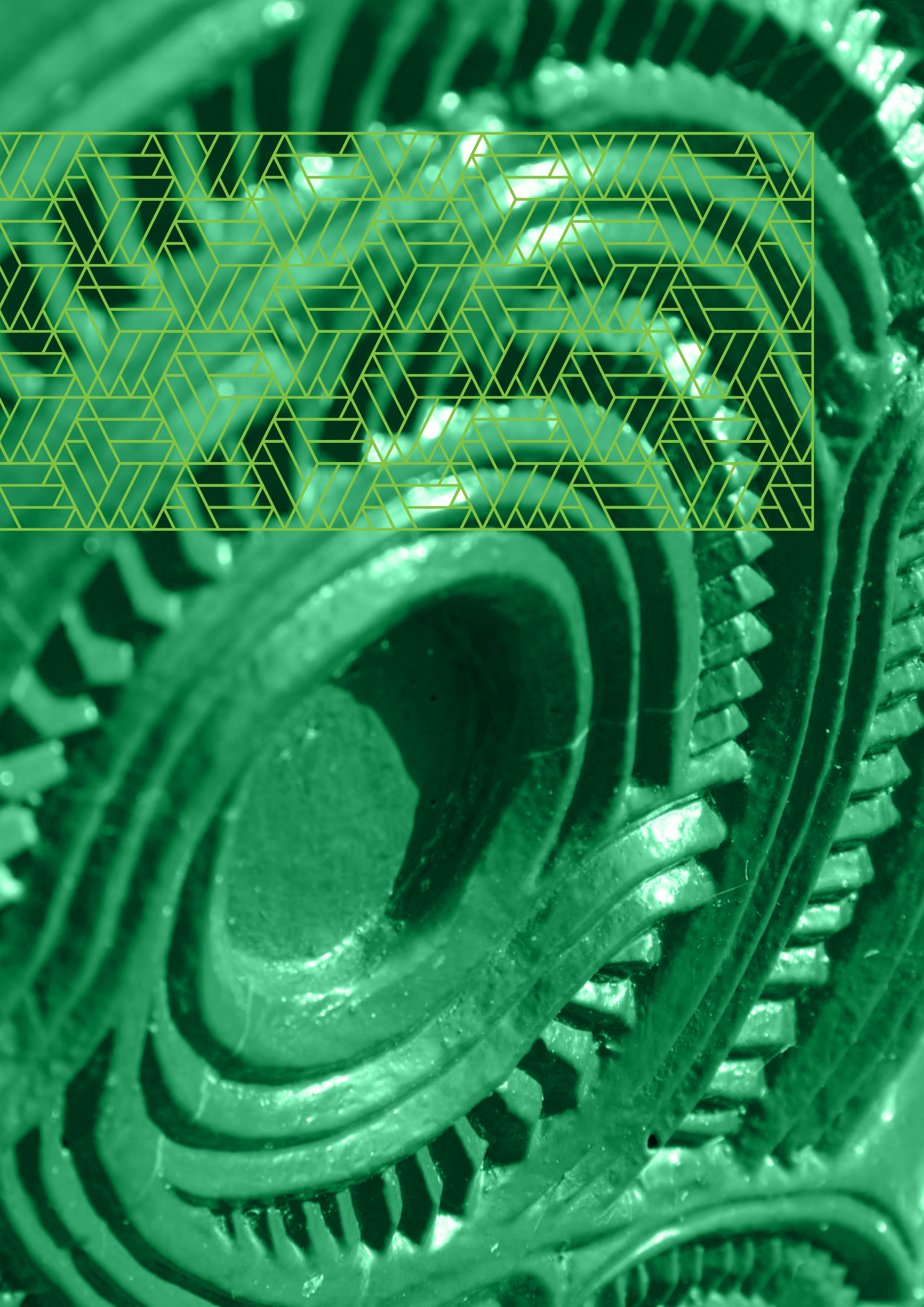
	JULY 2020	JUNE 2021	% REDUCTION
Confidential	40	6	85%
Secret	135	4	97%
Top Secret	270	168	38%
Top Secret Special	246	146	41%

## Tiaki – the new Security Vetting system

Over the last two years, work has been underway to design and develop a new Security Vetting Management system – Tiaki. The new system is designed for customers to use when applying for a national security clearance and for agencies to manage their security clearance holders. More than 20,000 individual customers and referees, and more than 50 government agencies will use the new system.

Tiaki will ensure that accurate, necessary, and relevant information is provided to the NZSIS to assess a person’s suitability to hold a New Zealand national security clearance. The system will both modernise the information the NZSIS receives and significantly improve the experience customers have when applying for a security clearance.

<sup>5</sup> A security clearance application waiting to be processed has been received by the NZSIS but no work has started on the application. It is sitting in the queue waiting to be assigned to a staff member.



# 04

## **National Security Risk Advice**

### Ngā Tohutohu Tūraru Whakahaumarū ā-Motu

The NZSIS provides National Security Risk Advice to New Zealand government agencies in order to inform their decision-making.

Individuals seeking access to sensitive information or assets, or a location where these assets may be secured, and individuals seeking physical entry to New Zealand are assessed to understand their relevance to national security. The NZSIS assesses these individuals against a range of national security harms including terrorism, espionage, and foreign interference. Although visa screening reduced over the past year due to COVID-19 border restrictions, the NZSIS continues to provide a broad range of security risk advice to New Zealand government agencies.

# Security Screening

**The NZSIS supports border security agencies to maintain the integrity of New Zealand’s border. Each year we screen the details of thousands of individuals before those travellers enter the country.**

The NZSIS seeks to identify travellers with links to international extremist groups, espionage activities, or the proliferation of weapons of mass destruction. This process enables New Zealand’s border protection agencies to prevent people who may pose a risk to national security from entering the country.

In March 2020, the New Zealand Government put in place border restrictions in response to the COVID-19 pandemic. Due to the ongoing nature of the pandemic these restrictions remain largely in place, and this has significantly reduced the number of visa applications, specifically temporary visas, being screened. The NZSIS continues to closely

monitor the border to ensure any possible national security threats are identified and mitigated. We note, however, that while the border is closed to the majority of foreign travellers, the likelihood of a threat presenting through travel movements is much less.

