



Proactive release of material

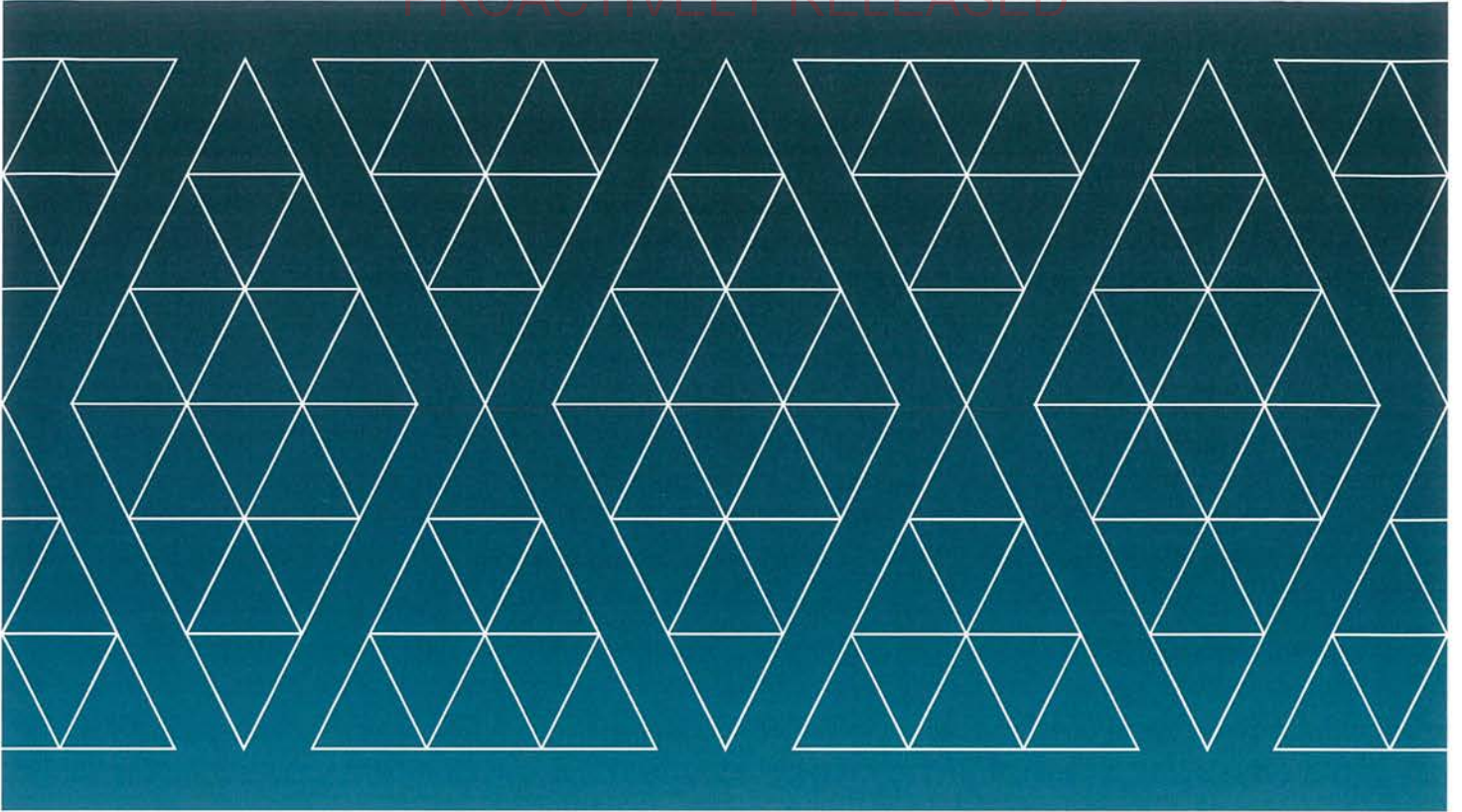
The following document has been proactively released by the GCSB and NZSIS on behalf of Hon Judith Collins, Minister Responsible for the GCSB, and Minister Responsible for the NZSIS:

Date	Title
November 2023	Briefing to the Incoming Minister

Some parts of this information release would not be appropriate to release and, if requested, would be withheld under the Official Information Act 1982 (the Act). Where this is the case, the relevant sections of the Act that would apply have been identified. Where information has been withheld, no public interest has been identified that would outweigh the reasons for withholding it.

Key to Redaction Codes:

Section	Explanation
6(a)	To avoid prejudice to the security or defence of New Zealand or the international relations of the Government of New Zealand
9(2)(ba)(i)	To protect information subject to an obligation of confidence, where revealing it would prejudice the supply and it is in the public interest that it continue to be supplied
9(2)(f)(iv)	To maintain the constitutional conventions for the time being which protect the confidentiality of advice tendered by Ministers of the Crown and officials
9(2)(g)(i)	To maintain the effective conduct of public affairs through the free and frank expression of opinions by or between or to Ministers of the Crown
18(d)	The information will soon be publicly available



Te Tira Tiaki
Government Communications
Security Bureau



Te Pā Whakamarumaru
New Zealand Security
Intelligence Service

Briefing to the Incoming Minister 2023

www.gcsb.govt.nz | www.nzsis.govt.nz

**PART ONE
ABOUT US**

The GCSB and NZSIS	6
Government Communications Security Bureau	7
<i>How does the GCSB collect intelligence?</i>	9
<i>GCSB Senior Leadership Team</i>	10
New Zealand Security Intelligence Service	11
<i>How does the NZSIS collect intelligence?</i>	12
<i>NZSIS Senior Leadership Team</i>	13
How our agencies work together	14
Financial sustainability	16
Contributing to the public conversation about national security	17
Your statutory role under the ISA	19
<i>Warrants and authorisations</i>	19

**PART TWO
THREAT ENVIRONMENT
AND OUR RESPONSE**

Geostrategic competition	22
Detecting and monitoring foreign interference activities in New Zealand	23
Countering the threat of terrorism	24
Partnering across the public and private sector for cybersecurity	26
Pacific regional security	28

**PART THREE
WORKING WITH OTHERS**

DPMC's role in the NZIC	30
<i>The Government's Response to the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain</i>	30
Working with Defence	31
Working with law enforcement	31
The Combined Threat Assessment Group	32
Border protection	33
National security clearances	33
Regulatory roles across Government	34
<i>Telecommunications (Interception Capability and Security) Act 2013 (TICSA)</i>	34
<i>Overseas Investment Act 2005</i>	34
<i>Outer-space and High-altitude Activities Act 2017 (OSHAA)</i>	34
<i>Radiocommunications Act 1989</i>	34
International partners	35
Public attribution statements	36
Private sector partners	37
Community partners	38

PART FOUR SUPPORT FOR THE FIRST 100 DAYS

In the first 100 days you will see	39
<i>Intelligence and Security Committee</i>	40
<i>March Baseline Update</i>	40
<i>Contingent liabilities register</i>	40
<i>Cyber attribution</i>	40
s6(a)	40
<i>Payload permit briefings</i>	40
<i>National Terrorism Threat Level</i>	41
s6(a)	41
<i>Warrants and authorisations</i>	42
Key issues that may arise	43
s6(a)	43
<i>Integration programme – lead operational cyber security agency</i>	43
<i>Pacific Regional Security</i>	44
s6(a) <i>Data Centre</i>	45
<i>Cryptographic infrastructure</i>	46
<i>Improvements to the National Security Screening System</i>	47
<i>Government Chief Information Security Officer</i>	47
<i>Protective security lead</i>	48
Upcoming policy work with other agencies	49
<i>Intelligence and Security Act review</i>	49
<i>Foreign interference and espionage</i>	49
<i>Space security</i>	50
<i>Emerging, critical and sensitive technology</i>	50
s6(a)	50

PART FIVE STRATEGY, POLICY AND ACCOUNTABILITY

51	51
National Security Intelligence Priorities	51
The National Security Strategy	52
NZSIS Strategy 2024-2029	54
GCSB Strategy 2023-2027	57
Ministerial Policy Statements	59
Oversight and accountability framework	60

PART SIX ORGANISATIONAL HEALTH

Organisational Health	62
-----------------------	----

PART SEVEN HOW WE WILL SUPPORT YOU

63	63
Directors-General	64
Responsibilities to the Prime Minister, Leader of the Opposition and Ministers	64
Private Secretary	65
Strategic Direction, Governance and Policy Directorate	65

INTRODUCTION

Congratulations on your appointment as the Minister Responsible for the Government Communications Security Bureau (GCSB), and Minister Responsible for the New Zealand Security Intelligence Service (NZSIS). We are keen to discuss your priorities and how we can support you at the earliest opportunity. We look forward to working with you to achieve the Government's objectives.

As set out in the Intelligence and Security Act 2017, our work contributes to:

- The protection of New Zealand's national security;
- The international relations and well-being of New Zealand; and
- The economic well-being of New Zealand.

Under the Intelligence and Security Act 2017, the agencies have four core functions:

- Intelligence collection and analysis;
- Provision of protective security services, advice and assistance;
- Co-operation with other public authorities to facilitate their functions; and
- Co-operation with other entities to respond to imminent threat.

New Zealand faces a range of national security threats. These include malicious cyber activity against organisations and individuals, foreign interference and espionage, violent extremism and terrorism, and insider threats. These threats are not unique to New Zealand: they also impact the wider Pacific region and our partners.

Threats to national security are often sophisticated, the potential impact is significant, and they are often secret or not widely known. To respond to them, under the Intelligence and Security Act 2017, our two agencies can use capabilities that are unique and form a key part of New Zealand's national security system.

Our intelligence capabilities allow us to identify, investigate, collect and report on these threats. We use these intelligence collection capabilities, supplemented by intelligence received from partners, to support government agencies in their operations and decision making, and to carry out their legislatively mandated functions. We also reduce the risk these threats pose through our protective security functions, working to improve information and physical security across government.

Our two agencies are closely aligned and share a number of functions to maximise our efficiency and effectiveness. We also work collaboratively with others. Often our role is to support New Zealand's law enforcement agencies, the New Zealand Defence Force, the wider public sector, and a range of private sector organisations of national significance.

We also work with our partners in the Five Eyes, an intelligence sharing partnership made up of Australia, the United Kingdom, the United States, Canada and New Zealand, to ensure we have access to the capabilities, intelligence and skills we need to keep New Zealand safe.

Everything we do needs to be in accordance with New Zealand law and our international human rights obligations, and aligned with the requirements, spirit and values of New Zealand's public sector.

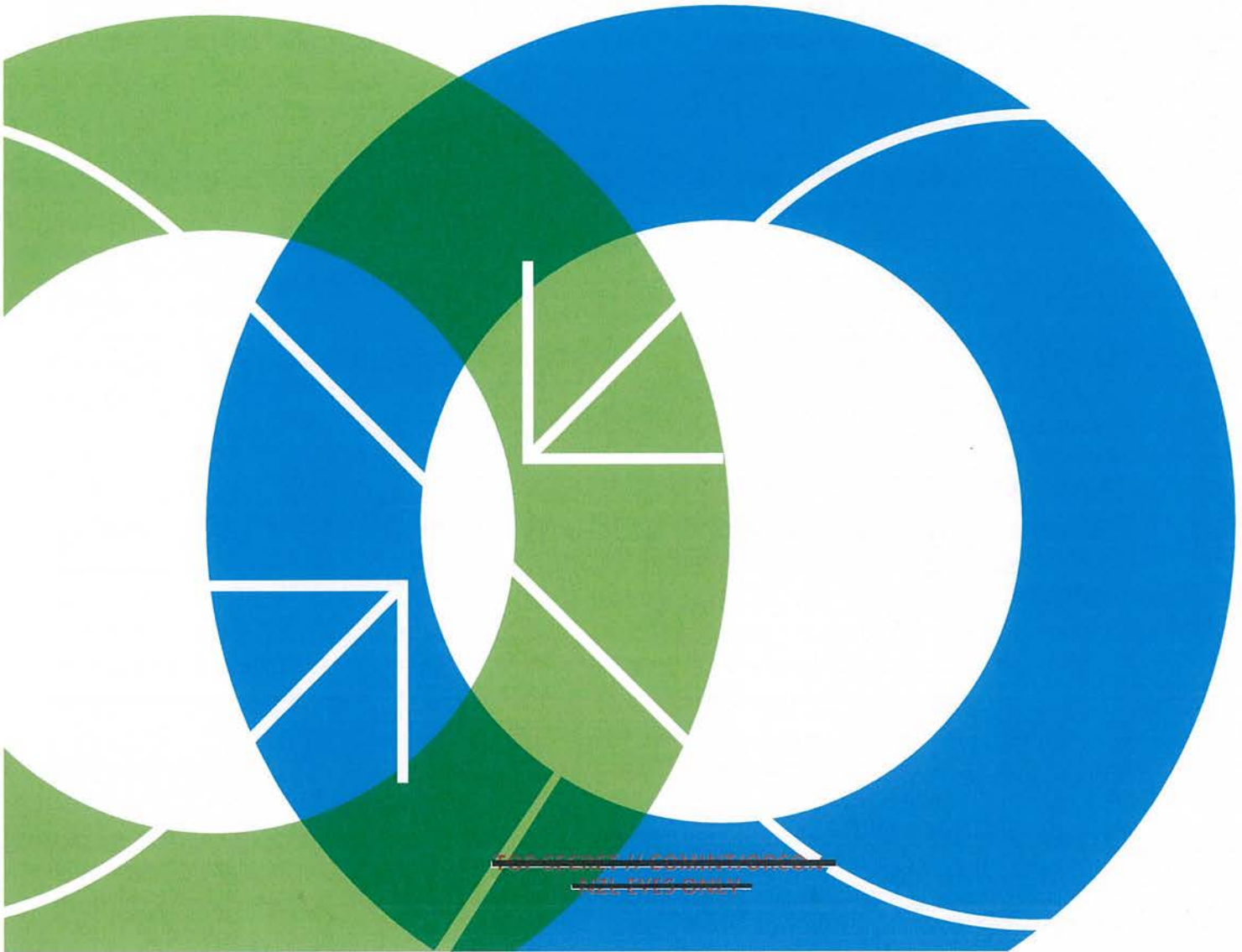
The GCSB and NZSIS strive to build a workforce that reflects New Zealand's communities, and is supportive of their wellbeing.