The NZSIS has a statutory responsibility under the Citizenship Act 1977 and the Civil Aviation Act 1990 to screen individuals applying for citizenship and individuals seeking access to secure airport environments. The NZSIS has maintained this function throughout the ongoing impacts of the pandemic, though we note the demand for this service has decreased due to border restrictions.

# Overseas Investment Assessments

## **In May 2020, the Overseas Investment Act 2005 was amended by the Overseas Investment (COVID-19 Emergency Measures) Amendment Act 2020 to address heightened risks associated with foreign investment in the context of COVID-19.**

This Emergency Notification Regime (ENR) endured over the reporting period. Under the ENR, the NZSIS has a role in supporting the Overseas Investment Office by providing national security screening services and advice on proposed transactions that may pose significant national security risk. In performing this work, the NZSIS uses the Cabinet endorsed non-exhaustive set of risk factors as guiding principles. Specifically, the NZSIS provides national security risk advice to inform the Overseas Investment Office on:

- Whether the foreign actor has access to sensitive information or information that may be used to exploit or advance their strategic position;
- Whether the investment increases the foreign actor's ability to influence social or political spheres;
- Whether the investment would undermine New Zealand's national security;
- Whether the investment would give the foreign actor the ability to disrupt domestic supply chains to weaken New Zealand's economic well-being and security; and
- Whether the investment would increase the foreign actor's access to other means of influence.



# Countering the Proliferation of Weapons of Mass Destruction Technology

## **The proliferation of Weapons of Mass Destruction (WMD), including nuclear, chemical and biological weapons, is a significant threat globally.**

The NZSIS supports New Zealand's efforts to counter this threat by ensuring we do not contribute to the transfer of knowledge or expertise that could be used in WMD programmes.

New Zealand has no industry directly related to WMD production, but we are technologically capable in a number of areas with dual use potential. Some examples include the development of our space industry, biotechnology research, and drone technology. The technology being developed may be attractive to those seeking to acquire it for unethical purposes.

The NZSIS provides advice to Immigration New Zealand in relation to the transfer of knowledge or expertise that could be used in WMD programmes. Individuals meeting certain criteria are subject to NZSIS national security screening.

Student visa applicants that may present a risk to New Zealand have declined following the ongoing closure of New Zealand's borders due to COVID-19.

## Space and High-altitude Activity Assessments

### **New Zealand's space industry provides significant economic opportunities for New Zealand.**

New Zealand provides a uniquely beneficial environment for space-related activities. Our uncluttered air space provides multiple launch windows. We also have a modern legislative environment that allows for a safe, sustainable, and thriving space industry.

The Outer Space and High-altitude Activities Act (OSHAA) 2017 provides a regulatory framework to manage any risks to New Zealand's national security and interests.

A core role for the NZSIS and the GCSB is to undertake national security threat assessments for all activities licensed or permitted under OSHAA and provide national security risk

advice on outer space and high-altitude activities to the Minister Responsible for the NZSIS and the GCSB. For activities governed by the Act, this national security risk advice is used to inform the Ministerial-level consultation required by the Act.

The space industry in New Zealand continues to gain significant interest from overseas partners, including Rocket Lab's launch activities in Mahia.

In 2020/21, the NZSIS undertook 18 security assessments on space-related activities.

# 05

## **Protecting Regional Security**

Te Tautiaki

Whakahaumarū ā-Rohe

Despite our relative geographic isolation, our region experiences the same trends that shape the global security environment. These trends manifest in New Zealand's domain and throughout the Pacific as a diverse array of security challenges.

The global nature of modern national security threats and New Zealand's unprecedented connectedness to the world will invariably see global trends become domestic issues. Our international intelligence and security partnerships provide us with insights on global trends and developments, which increasingly stand to affect our country and the region we share.

# Contributions to Pacific Regional Security

**New Zealand's national security is intrinsically linked to the security and prosperity of the region we share with our Pacific Island partners. The NZSIS has a clear role to play in achieving the outcomes sought under the Government's Pacific Reset objectives, and the undertakings of the Boe Declaration.**

Our role is to work with our Pacific counterparts to support a stable Pacific region, and work with Pacific leaders in the protection of our shared fundamental values of democracy, human rights, and the rule of law.

The NZSIS informs wider New Zealand Government efforts to keep the region safe and secure. When working in the Pacific, the NZSIS liaises with other New Zealand agencies.



# Contributions to International Security

## **The NZSIS's international relationships enable New Zealand to have far greater visibility of risks to its own national security interests through access to global sources of high-quality intelligence.**

These relationships also allow us to provide partners with our own unique and valuable contribution to the common picture of regional and global trends.

The NZSIS's relationships with the Five Eyes network of partners are vital to our ongoing ability to deliver positive security and intelligence outcomes for New Zealand.

Strong relationships outside of the Five Eyes are also important. Our relationships with a range of security and intelligence partners in Europe, Scandinavia, Asia, and the Pacific are increasingly significant to the NZSIS and New Zealand, and will continue to grow in importance.

COVID-19 has impacted our ability to engage with overseas partners physically as international travel is currently extremely limited. The NZSIS has maintained our international relationships despite this challenge through secure video conferencing technology.

Our international partners share our belief that COVID-19 and its associated challenges demand a collaborative and joined up approach, so our international relationships remain as important as ever.

## International Liaison

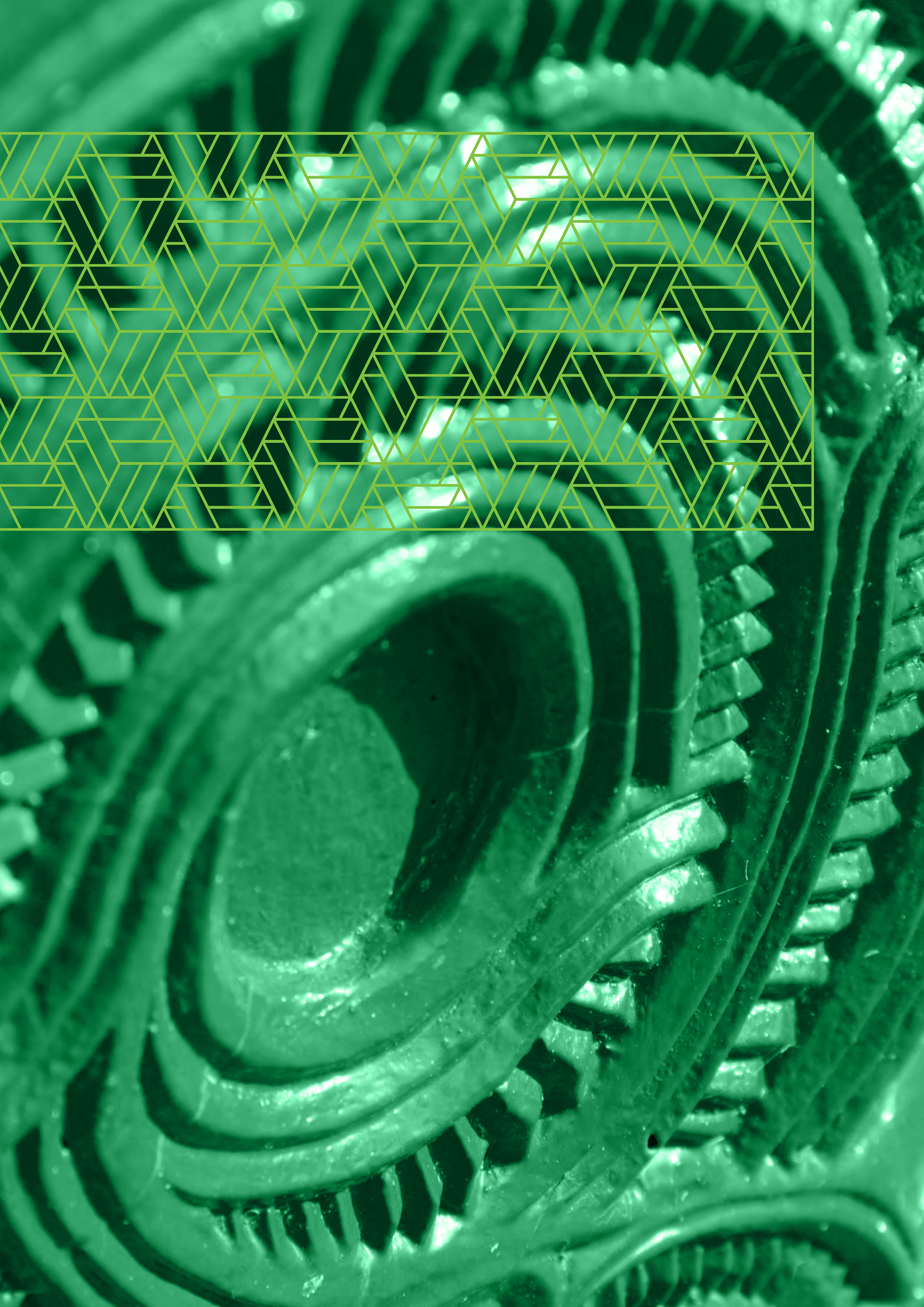
### **The NZSIS has a small network of Security Liaison Officers (SLOs) who are posted overseas to engage with key international partner governments and agencies.**

SLOs represent the interests of the NZSIS and are a conduit for requests for information sharing, joint training, and other forms of cooperation.

The NZSIS SLOs work closely with other New Zealand government staff in their respective countries, particularly those

with national security and intelligence responsibilities. The SLO network assists the NZSIS to develop and maintain strong relationships with international partners, which in turn are instrumental in helping New Zealand protect its borders and support the safety and wellbeing of New Zealanders at home and overseas.







# 06

## **Organisational Capability**

### Ngā Āheitanga Whakahaere

The NZSIS is committed to ensuring it can continue to meet the security and intelligence needs of the New Zealand Government and public.

To this end, the NZSIS devotes considerable effort to developing cutting edge capabilities, enhancing the capabilities that we already have, and ensuring that our staff have the training and resources they need to succeed in their roles. The NZSIS also works to ensure that our systems, policies, and processes are fit-for-purpose.

## Data and Information

One of the challenges facing the NZSIS is to maximise our ability to access, manage, and use data and information effectively to identify those who intend harm to New Zealand and New Zealanders. We need to reduce the time and effort our people spend on low value work, enhance our ability to prioritise, remove duplication or waste, and automate where it makes sense.

To address this challenge, the NZSIS has embarked on a Data Transformation Programme to help deliver on our Discover Strategy and to transform the way our people access and work with data to keep New Zealand safe in a modern digital environment.

While the programme is a long-term initiative, foundational work has progressed on data ethics, information management policy and practice, workforce competencies, and public understanding.

## Operational Training

The continued success of the Investigator and Case Officer foundation courses in 2019/20 allowed the Operational Training Team to broaden its focus in the 2020/21 year. Achievements of note included supporting increased workforce flexibility through the Intelligence Analyst programme as well as expanding the training focus into roles within Protective Security. The Operational Training Strategy continues to drive future effort; maintaining a focus on the right people getting the right training at the right time.

# 07

## **Our People**

### Ō Mātau Tāngata

Over the past five years, a number of initiatives have been underway to increase the diversity and inclusiveness of our organisation.



# Our People

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

## **Retain, develop, and recruit the best people**

In October 2020, we launched a recruitment campaign to raise awareness of who we are, the career opportunities available at the NZSIS and GCSB, 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 needed to better promote ourselves including the work we do, the range of career opportunities available, and our strong focus on creating a diverse and inclusive work environment.

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

## **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 two cohorts of tier 4 and 5 leaders. The programme consists of six full-day workshops, one half-day workshop, seven online modules and three peer coaching sessions. Topics include Leadership, Strategic Execution, Leading Change and Resilience, Teamwork and Collaboration, and Decision-Making in Complexity and Ambiguity.