This briefing provides you with an overview of our operating context, structure, most significant challenges and empowering legislation. It also sets out your statutory roles in relation to the GCSB and NZSIS. This briefing includes an introduction to our capabilities, as well as the threats New Zealand faces, and the specific ways in which we respond to them.

We will work with you and your office to tailor a series of more detailed briefings on our functions and current operations.

PART ONE ABOUT US

GCSB and the NZSIS are two of the several agencies that come together to form New Zealand's national security community. This community is focussed on protecting a secure and resilient Aotearoa New Zealand—one that is a free, open and democratic society for future generations. The work of the GCSB and NZSIS makes a key contribution to New Zealand's national security.



Te Tira Tiaki

Government Communications Security Bureau

GCSB is Aotearoa New Zealand's lead organisation for signals intelligence (known as SIGINT, collecting intelligence through electronic means such as accessing information infrastructures), cyber security, and cyber resilience.

Our mission is to equip our customers with the intelligence and cyber resilience necessary to forecast and successfully navigate Aotearoa New Zealand's changing strategic environment. GCSB plays a crucial part in how Aotearoa New Zealand makes sense of the world and manages national security threats.

As the global community begins to move beyond the disruptions of the COVID-19 pandemic, we continue to operate in a complex and challenging threat environment. Our specialist knowledge and technical expertise repeatedly leads to reporting that provides unique insights to our domestic and international partners. Our contributions continue to be crucial s6(a) s6(a)

Information assurance and cyber security

Under its information assurance and cyber security functions, GCSB works to protect information systems and communications critical to New Zealand's national interests from sophisticated security threats. Through the National Cyber Security Centre (NCSC), GCSB provides cyber security services and advice to public and private sector organisations. GCSB is the lead agency for information security for

government. GCSB also acts as the New Zealand national authority for communications security – the technology and processes used to protect our most sensitive data through advanced encryption. Our work contributes to the cyber security of millions of New Zealanders.

On 31 August 2023, the functions of New Zealand's Computer Emergency Response Team (CERT NZ) were transferred from the Ministry of Business, Innovation and Employment (MBIE) to GCSB, and the NCSC is working on integrating with CERT NZ. While the NCSC always worked closely with CERT NZ, integrating the two functions will enhance New Zealand's ability to tackle emerging cyber security challenges and provide joined-up, customer-centric services for New Zealanders. With this, we are now New Zealand's lead operational cyber security agency.

GCSB plays a role in the Telecommunications (Interception Capability and Security) Act 2013 (TICSA). TICSA requires public telecommunications network operators to notify the GCSB if they are planning a network change within certain areas of specified security interest. Notifiable changes include the purchase or acquisition of equipment or services, changes to network architecture, or changes in ownership or control. You can read more about TICSA and your role on page 34.

GCSB also provides its CORTEX programme, to counter cyber threats to both public and private sector organisations of national significance. This involves GCSB using tools and threat information to protect these organisations from advanced persistent malicious software (malware). CORTEX cyber protection services operate a highly targeted range of capabilities and are only deployed with the express agreement of the organisation involved. CORTEX has helped reduce \$382 million worth of harm since 2016.

GCSB also works in partnership with internet service providers to deliver a capability called Malware Free Networks™. Malware Free Networks™ is a scalable malware detection and disruption service which involves the NCSC generating, and near real-time sharing, cyber threat intelligence with consenting organisations. Since 2021 GCSB has disrupted over 2 million malicious cyber events as part of Malware Free Networks™. This service recently won the Prime Minister's award and the Service Excellence award as part of the Public Service Commission's annual Spirit of Service awards.

The NCSC works with organisations to help respond to cyber incidents. This involves finding and removing network compromises and providing advice and support on remediation and prevention. The NCSC's Incident Co-ordination and Response team is on call to victims of cyber incidents and ready to deploy 24/7.

The Director-General GCSB also acts as the Government Chief Information Security Officer (GCISO). Cyber security is a critical enabler of an effective, trusted and reliable public service,

and the GCISO drives system coherence to the government's approach to cyber security to lift New Zealand's overall cyber resilience. The purpose of this approach is to enhance the capability of the public service to move at pace with modern tools, technology and wider changes in the digital environment such as Cloud adoption, federated data and artificial intelligence.

Cabinet confirmed a refreshed GCISO mandate in April 2023 to strengthen the cyber security of public services. The expanded mandate aims to modernise the public service's cyber security, including through setting expectations on agencies and providing investment advice to the government. As the NCSC works to deliver this expanded mandate, we aim to be able to provide you with greater visibility of cyber security across government and where investment should be prioritised to have the greatest impact.

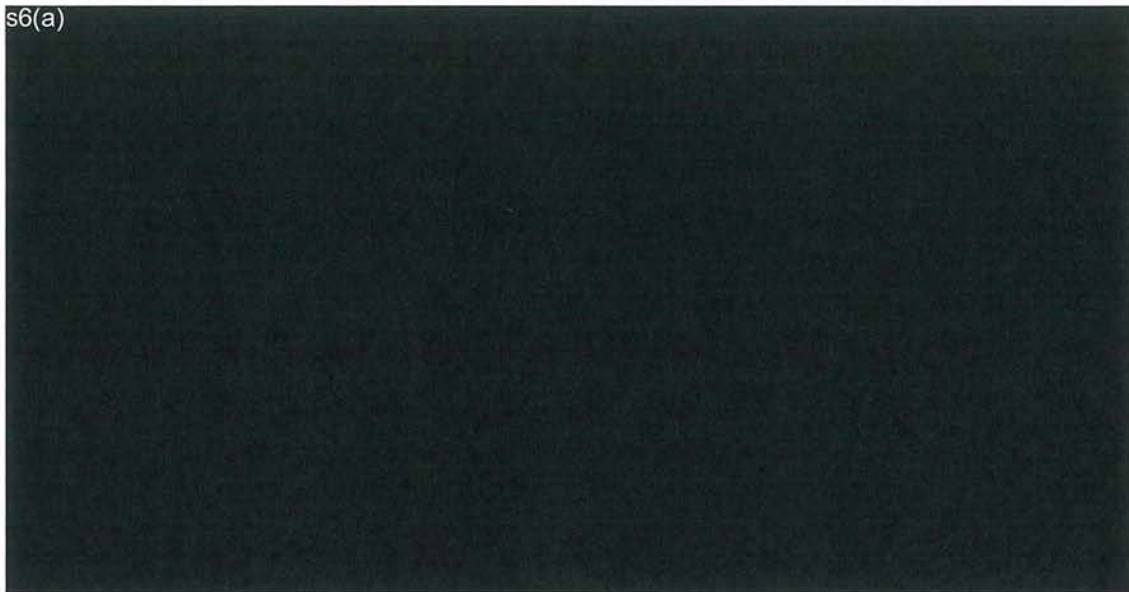
s9(2)(f)(iv)

The GCISO works closely with the other system leads, particularly the Government Chief Digital Officer and the Government Chief Data Steward to create trusted, secure and high-quality data, information and technology that enables our public service to deliver better outcomes for the wellbeing of Aotearoa New Zealand.

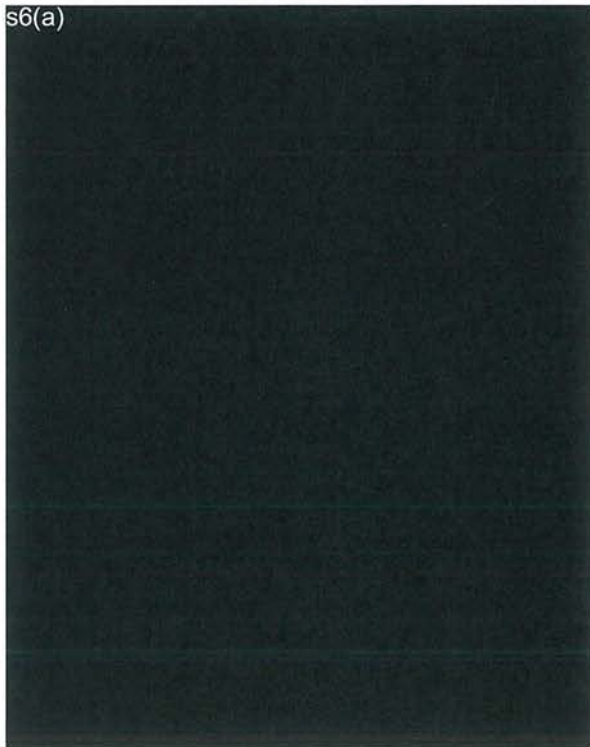
How does GCSB collect intelligence?

GCSB collects intelligence using several methods. These include but are not limited to:

s6(a)



s6(a)



s6(a)



s6(a)



GCSB's role is to collect intelligence and develop intelligence products and ensure this information gets to the relevant international and New Zealand agencies to inform policy advice, operations and enforcement. These agencies can include Immigration New Zealand, New Zealand Customs Service, NZSIS, New Zealand Police, New Zealand Defence Force, Ministry of Foreign Affairs and Trade and the Ministry of Business, Innovation and Employment. GCSB also provides support to military operations.



GCSB Senior Leadership Team

Andrew Clark is the Director-General of GCSB. He began this role on 30 October 2023.

He is the system lead for cyber security across the New Zealand Government, as the Government Chief Information Security Officer, reporting to the Digital Executive Board overseen by the Minister for Digital Economy and Communications. He is also a member of the New Zealand National Security Board¹.

Prior to his role at GCSB, Andrew spent 37 years in the New Zealand Defence Force and was the Chief of Air Force before he left. He held a number of other leadership roles at NZDF before this.

Andrew is supported by GCSB's Senior Leadership Team:

- **Lisa Fong** – Deputy Director-General, National Cyber Security Centre
- **Monica Silverwood** – Chief Legal Advisor
- **s6(a)** – Deputy Director-General, Intelligence
- **Nicky Haslam** – Deputy Director-General Finance, Commercial and Support Services *
- **s6(a)** – Deputy Director-General, Technology*
- **Shelly Thompson** – Deputy Director-General, People and Capability*
- **Bridget White** – Deputy Director-General, Strategic Direction, Governance and Policy*
- **Robynleigh Cowan-Emery** – Chief Advisor Māori*

Location

The GCSB's head office is based in Pipitea House on Pipitea Street in Wellington. As of 30 June 2023, GCSB had 540 full-time equivalent staff. We have offices in three locations; Wellington, Auckland and Waihopai, near Blenheim **s6(a)**. We also have a high frequency radio interception and direction-finding station in Tangimoana, near Palmerston North. GCSB hosts most of the shared and joint functions with NZSIS.

* These roles are formally part of both agencies' leadership teams as part of our joint enabling functions (page 14).