## Retaining talent

Retaining top talent is vital, particularly in light of the unique and challenging environment that NZIC staff operate in, and the time involved in recruiting, vetting, and training suitable people.

In July 2020, 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. There are six focus areas:

- **Leadership:** our leaders will be at the forefront of retention.
- **Culture:** we will have a workplace where everyone is included and valued for their contribution.
- **Career development:** everyone will get development opportunities that align with their career aspirations.
- **Job satisfaction:** employees will have clear role expectations and be satisfied with the work they do.
- **Pay and benefits:** we recognise the talent and commitment of our employees by providing a competitive employment package.
- **Data:** our data will provide the insights we need to enhance our retention initiatives.

The NZSIS supports staff retention through providing significant investment in learning and development and a clear view of career pathways where appropriate. We continue to work with Victoria University, the Combined Legal Agencies, Massey University Research Network, New Zealand Police, and the New Zealand Defence Force to provide unique and engaging learning experiences. We also work with several independent training providers to develop learning opportunities that are especially relevant to the intelligence community.

Another way we recognise, reward, and retain our talented staff is through our Long Service Recognition programme and the Exceptional Achievement Awards, which were established for the first time 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. The awards will occur on an annual basis, and there are six award categories:

- Operational or mission-based excellence (including mission enablement)
- Exemplifying our values
- Collaboration (within our agency, NZIC, with other New Zealand government agencies or international partners)
- Innovation
- New talent (anyone within their first three years of service with the NZIC)
- Leadership (up to and including Level 3 line managers).

Our turnover has increased by 0.2% this year, however remains relatively static since FY 2018/19.

**TABLE 1: (U) NZSIS ANNUAL STAFF CORE TURNOVER**

	2015/16	2016/17	2017/18	2018/19	2019/20	2020/21
NZSIS	9.6%	11.5%	10.3%	12.1%	12.3%	12.5%
Public sector	11.1%	11.5%	12.1%	11.8%	10.1%	tbc



# Diversity in the workforce

**New Zealand faces a rapidly changing and challenging security outlook, and threats to New Zealand's national security will continue to intensify. To succeed against these threats 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 GCSB in March 2018, we focused on two priority areas – increasing representation of women, and ethnic diversity at all levels of our workforce. To support this, we delivered a range of D&I initiatives across attraction, leadership, inclusion, and reporting of D&I data.

At the end of June 2021 we have achieved 46% of female representation across the workforce, just below our goal of 47%. We increased our ethnic diversity to 18.4%, achieving our goal of 13.1%. This shows we have made some great progress, but we know we still have a long way to go.

In July 2021 our refreshed D&I Strategy 2021-2025 will be launched. Through our refreshed strategy we will learn from our successes, sustain the good work we have done, and look for additional ways to increase diversity in all areas. We are committed to:

- A continued focus on increasing our gender representation and ethnic diversity at all levels of the NZIC
- Placing more emphasis on inclusive work practices to ensure we can attract and retain our diversity
- Building on our existing initiatives to further develop our D&I capability.

## D&I embedded in our performance framework

To further cement our commitment to building a diverse and inclusive workplace, the NZSIS 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 NZSIS to recognise the contribution individuals make to develop a diverse, inclusive, and healthy workplace culture.

## Gender diversity

Women currently make up almost half of the NZSIS's workforce and over a third of our senior management group. In our 2017-2020 D&I strategy, we set ourselves an aspiration of increasing overall representation of women by 1% each year for a total of 3% over three years. We've achieved this target with a 3.6% increase in overall representation of women (to 46%), and 5.5% increase in representation of women in senior leadership roles (to 38.5%) over the past three years.

While we achieved our overall representation goal last year, our representation of women has reduced by 1.4% this year. We have increased representation of women in senior leadership roles by 13.5% over the past 12 months, resulting in a total improvement of 14.5% since 2015.

**TABLE 3: GENDER DIVERSITY WITHIN THE NZSIS**

	2015/16	2016/17	2017/18	2018/19	2019/20	2020/21
Overall Male	59.4%	56.7%	57.6%	53.3%	52.6%	52.5%
Overall Female	40.6%	43.3%	42.4%	46.7%	47.4%	46.0%
Undisclosed	-	-	-	-	-	1.5%
	2015/16	2016/17	2017/18	2018/19	2019/20	2020/21
Senior Leaders Male	76.0%	67.0%	67.0%	69.0%	75.0%	61.5%
Senior Leaders Female	24.0%	33.0%	33.0%	31.0%	25.0%	38.5%

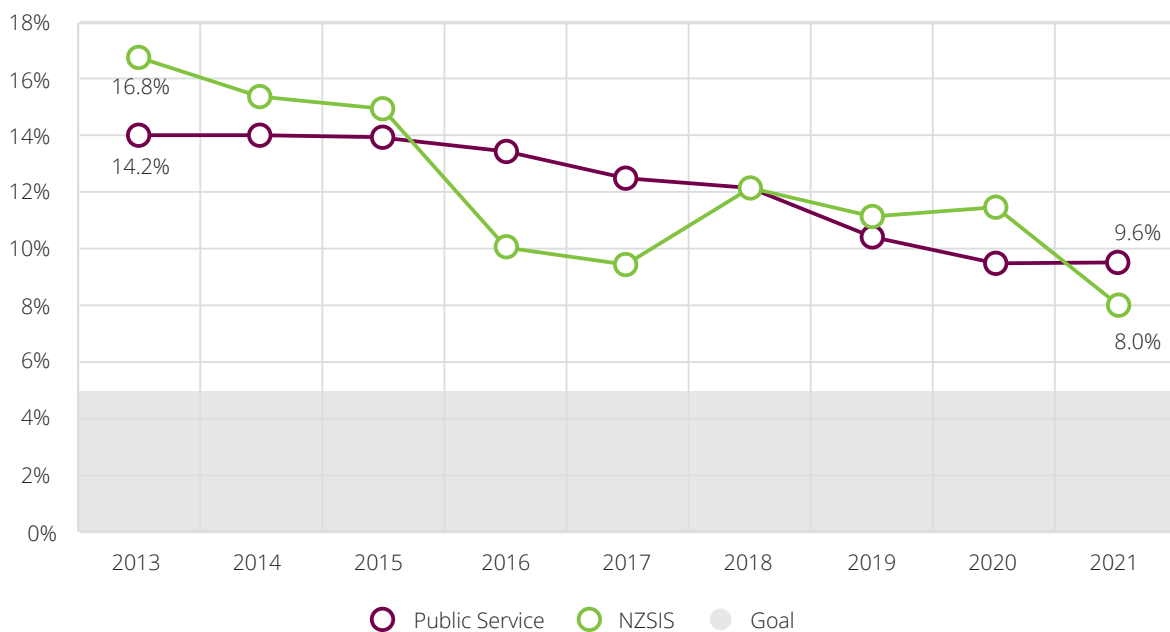
*This is the first year that we have had staff with undisclosed genders, and as such have included them in our reporting.*

## Closing the Gender Pay Gap

The NZSIS has addressed its like-for-like gender pay gap through successive remuneration rounds. This means men and women who have been in the same roles for the same amount of time and who are performing at the same level are paid equally. We will continue to monitor the like-for-like gender pay gap to ensure staff remuneration remains equitable.

Our target was to reduce the NZSIS's whole-of-organisation average gender pay gap to a maximum of 5% by 2021. The gender pay gap has significantly decreased this year, by 3.5%. While we have not reached our target, this is the closest we have been. At June 30 2021, the gender pay gap was 8%.

**GRAPH: GENDER PAY GAP (AS AT 30 JUNE)**



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

A significant contributor to the gender pay gap is lower representation of women in team leader roles and senior technical expert cohorts.

As a career service, the capabilities and experience required are not readily available to us via the external market. The best way for the NZSIS to continue closing the gender pay gap is through the recruitment and development of women who remain with the NZSIS and progress into technical expert and leadership roles. The NZSIS recognises that this will take time and remains committed to working with staff associations and network groups to meet these goals.

We are seeing more female staff being employed and/or promoted to more senior roles within the agency. This is having a positive impact on reducing our gender pay gap (as evidenced in Table 3).

## Gender Pay Gap Action Plan

Our Gender Pay Gap Action Plan incorporates the four core milestones from the Public Service Commission:

- 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, significant progress towards these goals. Our gender pay gap is declining, as at 30 June 2021 we have improved representation of women in senior leadership (38.5%), 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

Our ethnic representation has significantly improved this year. Additionally, around 65% of our ethnically diverse staff have started within the last four years, showing the impact of our focus on diversity and inclusion.

**TABLE 2: ETHNIC DIVERSITY WITHIN THE NZSIS**

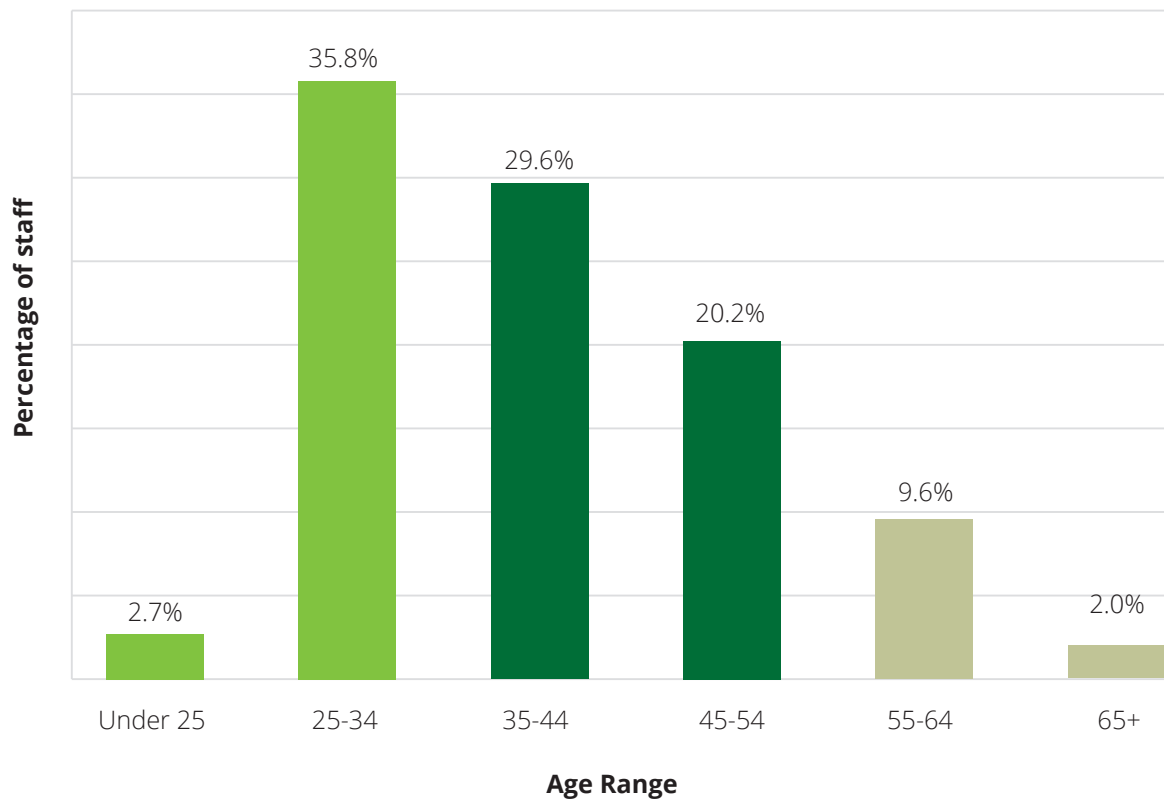
	2015/16	2016/17	2017/18	2018/19	2019/20	2020/21
New Zealand European & European	59.6%	65.1%	65.0%	71.2%	73.1%	81.1%
New Zealander	-	-	28.4%	27.5%	25.2%	20.7%
Māori	6.9%	6.7%	6.5%	5.1%	6.8%	6.1%
Asian	4.6%	5.1%	6.5%	5.7%	5.1%	5.6%
Pasifika	1.5%	1.9%	2.6%	2.8%	3.7%	4.1%
Middle Eastern, Latin American, & African	-	1.1%	2.0%	1.6%	1.4%	2.3%
Other	-	0.4%	0.3%	0.3%	0.3%	0.3%