1 The National Security Board is a group of public sector chief executives who meet regularly to provide strategic leadership, oversee capability development and ensure that agencies' policies and activities align.

Te Pa Whakamarumarū New Zealand Security Intelligence Service

The NZSIS's mission is to keep New Zealand and New Zealanders safe and secure by identifying, understanding and mitigating threats to New Zealand's national security. We do this through our security intelligence, foreign intelligence and protective security services. We have four key impact areas that are outlined below.

Countering espionage and foreign interference

The NZSIS detects, investigates and disrupts possible espionage and foreign interference threats taking place in or against Aotearoa New Zealand. We seek to understand and assess the threats and provide timely advice and intelligence reporting to help counter these activities.

Countering violent extremism and terrorism

To counter terrorism and violent extremism, the NZSIS detects and investigates violent extremism threats against Aotearoa New Zealand's interests and works with other agencies to prevent these threats from escalating into acts of terrorism.

We look at global and domestic events and developments relating to violent extremism in order to understand the possible impact on violent extremist activity in Aotearoa New Zealand. The NZSIS assesses whether existing domestic threats are increasing or diminishing, and works to detect and understand new or emerging threats.

Our protective security leadership

The NZSIS has a statutory responsibility to provide protective security services, advice and assistance to the public sector. The Director-General is the Government Protective Security Lead.

Through its Protective Security directorate, the NZSIS provides information, tools and guidance to government agencies to ensure they have appropriate protective security measures. The core tool for providing security advice to government agencies is the Protective Security Requirements framework. Implementing the Protective Security Requirements framework is mandatory for 37 government agencies, and there are six agencies that voluntarily implement the framework.

The NZSIS has 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.

Contributing to a secure, prosperous and resilient Pacific

New Zealand has a critical, long-term and non-discretionary stake in supporting and advancing peace, stability, prosperity and resilience in the Pacific.

The NZSIS's role is to detect, disrupt and deter activities which undermine New Zealand's national security and that of our partners in the Pacific. This includes supporting Pacific partners to build their protective security.

How does the NZSIS collect intelligence?

Many of the functions outlined above are enabled through a range of collection methods including physical surveillance, technical interception, specialist technical collection activity and human intelligence activities – "HUMINT".

HUMINT may come from a range of sources – from covert human intelligence sources, to private individuals who may offer information. This requires methods including face-to-face meetings, community engagement, over the internet, or via other forms of communications. NZSIS also uses other collection methods including physical surveillance, tracking devices, technical interception, listening devices, open source data analysis, and tracking online activity. The NZSIS can task GCSB to assist with our work, using their unique intelligence capabilities.

The increasingly digital and data-driven world has impacted on both the information the NZSIS can access and the way NZSIS needs to work in order to deliver on our functions. To fulfil our mission NZSIS needs to access, analyse and use data that has become more complex, more hidden and more fragmented. Accessing, analysing and assessing data in order to deliver actionable intelligence has never been more difficult.

The NZSIS has always been required to understand emerging threats but the way NZSIS does that has changed significantly in recent years. Insights now increasingly come from our ability to acquire and make sense of different data, pulling together different information threads to connect dots to show where threats may lie.

The NZSIS is not a law enforcement agency. If, through the course of our work, we discover intelligence of security concern, the NZSIS can share this information with appropriate agencies, such as the New Zealand Police, New Zealand Customs Service or Immigration New Zealand, in order to disrupt such threats and mitigate risks to the public.

Location

The NZSIS's 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 2023, the NZSIS had 420 full-time equivalent staff.



NZSIS Senior Leadership Team

Andrew Hampton is the Director-General of Security. He has been in this role since April 2023.

Before joining the NZSIS, Andrew Hampton was Director-General of the GCSB for seven years.

Prior to joining the GCSB, Andrew spent much of his career in the justice sector, including Treaty settlement negotiations, courts administration and leading various significant change programmes. Senior positions he held in the justice sector include Director of the Office of Treaty Settlements, Deputy Secretary for Courts, and Deputy Chief Executive at the Crown Law Office. Andrew has also held senior leadership positions elsewhere in the state sector. He was Deputy Secretary and Director of the Secretary's Office at the Ministry of Education, and was also the Government Chief Talent Officer at the Public Service Commission.

Andrew is supported by the NZSIS's Senior Leadership Team:

- **Anna Foley** – Deputy Director-General, Capability
- **Sharee Christensen** – General Counsel
- **Phil McKee** – Deputy Director-General, Intelligence
- **Nick Marks** – Deputy Director-General, Protective Security
- **Nicky Haslam** – Deputy Director-General Finance, Commercial and Support Services *
- **s6(a)** – Deputy Director-General, Technology*
- **Shelly Thompson** – Deputy Director-General, People and Capability*
- **Bridget White** – Deputy Director-General, Strategic Direction, Governance and Policy*
- **Robynleigh Cowan-Emery** – Chief Advisor Māori*

* These roles are formally part of both agencies' leadership teams as part of our joint enabling functions (page 14).

How our agencies work together

GCSB and the NZSIS work closely together to ensure a secure and resilient Aotearoa New Zealand, one that is protected as a free, open and democratic society for future generations.

We frequently leverage our common intelligence functions and work together to detect, deter and disrupt specific threats to New Zealand's national security. These threats are discussed in the next section. The NZSIS and GCSB's complementary intelligence capabilities cover a broad spectrum of intelligence sources.

For example, HUMINT activities may provide a lead or details of a target that enable a SIGINT access to be exploited, and vice versa. While this collaboration is essential, the disciplines remain unique, with distinct tradecraft, systems and expertise required to execute operations successfully.

Both agencies have regulatory roles that we exercise together regarding foreign investments and outer-space and high-altitude activities. As well as collaborating in the intelligence space, the agencies have a range of joint enabling functions:

- finance
- human resources
- technology
- ministerial services functions (including OIA and Privacy Act requests)
- communications
- international engagement
- security services
- procurement
- facilities
- policy and strategy.

PROACTIVELY RELEASED

Financial sustainability

Following several critical reviews of the agencies around a decade ago, the government recognised that the agencies were underfunded to perform the roles expected of them. As a result, a Strategy, Capability and Resourcing Review (SCRR) was undertaken in 2015 to determine appropriate funding levels for the agencies, and Budget 2016 included a staged multi-year funding uplift for both agencies. This was refreshed in Budget 2020, with a further increase provided at that point to recognise changes in the operating environment and in the agencies' cost drivers.

The increases in the agencies' funding in recent years are largely driven by these SCRR funding increases. Other more minor funding increases reflect the outcome of individual Budget

initiatives, including funding for our counter-terrorism mission following the 15 March 2019 mosque attacks, funding for our cyber security and foreign interference missions, and funding to help address price pressures.

Being financially sustainable is fundamental for the work the agencies do. With this in mind, we have developed a financial sustainability programme for the agencies. Building on a strong understanding of our underlying cost drivers and how these are best managed through time, we are identifying opportunities to reduce inefficiency and increase effectiveness. In doing so, we will demonstrate that we are maximising the value we deliver with our funding.

The programme is comprised of four workstreams:

Workforce planning Strengthening our workforce information to enhance decision-making	Functional analysis Removing duplication or inefficiencies in our operating model	Efficiency review Maximising service delivery from our spending	Effectiveness review Ensuring spending is aligned to key priorities.
---	---	---	--

The agencies have received a series of small budget increases in recent years to respond to the fast changing threats that New Zealand faces. These have included investments in our counter-terrorism, cyber security and foreign interference missions. Ensuring that the agencies deliver value to New Zealand and New Zealanders as a result of this investment is a top priority.

s6(a) - relates to changes in agencies' capacities

s6(a) - relates to changes in agencies' capacities

Contributing to the public conversation about national security

The agencies have responded to shifting threats and increased public demand for information about national security. Through the Department of the Prime Minister and Cabinet's (DPMC) annual National Security Survey and the findings from the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain, we know that the public want to be better informed about security risks.

By routinely being more open about national security, we can develop a greater understanding and help the public to be better placed to manage risks. Below are some examples of how we regularly communicate with the public about national security. We will engage with you and your office in the lead-up to these publications and public statements.

Kia mataara ki ngā tohu – Know the signs: a guide for identifying signs of violent extremism

The NZSIS has researched the common behaviours and activities displayed by violent extremists who mobilise to violence. This research drew on case studies from New Zealand dating back to 2006, of violent extremists that were motivated by a variety of ideologies. The research was validated by case studies from around the world and led to the development of the NZSIS Terrorism Indicator Framework. The work evolved to become the NZSIS's first-ever public guide to help New Zealanders identify behavioural signs of violent extremism: *Kia mataara ki ngā tohu – Know the signs: a guide for identifying signs of violent extremism*, which was published in 2022. The NZSIS uses the guide as an engagement tool to work with stakeholders and communities on how to

identify the signs and report behaviour of concern. There is potential to do much deeper engagement with the likes of teachers and schools. If some of these signs are observed and reported at an early stage, it could disrupt someone on the path of radicalisation. We plan to update this guide as new trends emerge.

National Terrorism Threat Level

The Director-General of Security is responsible for reviewing the National Terrorism Threat Level annually. The purpose of the National Terrorism Threat Level is to inform the national security system, and the public, about the likelihood of a terrorist attack in New Zealand. The threat level is based on an assessment made by the multi-agency Combined Threat Assessment Group and is continually evaluated, meaning it could change at any time. The threat level is published on the NZSIS website. The last annual review was in November 2022, where the threat level was revised from Medium to Low. The next routine review is due to be completed in November 2023.

Annual Security Threat Environment report

In August 2023, following the release of other documents relating to foreign policy and national security policy, the NZSIS released its first annual unclassified threat assessment. It covers the threats for which NZSIS has responsibility including terrorism, violent extremism, foreign interference and espionage. The report was the first time that the NZSIS named foreign states involved in acts of foreign interference and espionage in New Zealand. We are planning to release the second edition around August 2024.

Annual Cyber threat report

GCSB's NCSC releases an annual cyber threat report. This report provides an overview of New Zealand's cyber threat landscape.

The most recent cyber threat report was published on the NCSC website on 2 November 2023.

Cyber attributions

GCSB, through the NCSC, conducts technical attribution of malicious cyber activity and provides this, usually at a classified level, to the Government. The Government may draw on the NCSC's technical attribution – as part of an all-of-government process – and use this information to publicly call out a malicious cyber actor.

GCSB also joins our partners in publicly calling out malicious cyber activity and these are published on the NCSC website. New Zealand only attributes malicious cyber activity when it is in our national interest to do so. You can read more about the process and decision-making for cyber attributions on page 36.

Cyber advisories

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

Your statutory role under the ISA

As already noted, the governing legislation for GCSB and NZSIS is the **Intelligence and Security Act 2017**. The ISA sets out our functions, powers and duties and provides the legislative framework that enables us to carry out activities to contribute to the protection of New Zealand's national security, its international relations and well-being and its economic well-being. The Act also provides appropriate limitations and robust oversight mechanisms.

The ISA confers significant responsibilities on the Minister Responsible for the GCSB and the NZSIS. These include:

- Issuing intelligence warrants and removal and practice warrants (including in some cases in conjunction with a Commissioner of Intelligence Warrants);
- Approving a Director-General to issue business records directions and granting permission to access restricted information;
- Authorising others to receive intelligence;
- Authorising the provision of protective security services, advice and assistance by GCSB and NZSIS to any person/class of persons;
- Issuing Ministerial Policy Statements, a unique legislative tool which provides guidance to GCSB and NZSIS on lawful activities; and
- Providing a response to inquiries undertaken by the Inspector-General of Intelligence and Security (IGIS).

Warrants and authorisations

The GCSB and NZSIS use intelligence warrants to carry out much of their work. There are two types of intelligence warrants, as follows:

Type 1

A Type 1 intelligence warrant authorises an intelligence and security agency to carry out an otherwise unlawful activity for the purpose of collecting information about, or to do any other thing directly in relation to,—

- (a) any person who is—
 - (i) a New Zealand citizen; or
 - (ii) a permanent resident of New Zealand; or
- (b) a class of persons that includes a person who is—
 - (i) a New Zealand citizen; or
 - (ii) a permanent resident of New Zealand.

Type 2

A Type 2 intelligence warrant authorises an intelligence and security agency to carry out an otherwise unlawful activity for the purpose of collecting information, or to do any other thing, in circumstances where a Type 1 warrant is not required.

Applications for Type 1 warrants are issued jointly by you as the authorising Minister, and a Commissioner of Intelligence Warrants, whereas Type 2 warrants are issued solely by the authorising Minister. There are three Commissioners of Intelligence Warrants, with one appointed as the Chief Commissioner (currently Sir Bruce Robertson). All have previously been High Court or Court of Appeal Judges.

Intelligence warrant applications must meet certain criteria and warrants are issued to enable certain activities against individuals or classes of people or things. The activities include surveillance, interception, search, seizure and human intelligence.

Because of your statutory role, we regularly request meetings to seek warrants and authorisations. From time to time, fast-moving or urgent operational matters may mean we need to brief you at short notice, but otherwise we provide your office with warrant applications at least two working days prior to any meeting. If a Type 1 warrant is sought (one involving New Zealanders), a Commissioner of Intelligence Warrants will have already reviewed the application and will attend the meeting with you.

The Minister of Foreign Affairs is statutorily required to be consulted in relation to warrants that authorise activities likely to have implications for New Zealand's foreign policy or New Zealand's international relations. Practice over the previous parliamentary term has been for the Minister of Foreign Affairs to receive written briefings from MFAT officials, where required, following input from the agency.

The Intelligence and Security Act has recently been reviewed and the incoming Government will need to consider its response to the reviewers' recommendations. You can read more about this on page 47.

PART TWO

THREAT ENVIRONMENT AND OUR RESPONSE

This section outlines the main national security threats New Zealand faces and how the agencies are seeking to keep ahead of the threats.

The security environment in which New Zealand operates is now more challenging and less predictable than has been the case in recent decades.

New Zealand faces a range of national security threats. These include malicious cyber activity against organisations and individuals, foreign interference and espionage, violent extremism and terrorism, and insider threats. These threats are not unique to New Zealand: they also impact the wider Pacific region and our partners.

Many of the threats faced by New Zealand originate from actors who go to great lengths to hide their activities. Sophisticated security awareness and counter-intelligence capabilities are increasingly not solely the purview of state sponsored intelligence officers. Both state sponsored and criminal cyber actors use technically complex means to exploit their

targets and avoid identification. Likewise, groups and individuals with extremist ideologies can cover their tracks through the use of readily available encrypted communications previously unavailable to them.

It is for these reasons that the capabilities, functions and operations of New Zealand's security and intelligence agencies require the highest levels of security and classification. A target's knowledge that they are or are not of interest to the agencies, or knowledge of the capabilities of the New Zealand security and intelligence agencies, will invariably alter that target's behaviour.

Geostrategic competition

Strategic competition is where states seek to advance competing visions for regional and global orders. We have seen this return to the forefront between the major powers, which is making the global and regional security environment more complex and unpredictable.

There are clear implications for New Zealand and our home region when geopolitical tensions become more intense. New Zealand is a small, export nation which relies on stable international rules-based order. Intense strategic competition means states are looking to change rules-based order, which creates instability and makes it harder for export nations such as New Zealand.

Some states will seek to gain an advantage in any way they can. Technological developments are a common feature of strategic competition but attempts to drive social changes are becoming equally commonplace. The race to gain an upper hand is also helping to fuel a hyper-active information environment in which disinformation can spread rapidly.

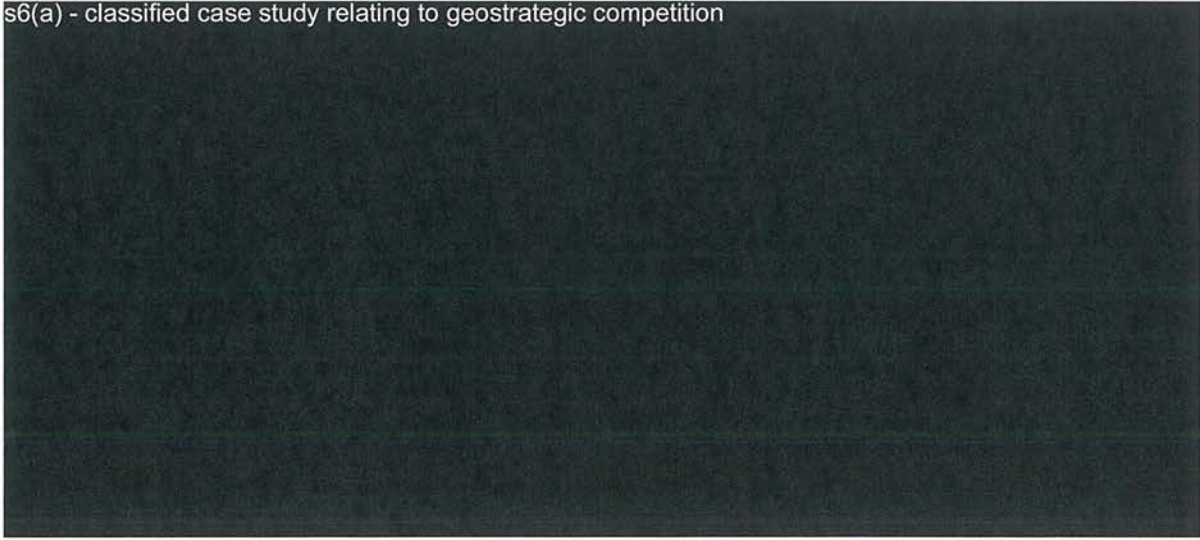
Strategic competition and general disruption are the common themes behind many of the changes seen in New Zealand's threat environment over the recent years.

The Indo-Pacific region has seen increased geostrategic competition and we have a role in supporting the resilience of our regional partners to ensure the stability and prosperity of the region. More information on our work in the Pacific is on page 28.

The increasingly complex geostrategic environment means the pivotal role the agencies play in providing both intelligence and protective security services will only become more important.

One of the most visible ways geopolitics has manifested in our society has been through foreign interference activity.

s6(a) - classified case study relating to geostrategic competition



Detecting and monitoring foreign interference activities in New Zealand

Foreign interference is an act by a foreign state, often through someone working on its behalf (a proxy), intended to influence, disrupt, or subvert New Zealand's national interests by deceptive, corruptive, or coercive means. It can be divided into two main forms: political and societal.

- Political interference may target governance systems (including the electoral process), the information environment, and politically influential people.
- Societal interference may target individuals, communities, businesses, social and activist groups or the information environment.

Foreign interference poses a significant threat to New Zealand's interests. Some foreign states target New Zealand for political, economic and military advantage through the use of espionage and interference. Suspected foreign intelligence officers travel to New Zealand without declaring their true employment, and suspected assets of foreign intelligence services operate and reside here.

Both political and societal interference have been detected in New Zealand but the latter is probably more common. The main targets of interference activities in New Zealand are our migrant and well-established communities who may be viewed as dissidents by a foreign state. These communities can receive unwanted and unjustified attention from foreign states who conduct malicious activities designed to threaten and disrupt their peaceful life in New Zealand. The NZSIS has observed indications of interference efforts

targeting our political, academic, and media sectors, and several of our migrant communities.

Many foreign interference activities occur without reaching the threshold of New Zealand espionage laws, providing limited avenues for recourse.

s6(a)



Espionage and foreign interference present substantial challenges for the intelligence community. State intelligence apparatuses are often well resourced, practised in their tradecraft and security practices, and supported by ideologically motivated or compromised co-opted persons within New Zealand. Such activities exist within a politically charged environment, with the potential to collect intelligence on prominent, influential or sensitive targets.

Countering the threat of terrorism

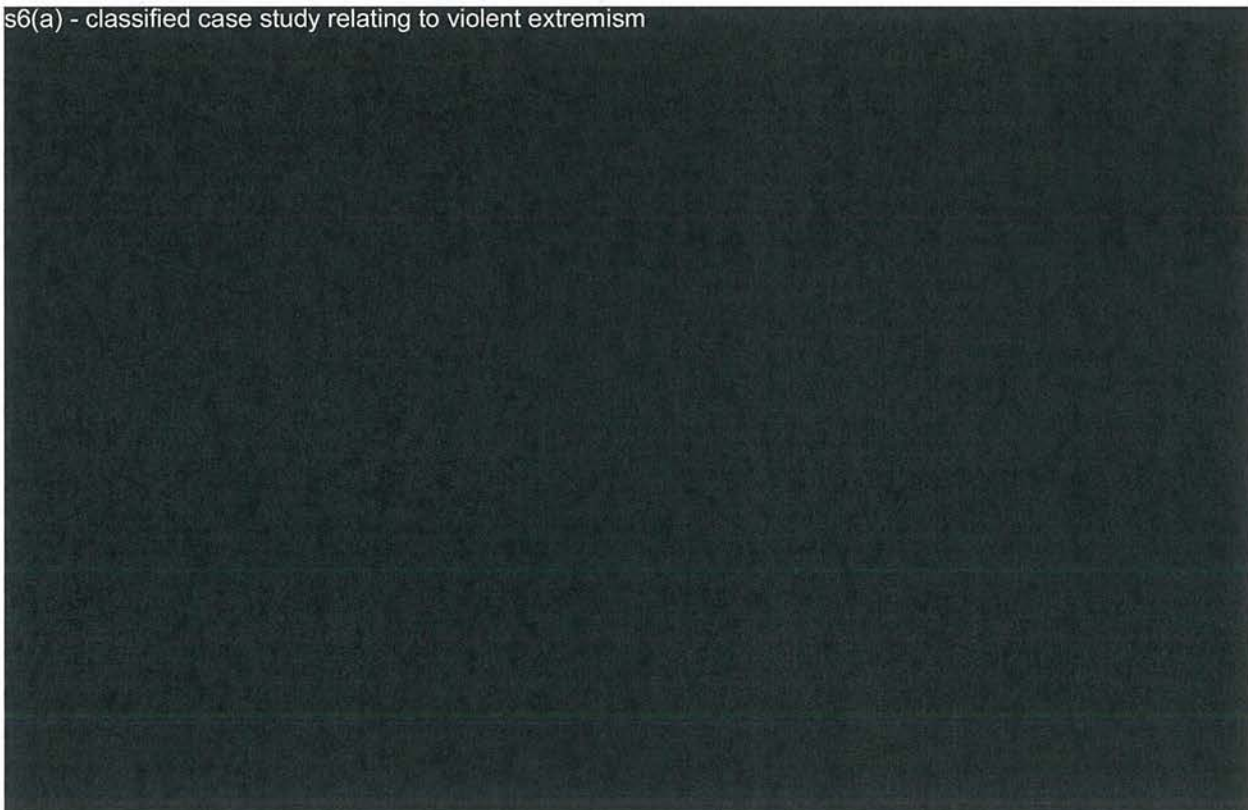
The spectrum of violent extremist activity in New Zealand mostly consists of expressing support for violent extremist ideologies.

A spectrum of ideologies influence New Zealand's violent extremism environment, including Politically-Motivated Violent Extremism, Identity-Motivated Violent Extremism and Faith-Motivated Violent Extremism. While most violent extremists hold easily identified violent extremist ideologies, we have observed an increase in individuals holding mixed, unstable and unclear ideologies. The traditional identity, faith and political motivations are still identified in violent extremists

that NZSIS detects and monitors in New Zealand, but this new trend has emerged around the edges.

The National Terrorism Threat Level was revised to Low in November 2022, meaning that a terrorist attack in New Zealand is considered a realistic possibility. Online spaces remain a haven for inflammatory language and violent abuse but the vast majority of those making threats are unlikely to follow through by committing a violent act in the real world.

s6(a) - classified case study relating to violent extremism



PROACTIVELY RELEASED

Partnering across the public and private sector for cybersecurity

The interests and activities of a range of actors in cyberspace, both state and non-state, threaten to degrade the cyber security of New Zealand. These threats come in many forms, continually changing to adapt to new technology or security measures. Cyber security is a rapidly evolving domain.

s6(a)

Cyber incidents provide a means for cyber criminals to target Aotearoa New Zealand organisations and citizens from anywhere in the world. Their motivations range from financial, pursued through ransom demands or theft, to the political. Criminal actors can be well-resourced and sophisticated in their methods, choice of targets, and organisation.

The GCSB's NCSC disrupts malicious cyber activity from impacting its customers' environments by blocking harmful activities through our active disruption capabilities. We intervene to remove malicious cyber actors from victim networks, and support affected organisations through service restoration and recovery. The NCSC's Malware Free Networks™ capability uses a range of intelligence to detect and disrupt malicious cyber activity targeting Aotearoa New Zealand. The threat intelligence feed contains indicators of malicious activity generated using automation from a range of sources and is curated by our analysts.

We partner with Aotearoa New Zealand industry to deliver Malware Free Networks™, and to drive system-wide improvements. One NZ provides Malware Free Networks™ to its broadband and mobile customers, approximately 2.4 million New Zealanders. Internationally, we worked to release joint products regarding the latest threats and best practice advice.