*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 of people who have provided an ethnic group. Employees may select more than one ethnic group, and are counted as part of each group they identify with. Metrics are taken as at 30 June of the relevant year. Not presented in the 2015/16 and 2016/17 years are staff who identified as New Zealander. This group was reported on for the first time in 2017/18.*

## Age demographics

The average age of our workforce is 40. The majority of our workforce (68%) are under 45, and of this group 65% have been with us for less than four years. This reflects both our investment in capability uplift and our emphasis on recruiting a diverse workforce.

**GRAPH: AGE DEMOGRAPHICS IN NZSIS 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. These activities include online and face-to-face experiences that we expect our people to engage in over the next couple of years. 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
- analyse gender and ethnicity data 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 or organisational values.

Our Understanding and Managing Unconscious Bias learning is now available online.

Seventy-three percent 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 the Selection Process training before serving on recruitment panels.

### Cultural competence

Developing a strategic approach to Māori cultural capability for the NZSIS and GCSB 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 NZSIS and GCSB 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.

Work is underway to source a suitable Māori Capability Advisor to help lead this work. This new role will enable a strategic and structured approach to developing Māori cultural capability across the NZIC. In the first instance this role will review and progress

recommendations identified via our internal maturity assessment against Te Arawhiti's organisational capability maturity model. The role will report directly to the Directors-General of the NZSIS and GCSB, and will provide leadership and advice on matters pertaining to te ao and tikanga Māori across the NZIC.

As we design our programme and source the capability to support our journey, we continue to build our Māori cultural competency through te reo Māori training and our highly regarded Crown Māori Relations programme for leaders. Since the initial delivery of this programme in late 2020, over 38% of our leaders have completed this programme. More offerings are scheduled for 2021/22.

## Inclusive leadership

The NZSIS 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, a range of Leadership Development Centre (LDC) programmes, and other externally-provided offerings.

In our refreshed D&I Strategy 2021-2025 we have an objective that is specifically focused on "enabling our leaders to practise inclusive leadership". Although this objective is focused on leadership, we believe leading inclusivity is the responsibility of all staff, and our range of D&I learning opportunities reflect this.

Within the leaders' component of our D&I learning programme there are offerings that encourage inclusive leadership. They include managing unconscious bias, anti-bullying and undesirable behaviour, bystander awareness and intervention, LGBTI+, Crown-Māori relations, and te reo Māori training.

During 2020/2021 28 programmes have been delivered covering the topics mentioned above. Just over 79% of our staff have participated in at least one of these programmes in the past 12 months beyond those already available.

All staff have access to view and register for the range of opportunities through our learning management system Ako. The NZSIS will continue to develop the range of opportunities to support learning and development across the signature traits<sup>6</sup> of inclusive leadership.

## 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.

All staff networks are supported on a bi-monthly basis through our D&I Working Group chaired by our Chief People Officer, and our D&I Advocacy Group co-chaired by our Directors-General. Through both forums, staff networks have the ability to drive their D&I agenda at the very top of the NZIC, with direct support from the Chief People Officer, and our Directors-General.

In our refreshed D&I Strategy 2021-2025 one of our objectives is to "enhance the role of staff networks as advocates for change, and driving the D&I agenda". We have also committed to empowering and enabling our staff networks to lead the celebration of D&I events.

<sup>6</sup> Bernadette Dillon & Juliet Bourke, *The six signature traits of inclusive leadership*. Deloitte University Press, 2016.

# Supporting inclusion in the NZSIS

## The NZSIS undertakes a number of initiatives to enhance diversity and inclusion across the organisation.

### Rainbow inclusion

In early 2019, Standing Out @ the NZIC – our Rainbow network – was established. In July 2019 we were accredited with the Rainbow Tick, and one of the recommendations from this exercise was the need for resources that support transgender and transitioning staff.

In 2020, we created a set of Transitioning Guidelines for staff and managers, and a brochure that 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.

We entered multiple categories at the 2020 Rainbow Excellence Awards. We were encouraged to see we were on the right track when we 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.

### Engagement with our people

We place a strong emphasis on engaging with staff to understand what matters most to them. We do this through a range of channels: employee surveys, staff network groups, internal research, and workshops.

In 2019, we carried out internal research into the experiences of women in the workplace. In 2020 we then co-designed a number of solutions with staff, resulting in a two-year programme of work. Over the past 12 months we have implemented a range of initiatives across culture, leadership, career development, and flexibility. This programme of work will continue over the next 12 months, and is focused on improving the overall experience for women in the NZSIS and GCSB.

# Talent outreach and engagement

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

Our activities within this strategy are designed to help us:

- recruit more women, ethnically diverse, neuro-diverse, and disabled candidates
- demystify or alleviate security clearance concerns potential candidates may have
- build enduring partnerships with key producers, channels, and champions of talent; and
- socialise and strengthen community understanding of our mission.

The Talent Outreach and Engagement strategy includes establishing graduate and scholarship offerings within the NZSIS to complement existing graduate programmes within the NZIC (Ethnic Community Graduate Programme and GCSB Women in STEM Scholarship and Graduate Programmes).

# 08

## **Accountability and Transparency**

Te Noho Here me  
te Pūataata

Having the trust and confidence of the Government, the general public, and domestic and international partner agencies is an essential element of the ongoing success of the NZSIS.

To earn this confidence, the NZSIS works hard to build positive engagement with our partners, proactively engages with our oversight bodies, and tries to be as transparent as possible with the New Zealand public.