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

PROACTIVELY RELEASED

Pacific regional security

What happens in the Pacific has a fundamental impact on Aotearoa New Zealand's own national security, prosperity and identity. New Zealand and our Pacific neighbours exist in a security environment that is becoming increasingly challenging for governments to navigate.

s6(a)

The NZSIS has a clear role to work with our Pacific counterparts to support a secure and prosperous Pacific region, and work with s6(a) s6(a) to protect our shared fundamental values of democracy, human rights, and the rule of law. The NZSIS Pacific Mission focusses on detecting, deterring and disrupting s6(a) in the region. You can read more about this on page 42.

Recently Aotearoa New Zealand and our Pacific neighbours' security threat environment has become increasingly complex and challenging to navigate. Our place in the Pacific region, and our influence in the South Pacific, has required Aotearoa New Zealand to manage heightened strategic tension, disruption and risks s6(a)

s6(a)

s6(a)

The NZSIS is uniquely placed among Five Eyes partners in the region, because our domestic security remit means we confront many of the same threats as our Pacific partners. They can learn from our domestic experience, which we have autonomy to share.

s6(a)

the agencies' role s6(a) includes ensuring that s6(a) are well informed regarding external activity. In pursuing this goal, the NZSIS works with our Pacific partners in building their understanding of, and resilience to, a range of threats and risks. GCSB's CERT NZ works with Pacific Island countries on their cyber resilience.

We work with a number of Pacific partners to share expertise on how to build and implement protective security frameworks that help protect people, assets and information from harm. The aim of this engagement is to support Pacific partners to implement their own bespoke arrangements that respond to their individual security environment and needs. The Protective Security Requirements team's Pacific outreach includes continuing engagement s6(a)

s6(a)

PART THREE

WORKING WITH OTHERS

GCSB and NZSIS partner with New Zealanders from across society to keep our country safe and secure. The agencies seek to be honourable Treaty partners who deliver national security outcomes in accordance with Te Tiriti o Waitangi.

A central mission of the security and intelligence agencies is to ensure Ministers, other government agencies and our international partners have access to timely and relevant intelligence to inform their decision making. As part of Aotearoa New Zealand's national security community, the GCSB and NZSIS work together with a range of agencies and organisations to help enhance Aotearoa New Zealand's national security.

The GCSB and NZSIS have a crucial role to play in understanding the threats Aotearoa New Zealand faces and to provide advice on how to guard against those threats. The provision of unique intelligence insights to policy and decision makers, directly contributes to building a safer and more prosperous Aotearoa New Zealand.

This section details many of our regular and enduring relationships across government, private sector and the community, as well as the importance of the Five Eyes partnership.

Government partners

DPMC's role in the NZIC

Our agencies work very closely with the National Security Group (NSG) in DPMC, which holds a collaborative leadership role within the national security community. The NSG leads on national security policy, including cyber security policy, and provides all-source strategic assessments on key issues and topics, often based on intelligence provided by our agencies.

The NSG's policy directorate operates in a similar way to how the Ministry of Justice provides policy advice about the operations of the New Zealand Police. The National Security Policy Directorate provides policy advice about the roles and functions of GCSB and NZSIS, to the Minister for National Security and Intelligence and to you as the agencies' responsible Minister. Cyber security policy has traditionally been part of the Digital Economy and Communications portfolio.

The NSG leads the development and coordination of the National Security Strategy, National Security Intelligence Priorities, and Ministerial Policy Statements, discussed in detail on page 49. It also acts as the lead for the implementation of any recommendations to the national security community arising from the Royal Commission of Inquiry into the Attack on Christchurch Mosques on 15 March 2019.

The National Assessments Bureau (NAB), which forms part of the NSG, provides strategic assessments to the Prime Minister, senior Ministers, and senior officials on international developments and events relevant to New Zealand's interests. The Director of NAB, is responsible for coordinating intelligence assessment and promoting standards of intelligence assessment across the national security community.

The Government's Response to the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain

After the 15 March 2019 terrorist attack, the Government set up a Royal Commission of Inquiry to investigate whether public sector agencies had done all they could to protect New Zealanders from terrorist attacks and whether more could be done. The report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain (RCOI) was released in December 2020. The report, *Ko tō tātou kāinga tēnei*, made 44 recommendations covering both national security, and wider social and community matters. The Government accepted the findings of the report and agreed in principle to the 44 recommendations.

The GCSB and NZSIS have continued to respond to relevant recommendations made by the RCOI through a range of initiatives such as the Indicators Framework ("Know the Signs") and the annual threat environment report, outlined above. Additionally, the NZSIS's Protective Security Requirements team refreshed the classification system in 2022 following the recommendation that public sector agencies should share information more widely. In particular, the RCOI referenced the need to classify information correctly and to use the need-to-know principle to enable rather than restrict information sharing. The 2022 changes have not fundamentally changed the classification system; rather they have introduced a change in emphasis to meet the RCOI recommendations.

DPMC leads the policy work to respond to the recommendations of the RCOI, working closely with GCSB, NZSIS and other agencies on national security community reform.

The response is led by the Lead Coordination Minister for the Government's Response to the RCOI. Kāpuia, the Ministerial Advisory Group was set up in 2021 in response to the RCOI report. Kāpuia provides independent advice to the Government on its response to the RCOI and both agencies have had regular interactions with the group.

Working with Defence

GCSB in particular, and the NZSIS, work in partnership with the New Zealand Defence Force to provide support to military operations, to provide force protection to New Zealand forces deployed overseas. s6(a)

s6(a)

s6(a)

Working with law enforcement

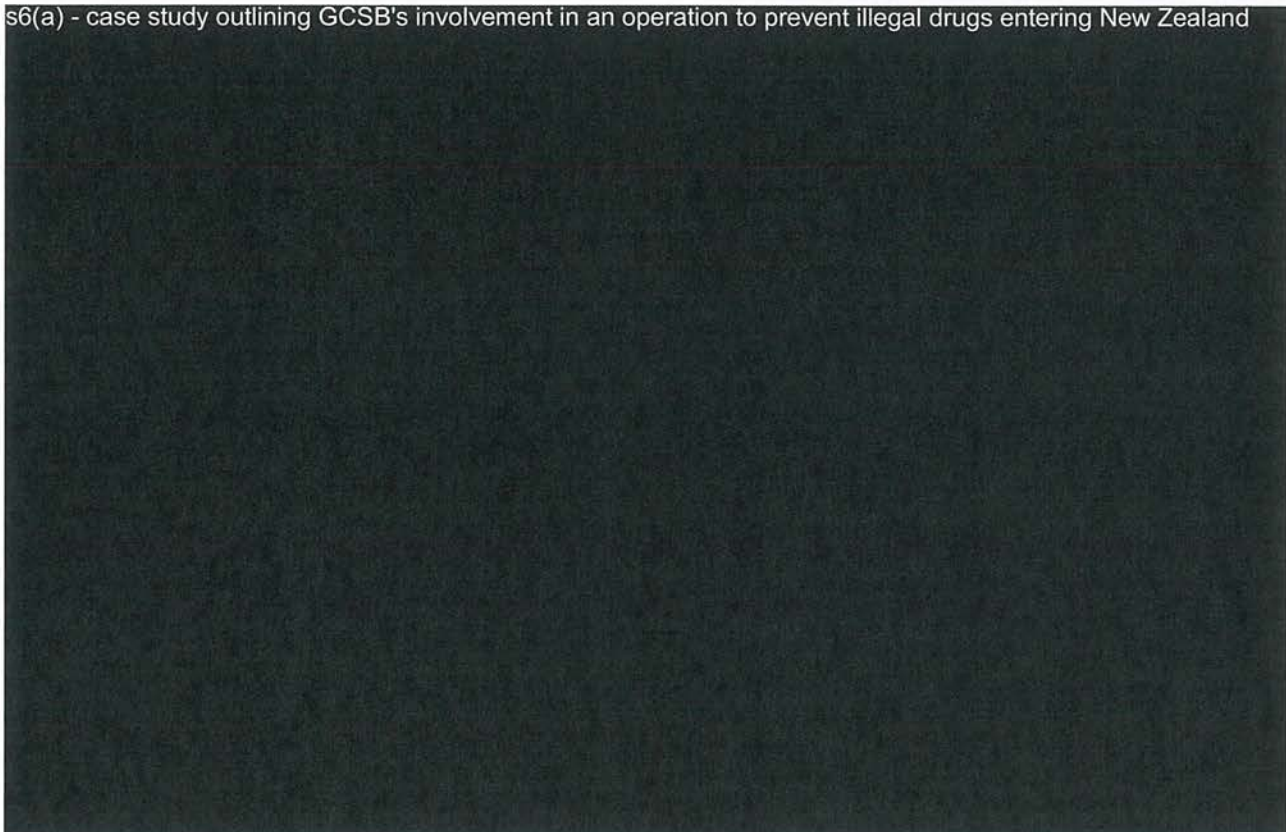
NZSIS in particular, and GCSB, work closely with a number of New Zealand law enforcement agencies, most prominently the New Zealand Police, to contribute towards domestic counter-terrorism and the identification of threats from extremist ideologies. One important way that NZSIS helps to keep New Zealanders safe is through investigating people who pose an actual or potential terror-related threat to New Zealand. The relationship between NZSIS and Police is essential in identifying, monitoring and mitigating New Zealand's terror threats. NZSIS and Police jointly manage the process of identifying and deconflicting threat information associated with extremist ideology and work together to mitigate threats using each agency's unique and complementary powers. We continue to seek out ways to strengthen our information-sharing practices with Police to keep improving how we share and manage lead information, so that we can more effectively respond to threats under our respective remits.

s6(a)

GCSB supports domestic and international efforts to counter transnational criminal activity targeting New Zealand, working with New Zealand Customs and New Zealand Police.

Through this work, GCSB contributes to efforts to counter transnational drug trafficking ventures, people smuggling and other criminal activity. The NCSC and New Zealand Police have recently established an exchange programme to support analysis of cyber incidents as a form of cyber crime. Both the GCSB and NZSIS receive leads from international partners and we pass these on to the appropriate domestic agencies.

s6(a) - case study outlining GCSB's involvement in an operation to prevent illegal drugs entering New Zealand



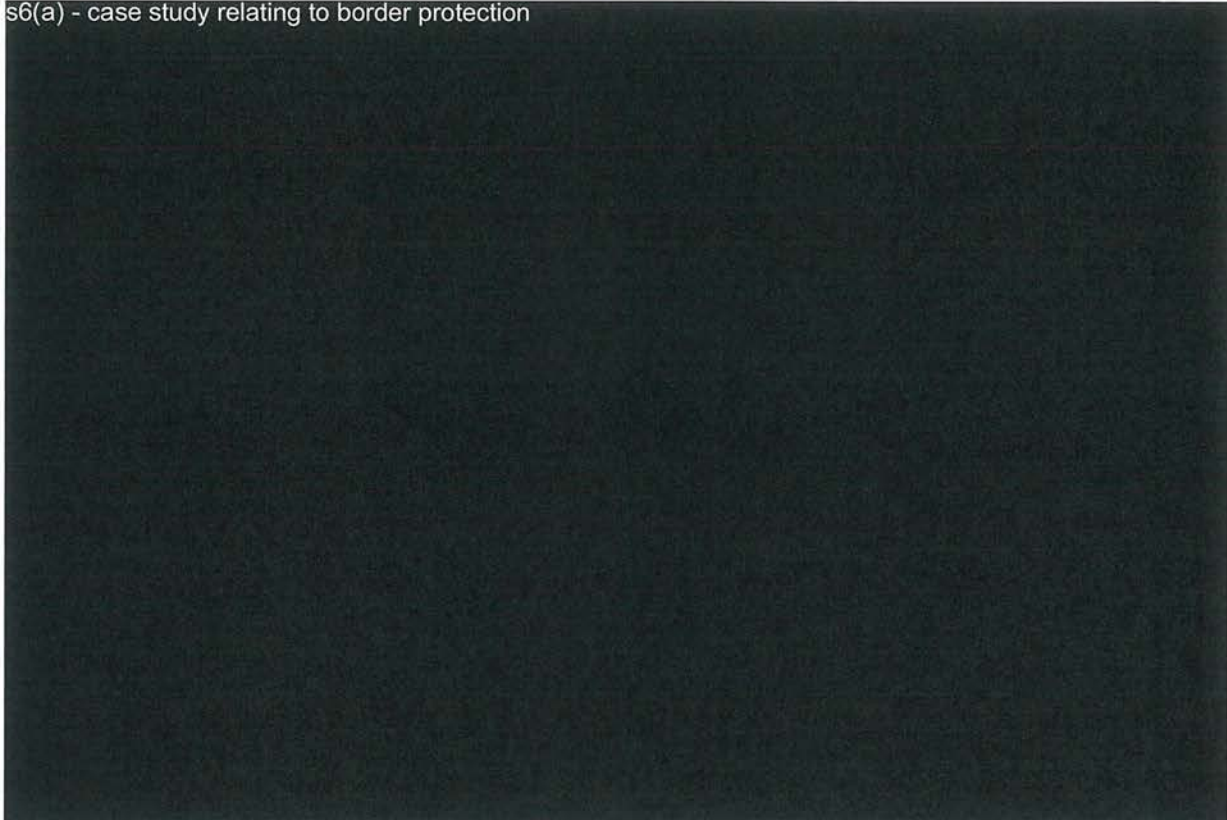
The Combined Threat Assessment Group

The Combined Threat Assessment Group (CTAG) is an interagency group hosted and led by the NZSIS. CTAG provides independent assessments to inform the national security community and wider government agencies of the physical threat posed by terrorism to New Zealanders and Aotearoa New Zealand's interests domestically and overseas.