# Engagement and Transparency

## Domestic partnerships

Since the Intelligence and Security Act 2017 came into force, the NZSIS has been able to work more closely with domestic agencies. Over the past few years, the NZSIS has worked to build effective collaboration with New Zealand's law enforcement and defence agencies. The GCSB and the New Zealand Police, in particular, are key partners for the NZSIS. The NZSIS also commonly engages with the Ministry of Foreign Affairs and Trade, the New Zealand Defence Force, and border agencies such as Immigration New Zealand and the New Zealand Customs Service.

The NZSIS provides assistance and advice to these agencies in matters relating to national security, and assists with the protection of New Zealanders overseas. Our work entails contributing to relevant cross-agency Cabinet decisions, conducting joint operational work, sharing specialist capabilities to ensure other agencies can perform their roles and functions, and undertaking joint operational training initiatives.

## Information requests

Each year, the NZSIS receives a range of information requests under the Official Information Act 1982 and Privacy Act 2020.

The NZSIS aims to be as open as possible about our work, while ensuring there is no risk of compromise to national security. In the last year we experienced close to a 23% increase in the number of information requests we received. Many of the requests were for information covered in the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019, and we endeavoured to release as much information as possible, including the Arotake internal review<sup>7</sup>, and numerous intelligence reports about counter-terrorism in the years leading up to the Christchurch attack.

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

- Completed 81 OIA requests. All requests were completed within the legislated timeframe.
- Completed 86 Privacy Act Requests. All requests were completed within the legislated timeframe.

<sup>7</sup> The Arotake report was a review into NZSIS processes and decision-making in the lead-up to the 15 March attack in Christchurch.

**TABLE 5: NUMBER OF INFORMATION REQUESTS COMPLETED, 2016–2021**

TYPE OF REQUEST	2016/17	2017/18	2018/19	2019/20	2020/21
Official Information Act	83	72	84	62	81
Privacy Act	63	49	66	74	86
Total	146	121	150	136	167

During the year, four complaints were made to the Office of the Ombudsman regarding the NZSIS's OIA responses. Two complaints were resolved in the NZSIS's favour, while the remaining two are still being considered.

One complaint was raised with the Office of the Privacy Commissioner during the reporting year. The Privacy Commissioner found in the NZSIS's favour.

### Compliance systems

An essential component of retaining the trust and confidence of the Government and the public is having robust processes in place to ensure the NZSIS complies with the law at all times. The NZSIS has intrusive powers and access to sensitive information. We have

a responsibility to ensure that we use our powers and access in a manner that is lawful, necessary, and proportionate.

To ensure that our staff use our powers in this way, the NZSIS has a compliance framework and runs a regular programme of audits and reviews. We encourage a culture of self-reporting of compliance incidents, which are reported to the Inspector-General of Intelligence and Security (IGIS). These incidents often highlight improvements required to systems and processes, which are then addressed.

The NZSIS Compliance team manages a compliance training framework that ensures all staff receive training on their compliance obligations every year.

# Oversight

**The NZSIS has its own internal processes to ensure legal compliance, and takes compliance very seriously. In addition, several external bodies provide oversight to the intelligence agencies, including the NZSIS.**

## **The Intelligence and Security Committee**

The Intelligence and Security Committee (ISC) is a parliamentary body. It looks at the intelligence and security agencies and examines the policy, administration, and expenditure of each organisation.

The ISC has seven members, comprising 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 Office of the Inspector-General of Intelligence and Security (IGIS) is the key oversight body of the NZIC. It is an important mechanism to provide independent assurance that the agencies are acting within the law and with propriety. The Office of the IGIS also independently investigates complaints relating to the activities of the NZSIS made by members of the public and reviews all authorisations issued.

The NZSIS has ongoing engagement with staff from the Office of the IGIS (at varying levels) relating to compliance issues, and also provides information and resources in support of IGIS investigations and queries.

The NZSIS recognises the importance of the IGIS's role, and continues to work cooperatively with the Inspector-General to respond to recommendations in their reports.

## **Ombudsman and Privacy Commissioner**

The Office of the Ombudsman and the Office of the Privacy Commissioner also provide important oversight over NZSIS activities.

# Statement on Warrants

## **In accordance with section 221(2) of the Intelligence and Security Act 2017 (ISA), the following statements are provided for the period 1 July 2020 to 30 June 2021.**

### **Co-operation (section 221(2)(a) and (b) of the ISA)**

There were three occasions on which the NZSIS provided assistance under section 13(1) (b) of the ISA to the New Zealand Police or New Zealand Defence Force to facilitate their functions.

No assistance was provided to other agencies under section 14 of the ISA to respond to an imminent threat.

### **Intelligence Warrants (section 221(1)(c) to (g) of the ISA)**

#### **TYPE 1 INTELLIGENCE WARRANTS**

- a. Twenty applications for Type 1 intelligence warrants were made and approved under sections 58 and 59 of the ISA. No applications under section 58 or 59 were declined.
- b. No applications for an urgent Type 1 intelligence warrant were made under section 71 of the ISA.
- c. No applications for a joint Type 1 intelligence warrant were made under section 56 of the ISA.

#### **TYPE 2 INTELLIGENCE WARRANTS**

- a. Five applications for Type 2 intelligence warrants were made and approved under section 60 of the ISA. No applications under section 60 were declined.
- b. No applications for an urgent Type 2 intelligence warrant were made under section 72 of the ISA.
- c. No applications for a joint Type 2 intelligence warrant were made under section 56 of the ISA.

#### **VERY URGENT AUTHORISATIONS (SECTION 221(2)(1)(E) OF THE ISA)**

- a. (U) No very urgent authorisations were given by the Director-General under section 78 of the ISA.