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

As the host agency, the NZSIS brings together insight from across government agencies to ensure that the Director-General of Security has the best advice to set the national terrorism threat level 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.

s6(a) - case study relating to border protection



Border protection

NZSIS contributes to the management and protection of Aotearoa New Zealand's border by identifying and investigating national security threats in support of New Zealand's border security agencies, and in support of immigration decision making. NZSIS does this by providing advice about persons who attempt to enter Aotearoa New Zealand, or who apply for residency status and might represent a threat to national security. Between Immigration New Zealand and NZSIS, we identify travellers with links to international extremist groups, espionage activities or the proliferation of weapons of mass destruction technology.

National security clearances

To keep Aotearoa New Zealand safe we help our partners across the New Zealand Government decide whether they can trust someone with access to classified information or resources. We work to deliver real value and expertise so that our agency partners, candidates and clearance holders can trust our processes and take positive actions.

Regulatory roles across Government

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

TICSA requires network operators to ensure their public telecommunications networks have interception capability. It also requires network operators and services providers to assist the intelligence and security agencies to give effect to intelligence warrants. Under Part 3 of TICSA, the Minister Responsible for the GCSB and the Director-General, GCSB have a range of responsibilities concerned with keeping Aotearoa New Zealand's telecommunications networks secure. TICSA requires public telecommunications network operators to notify the GCSB if they are planning a network change within certain areas of specified security interest. Notifiable changes include the purchase or acquisition of equipment or services, changes to network architecture, or changes in ownership or control.

If a significant network security risk is raised by a notification, the Director-General GCSB may refer the matter to the Minister Responsible for the GCSB for a direction to prevent, reduce, or mitigate the identified network security risk. TICSA sets out a process for making such a direction, which includes consultation with the Minister for Communications and Information Technology and the Minister of Trade.

s6(a)



Overseas Investment Act 2005

Foreign direct investment in Aotearoa is broadly considered to provide positive outcomes for Aotearoa. However, occasionally foreign investment can involve risks, including national security risks that need to be balanced with benefits for Aotearoa New Zealand.

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

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

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

A core role for the GCSB and NZSIS 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 GCSB and NZSIS. For activities governed by the OSHAA, this national security risk advice is used to inform the Ministerial-level consultation required by the Act.

Radiocommunications Act 1989

The GCSB and the NZSIS provide advice to the Minister for Economic Development on the outcome of national security risk assessments in relation to issuing licenses for satellite ground stations. This is based on a direction under section 112 of the Radiocommunications Act 1989, which authorises the Radio Spectrum Management team within MBIE to see such advice. The Space Activities Risk Assessment Group coordinates advice provided in relation to these applications.

International partners

International intelligence-sharing arrangements are vital to Aotearoa New Zealand's national security and fundamental to how the GCSB and NZSIS carry out their functions. Aotearoa New Zealand could not deliver our security and intelligence activity alone. Our most significant relationship is as part of the Five Eyes partnership, but the global nature of threats is increasingly requiring engagement with a far broader number of partners.

At a technical level, the Five Eyes relationship provides access to advanced technology and tradecraft techniques that Aotearoa New Zealand could not develop on its own. We also get access to skills, training programmes, professional and security standards that would be difficult and expensive to source, or source at scale, in New Zealand.

The benefit of Aotearoa New Zealand's access to Five Eyes intelligence can often be an enhanced understanding of broad global trends as well as specific insight into a particular individual or situation. While intelligence information is regularly shared among groups and countries that are not part of the Five Eyes, the information we get from Five Eyes partners is more detailed, reliable and timely than tip-offs we might receive from others.

Everything we do is in accordance with Aotearoa New Zealand law, human rights obligations and government priorities.

s6(a)

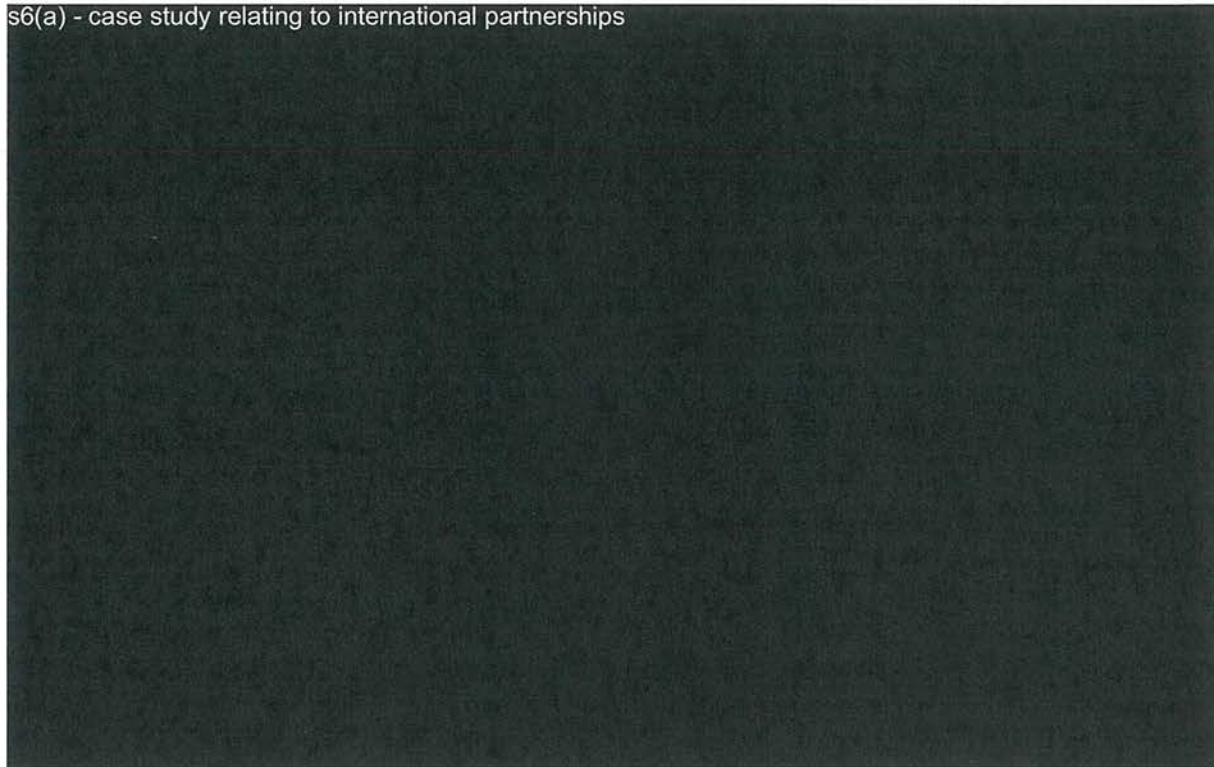


Working closely with our Pacific partners remains important to us. The Indo-Pacific region has seen increased geostrategic competition in recent years. This is reflected in the Government's NSIP 'New Zealand's strategic interests in the Indo-Pacific region.'

Under Ministerial authorisation, we also share intelligence with a range of other international counterparts, s6(a)

. These relationships are approached carefully and with regard to each country's human rights record.

s6(a) - case study relating to international partnerships



Public attribution statements

Public attribution statements are a tool used internationally to respond to malicious state-sponsored cyber activity. The key objective of public attribution is to deter states from engaging in this activity by strengthening international understanding of unacceptable state behaviour online. New Zealand has a vested interest in upholding the framework of responsible state behaviour in cyberspace and will publicly attribute when it is in our interests to do so.

The GCSB, acting on direction from responsible Ministers, has a history of joining like-minded partners in publicly calling out malicious cyber activity. New Zealand only attributes malicious cyber activity when it is in our national interest to do so. Incidents that may result in an attribution

include a partner's request for New Zealand to join a joint attribution statement, or a major cyber compromise affecting a New Zealand based entity.

If partners request support for a public attribution, the GCSB will engage in interagency consultation and provide you with the necessary advice to determine whether to direct the GCSB Director-General to make the attribution. Officials follow established processes to assess these requests, including engaging Ministers when necessary.

Private sector partners

New Zealand's private sector is well placed to benefit from the unique insights from the intelligence agencies on national security threats they may face. The NZSIS's Security Threat Environment report and the GCSB's Annual Cyber Threat report contain information that will be helpful for corporates to manage their own risk.

GCSB's NCSC's advice and services are not limited to national security – cyber security also encompasses digital transformation, emerging technology and critical infrastructure resilience.

Both agencies have best practice protective security advice on their websites that can be used to inform and improve other organisations' security posture. It is hoped we can build a security culture in New Zealand where best practice is adopted and concerning activities or behaviours of national security significance are reported.

The private sector is key in the GCSB's mission towards a cyber-resilient New Zealand. By providing them with high-quality cyber threat information that they can readily use to help protect their customers, in tandem with other commercial products, makes a real difference in the long term.

As explained earlier, GCSB works in partnership with internet service providers to deliver a capability called Malware Free Networks™. Malware Free Networks™ partners use our automated threat feed to detect and disrupt threats before they impact their customers' systems. They provide telemetry back to us, so we can understand the effectiveness of the MFN threat intelligence and gain greater understanding of the domestic cyber threat environment. Malware Free Networks™ now has 14 private sector partners who have live services utilising the Malware Free Networks™ threat intelligence; a range of other organisations have enquired about becoming a partner.

GCSB's NCSC was awarded the Public Service Commission's Spirit of Service – Te Tohu mō te Ratonga Whakahirahire, Service Excellence Award, and the overall Prime Minister's Award for its collaboration with industry partners to strengthen New Zealand's cyber defence capabilities.


Community partners

NZSIS is working to strengthen its relationships across a broad range of communities. The aim of these relationships is to develop a shared understanding about the work we do to keep New Zealanders safe as well as to build trust and confidence in our ability to do the job.

Protecting our national security is increasingly becoming a task we cannot afford to do alone. Information from members of the public could be vital for helping us to disrupt a potential threat. In order to facilitate that flow of information, we realise the importance of informing New Zealanders about the threats we face and talking about the types of behaviours that are concerning.

GCSB's NCSC plays a significant role by promoting good cyber security practice, receiving reports of cyber incidents, sharing information that supports New Zealanders to be more cyber resilient, and ensuring those incidents get to the right organisation for help. Community partners are important to ensure we reach a wide range of constituents to improve their cyber resilience.

s9(2)(ba)(i)




In August 2022, NZSIS hosted its first ever public meeting where flyers were distributed among the Christchurch Muslim community inviting them to a question and answer session with the Director-General. The event was a success and opportunities are being explored to host similar meetings in other locations in the future.

The NZSIS has relationships with a range of other communities and is conscious of the need to expand its reach to support those targeted by foreign interference activity for example.

There is a specific drive to improve our relationships with iwi Māori in order to become an honourable treaty partner and be in a stronger position to work together to improve national security outcomes.

Both agencies have been conducting their own engagement with iwi leaders and mana whenua on a programme to boost organisational capability on Te Ao Māori frameworks.

s9(2)(ba)(i)



PART FOUR

SUPPORT FOR THE FIRST 100 DAYS

The following section provides context on key issues, events or decisions that may support you in the first 100 days.

To further support you, we have developed a suggested set of written briefings providing an initial overview of our agencies, our functions and our work.

We will also provide you with classified threatscape briefings, s6(a)

s6(a)

In the first 100 days you will see

Intelligence and Security Committee

The Intelligence and Security Committee is likely to meet in early 2024 (February/March) for the 2023 Annual Review, which will consider the annual reports for the agencies. There will be both open and closed sessions to allow the committee to discuss classified information.

Full briefings will be prepared ahead of the meeting.

March Baseline Update

Baseline updates are a mechanism:

- for the Minister of Finance and the relevant appropriation Minister (“Joint Ministers”) to approve changes to appropriations that are fiscally neutral, technical, or do not involve significant policy change; and
- to reflect in baselines changes to appropriations previously approved by Cabinet or by Joint Ministers.

Preparation for the March Baseline Update will commence in early 2024.

Contingent liabilities register

Every six months (June and December) the Minister must certify that there are no additional contingent assets or liabilities that they are aware of, other than those contained in the register. We will be seeking this confirmation from you in February/March 2024.

Cyber attributions

As outlined on page 36, the GCSB, acting on direction from responsible Ministers, has a history of joining like-minded partners in publicly calling out malicious cyber activity. s6(a)

s6(a)

s6(a)

Payload permit briefings

Payload permits are granted by the Minister Responsible for the Outer Space and High-altitude Activities Act 2017 and administered by the New Zealand Space Agency. The Space Activities Risk Assessment Group (a New Zealand Intelligence Community working group comprising GCSB, NZSIS, NZDF and DPMC) undertakes a national security risk assessment in order to inform your consultation with the Minister Responsible for OSHAA. In the first 100 days you will receive a number of briefings informing you of the outcome of national security risk assessments for payload permits applied for under the OSHAA.

National Terrorism Threat Level

The National Terrorism Threat Level is reviewed annually, and the decision about setting the Threat Level is made by the Director-General of Security.

The annual process for reviewing the National Terrorism Threat Level has recently been completed, and on the basis of advice from the multi-agency Combined Threat Assessment Group, the Director-General decided that the Threat Level remains at Low: a terrorist attack is assessed as a realistic possibility.

You and the Prime Minister will receive a briefing note shortly formally informing you of the Director-General's decision and seeking agreement from the Prime Minister to the public notification of this decision.

s6(a)



s6(a)



Warrants and authorisations

s6(a) - outlines information the Minister will receive about warrant applications in the first 100 days



Key issues that may arise

s6(a)

Integration programme - lead operational cyber security agency

As outlined in the 'about us' section, CERT NZ was transferred to the GCSB's NCSC on 31 August 2023. The transfer brings together the NCSC's focus on state-sponsored malicious activity and national harm, with CERT NZ's focus on small to medium enterprises and the general public. The decision to bring these functions together was informed by input from a range of agencies across the private and public sectors that identified challenges in the previous multi-agency structure.

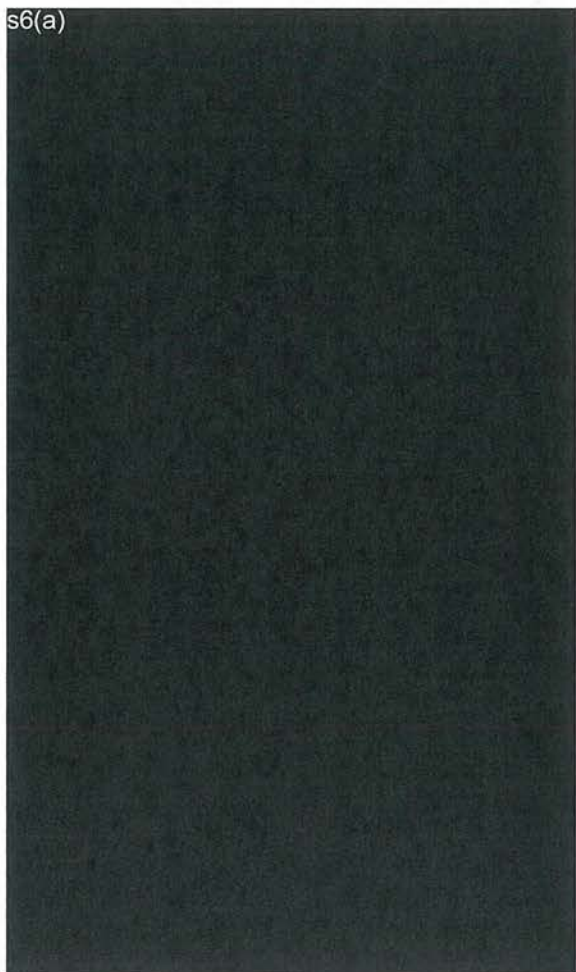
International reporting shows that sophisticated tools are more readily available to malicious cyber actors, increasing the risk of harm to New Zealanders. A joined-up agency consolidates our mandate and view of the operating environment, which will enable more authoritative guidance on how New Zealanders can protect themselves.

The initial transfer has been done from within existing baseline funding, as will the work to integrate functions. This work is focused on delivering the benefit of the consolidation of mandate and functions. s9(2)(f)(iv)

While work to integrate NCSC and CERT NZ functions occurs staff continue to deliver existing core services, so that customers receive ongoing support.

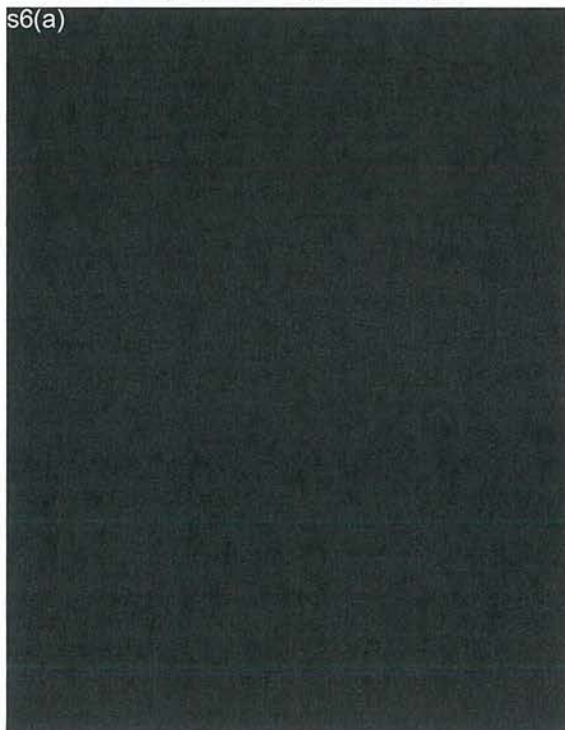
Pacific Regional Security

s6(a)



- Intelligence Cooperation involves intelligence diplomacy, including information sharing and joint investigations, as a reliable and trusted intelligence and security partner among Pacific counterparts.
- Intelligence Operations are required to identify national security risks in the Pacific region as a foundation for ongoing intelligence cooperation.
- Building Partner Capability efforts contribute to the maturing of intelligence and security practices and infrastructure among NZSIS's Pacific counterparts to improve their capability and capacity to manage geo-strategic challenges.

s6(a)



The NZSIS's Pacific Security Mission goals are pursued through three lines of effort, conducted in close coordination with domestic and foreign partners:

GCSB's CERT NZ delivers cyber capacity and capability training to 18 Pacific countries through the CERT NZ Pacific partnerships programme, funded by the Ministry of Foreign Affairs and Trade. The Pacific programme was established in 2019 and, since the ease of COVID-19-related restrictions, the programme has grown. Over the past year, the CERT NZ Pacific team has delivered multiple cyber upskilling sessions on incident response, communications, policy processes, and community engagement. Building on this success, they have supported the co-delivery of Cyber Smart weeks and awareness raising campaigns in Pacific countries. The team also advocates for the Pacific in cyber-related multilateral forums.

s6(a)

Data Centre

The s6(a) Data Centre is an all-of-government initiative that will provide infrastructure for s6(a) government agencies that rely on information systems to process information classified s6(a). The data centre will provide resilience and business continuity for the national security community in the event of a major earthquake and will provide sufficient capacity for storing classified information for up to 25 years.

The Data Centre is being constructed at RNZAF Base Auckland (Whenuapai). The GCSB, as the government lead for information security, will operate the facility on behalf of the range of government agencies that will use it.

Construction of the Data Centre is budgeted to cost around \$300 million, and the facility is expected to be operational by 2025.

s6(a)



Cryptographic infrastructure

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

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

s6(a)



s6(a)



Improvements to the National Security Screening System

The purpose of the National Security Screening System is to identify national security threats emerging from the intended migration of individuals to New Zealand, while providing assurance to the New Zealand Government and general public. The current system takes a broad s6(a) approach to screening. This approach is not agile enough to effectively respond to a dynamic security environment and future customer requirements.

The NZSIS has set up a programme s6(a), to improve the National Security Screening System by introducing a risk-based model that will enable us to focus our resources on high value/high risk assessments, providing a greater chance of identifying the individuals who pose a realistic and detectable threat to New Zealand. s6(a) will create a more agile, future proofed system that can effectively respond to a dynamic security environment and changing customer requirements. Through this initiative, our overarching goal for the future is to ensure the system has the capacity and capability to meet both immediate and future needs. The NZSIS will be able to scale delivery of proportionate assessments that provide clear, well understood, transparent assessment outcomes. Through s6(a) we will be also able to increase the speed of low risk assessments, providing a faster experience overall to those who do not pose a higher probable risk and do not require further assessment.

Government Chief Information Security Officer

The Director-General of GCSB is also the Government Chief Information Security Officer (GCISO).

The purpose of the GCISO is to enhance the capability of the public services to move at pace with modern tools, technology and wider changes in the digital environment such as Cloud adoption, federated data, artificial intelligence and digital identity. The GCISO draws on the technical expertise, relationships, and unique insights of the GCSB to uplift information security practice across government.

In 2022 the GCISO was designated a System Lead under the Public Service Act 2020. System leads are mandated to lead across the Public Service in relation to a particular area or function. They do this by creating a common vision for the future, setting standards and frameworks for agencies to operate within, co-ordinating and supporting best practice and looking for opportunities to work better together.

In Budget 2023 GCSB received \$13.2 million of new funding over the next four years for the National Cyber Security Centre to deliver on two related government priorities:

- \$3.956 million for operationalising the mandate for the Government Chief Information Security Officer (this funding is in a tagged contingency, with draw-down subject to a report-back to Cabinet on the expansion of the mandate, which we will brief you on separately); and
- \$9.232 million for technical advice and engagement to improve the cyber resilience of critical national infrastructure.

Protective Security lead

The Director-General of Security holds the role of Government Protective Security Lead (GPSL). Through this role, the Director-General provides protective security leadership, guidance, and support for chief executives, organisations, and systems across New Zealand.

The aim of the Government Protective Security Lead is to improve the overall resilience of organisations' security. The GPSL helps chief executives meet their responsibilities for protecting their organisations and addressing security risks.

Following the last round of Protective Security Requirements assurance reporting in 2022, the NZSIS's Protective Security Requirements unit engaged with agencies to query whether the current self-assessment model remained fit-for-purpose. While the fundamentals of the Protective Security Requirements remain sound, the assurance framework is complex and cumbersome for agencies to use and it does not reduce to the fullest extent possible the risk of inaccuracy and bias inherent in a self-assessment model.

To address these findings, a multi-year project (over the period to 2026) will be undertaken to clarify and better explain the requirements of the Protective Security Requirements and to simplify the assurance framework.

Upcoming policy work with other agencies

The GCSB and the NZSIS play a significant role in providing advice on, and input into, a range of policy work led by other agencies. While other agencies are responsible for managing national security risks within their portfolio responsibilities, we play an important role in informing the Government of the threat environment, providing advice on protective and cyber security, and conducting national security assessments to help mitigate these risks. We have a particular interest in ensuring that legislative and other changes reflect national security interests. More detail on the broader National Security Community work programme is referred to in DPMC's briefing to the incoming Minister for National Security and Intelligence, but key examples of upcoming policy work are set out below.

Intelligence and Security Act review

The Intelligence and Security Act 2017 requires periodic reviews. The first review was completed on 31 January 2023. This review was brought forward to address issues raised by the RCOI. The NZSIS and GCSB provided information to assist the reviewers to conduct their review. The review's report, Taumaruru: Protecting Aotearoa New Zealand as a free, open and democratic society, was made publicly available in May 2023. The report has 52 recommendations on a range of matters.