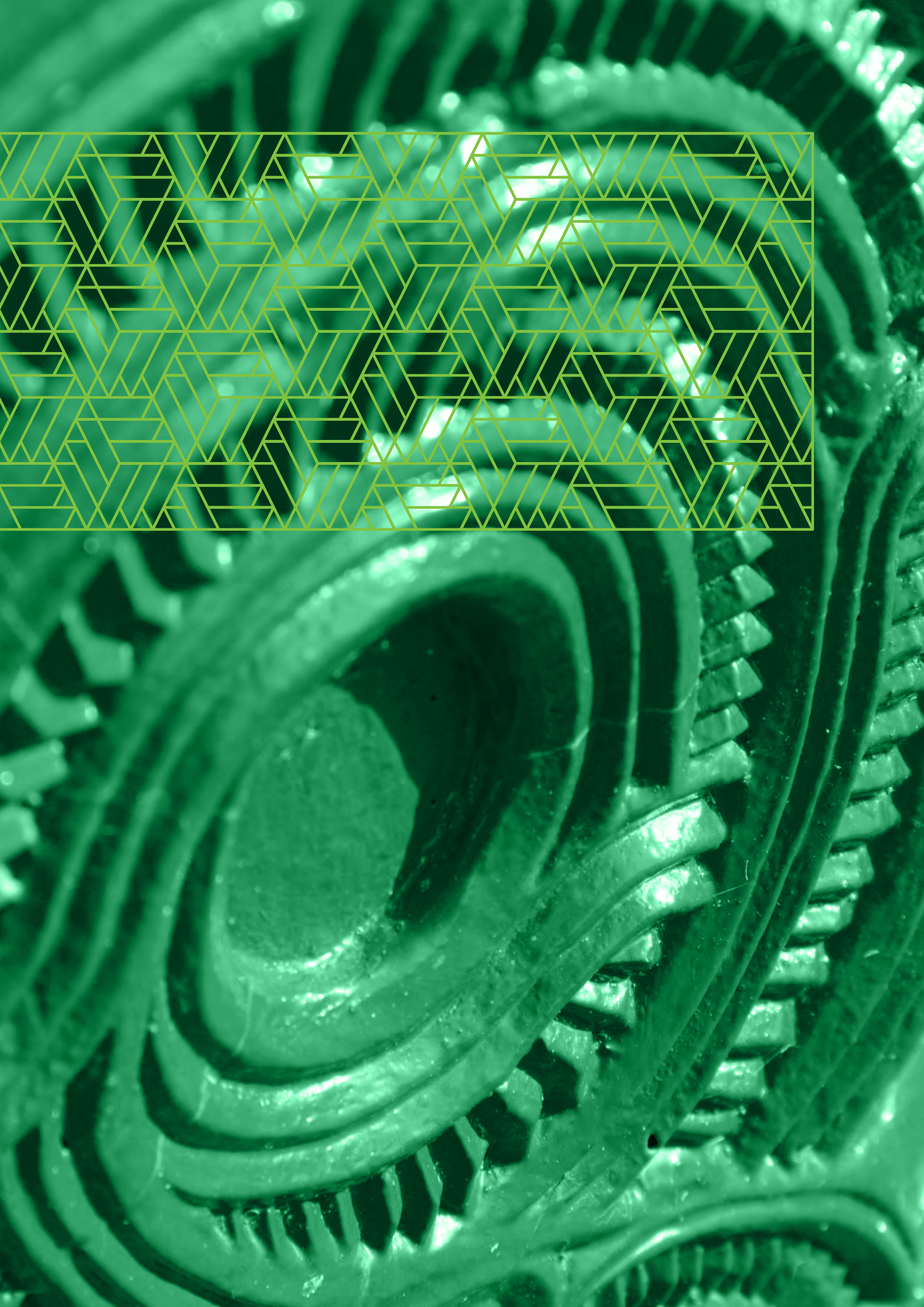
### **Restricted Information (section 221(2)(f) of the ISA)**

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

### **Business Records Directions (221(2)(h) of the ISA)**

513 business records directions were issued to business agencies under section 150 of the ISA.







# 09

## **Financial Statements**

Ngā Tauākī Pūtea



# Statement of Responsibility

I am responsible, as the Director-General of Security, and Chief Executive of the New Zealand Security Intelligence Service (NZSIS), for:

- The preparation of the NZSIS'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 NZSIS is provided in accordance with sections 19A to 19C of the Public Finance Act 1989, whether or not that information is included in this annual report; and
- The accuracy of any end of year performance information prepared by the NZSIS, whether or not that information is included in the annual report.

In my opinion:

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



Rebecca Kitteridge

Director-General of Security  
Te Tumu Whakarae mō Te Pā Whakamarumarū  
22 November 2021

# Independent Auditor's Report

## To the readers of the New Zealand Security Intelligence Service's statement of expenses and capital expenditure against appropriation for the year ended 30 June 2021.

The Auditor General is the auditor of the New Zealand Security Intelligence Service (the NZSIS). 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 NZSIS for the year ended 30 June 2021 on page 81.

### Opinion

In our opinion the statement of expenses and capital expenditure against appropriation of the NZSIS 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 Security 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 81 which outlines that the NZSIS 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 Security for the information to be audited

The Director-General of Security is responsible on behalf of the NZSIS for preparing a statement of expenses and capital expenditure against appropriation of the NZSIS that is presented fairly, in accordance with the requirements of the Intelligence and Security Act 2017.

The Director-General of Security 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 Security is responsible on behalf of the NZSIS for assessing the NZSIS's ability to continue as a going concern. The Director-General of Security 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 NZSIS, or there is no realistic alternative but to do so.

The Director-General of Security'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 Security 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 NZSIS'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 Security.
- We conclude on the appropriateness of the use of the going concern basis of accounting by the Director-General of Security and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the NZSIS'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 NZSIS 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 Security 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 Security is responsible for the other information. The other information comprises the information included on pages 3 to 76, 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 NZSIS 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 NZSIS.



**S B Lucy**  
Audit New Zealand

On behalf of the Auditor-General  
Wellington, New Zealand

# Statement of Expenses and Capital Expenditure against Appropriation

## FOR THE YEAR ENDED 30 JUNE 2021

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

	\$000
Total Appropriation	\$102,284
Actual Expenditure	\$94,457

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 New Zealand Security Intelligence Service 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.









New Zealand  
Security Intelligence  
Service

Te Pā Whakamarumarū