The Government response to the report is in the early stages and has been jointly led by the Prime Minister, as the Minister for National Security and

Intelligence, and by the Minister Responsible for the NZSIS and the GCSB. DPMC is the lead agency for the policy work to respond to the review, informed by and working closely with the GCSB and NZSIS. The agencies' focus is on ensuring the legislation remains clear, effective and fit for purpose, and we have a particular interest in the

s9(2)(g)(i)

We will provide you with briefings on key areas and recommendations from our agencies' perspective as this work continues.

Foreign interference and espionage

As part of a cross-Government programme, the GCSB and the NZSIS have been raising awareness about foreign interference risks across multiple sectors, including central government, to support agencies in identifying and building resilience to these threats in their policy work. Key policy work that will support the response and management of foreign interference and espionage in New Zealand includes

s9(2)(f)(iv)

Space security

In May 2023, the New Zealand Space Agency (NZSA) published Aotearoa New Zealand's first National Space Policy which provides an overview of the Government's values and objectives on space. This includes protecting and advancing New Zealand's national security interests, using space assets to protect and advance New Zealand's national security, understanding and managing the broad range of security risks in space and on Earth, and enhancing collaboration with international space and security partners.

The New Zealand Space Agency is the lead for space policy, regulation and sector development, working closely with GCSB, NZSIS and other agencies to address national security risks and matters contrary to New Zealand's national interest.

Work on a number of regulatory regimes is underway, as recommended in the statutory review of the Outer Space and High-altitude Activities Act 2017 and as directed by Cabinet.

s6(a)



Emerging, critical and sensitive technology

Emerging technologies have raised potential national security concerns for New Zealand. It is critical that the Government understands, and has the tools to manage, the range of risks and opportunities that technologies such as artificial intelligence and quantum computing present for Aotearoa New Zealand, and specifically for the GCSB and the NZSIS. The Ministry of Business, Innovation and Employment, and DPMC co-lead the policy work underway to address these issues.

s6(a)



PART FIVE

STRATEGY, POLICY AND ACCOUNTABILITY

National Security Intelligence Priorities

The National Security Intelligence Priorities – Whakaarotau Marumaru Aotearoa – define where intelligence should support government to make informed decisions about national security.

The 2023 National Security Intelligence Priorities were approved by Cabinet in June 2023. They help us to understand and take action on the national security issues, threats, and drivers of instability set out in *Secure Together, Tō Tātou Korowai Manaaki: New Zealand's National Security Strategy 2023 – 2028*.

The National Security Intelligence Priorities are:

1. Economic security
2. Emerging, critical and sensitive technology
3. Foreign interference and espionage
4. Malicious cyber activity
5. Maritime and border security
6. National security implications of climate change
7. National security implications of disinformation
8. New Zealand's strategic interests in the Indo-Pacific region
9. Pacific resilience and security
10. Space security
11. Strategic competition and the rules-based international system
12. Terrorism and violent extremism
13. Threats to New Zealanders overseas
14. Transnational serious and organised crime

The National Security Strategy

Aotearoa New Zealand's first National Security Strategy, *Secure Together, Tō Tātou Korowai Manaaki: New Zealand's National Security Strategy 2023-2028* (the Strategy), was agreed by Cabinet and released in August 2023. The Strategy provides overarching direction to the national security community, led by DPMC's National Security Group.

The Strategy sets out a vision for a secure and resilient New Zealand, describes our security outlook, and articulates a set of national security interests, outcomes, priorities, and principles. The Strategy describes the government's work in protecting New Zealanders through the management of 12 core issues – the issues that the national security community works on every day – and identifies broader drivers of insecurity such as climate change and social instability.

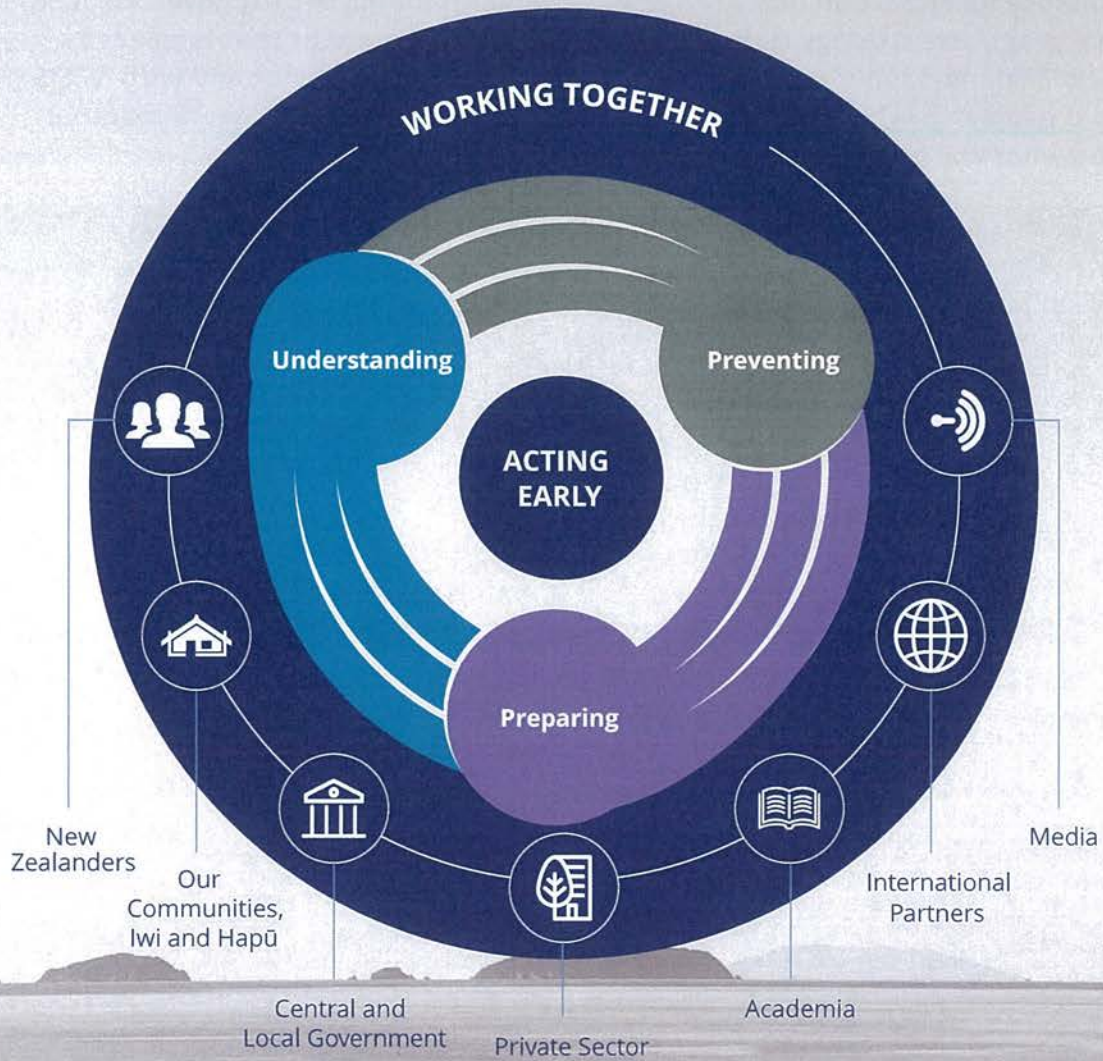
The Strategy's priorities, reflected in its Programme of Action, form the heart of the Strategy and drive the work of the national security community. These priorities are:

- **Acting early** to prevent national security threats and build New Zealand's resilience.
- **Working together** to foster collective understanding and approaches. This includes working across New Zealand society as well as internationally to build trust, understanding, and resilience.
- **Leading an integrated approach** with clear leadership and accountabilities, integrated advice, and a system-wide approach to capabilities. This will be led by Chief Executives across the national security community.

The NZSIS and GCSB have recently refreshed their organisational strategies to ensure we remain on course to address the challenges that have emerged in recent years. Our strategies align with the National Security Strategy.

The agencies have also developed a joint statement of purpose, to articulate how we work together to deliver on our common goal of ensuring we have a secure and resilient Aotearoa New Zealand, one that is protected as a free, open and democratic society for future generations.

The National Security Strategy

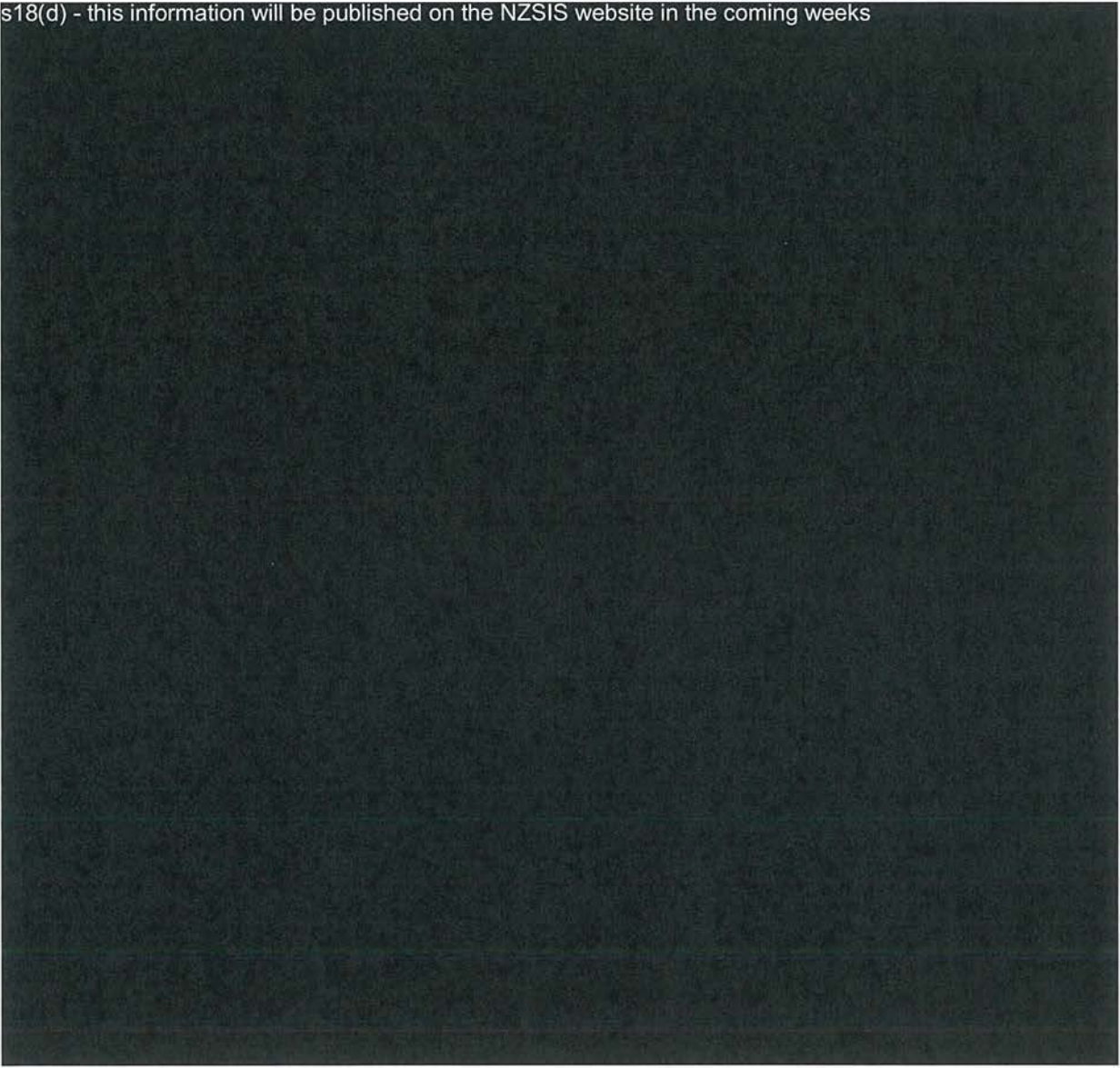


To be effective, each element requires the right capabilities, legislation and regulation, structures, and partnerships.

NZSIS Strategy 2024-2029

The NZSIS has refreshed its strategy to set a direction for how it intends to enhance its impact on Aotearoa New Zealand's national security over the next five years. The strategy is designed to be a public document that is clear to New Zealanders, our colleagues in the national security sector and with NZSIS's own people on what we aim to deliver for them, where we can work together and what will be our main areas of focus.

s18(d) - this information will be published on the NZSIS website in the coming weeks



NZSIS Strategy 2024-2029

s18(d) - this information will be published on the NZSIS website in the coming weeks

NZSIS Strategy

FOCUS AREAS

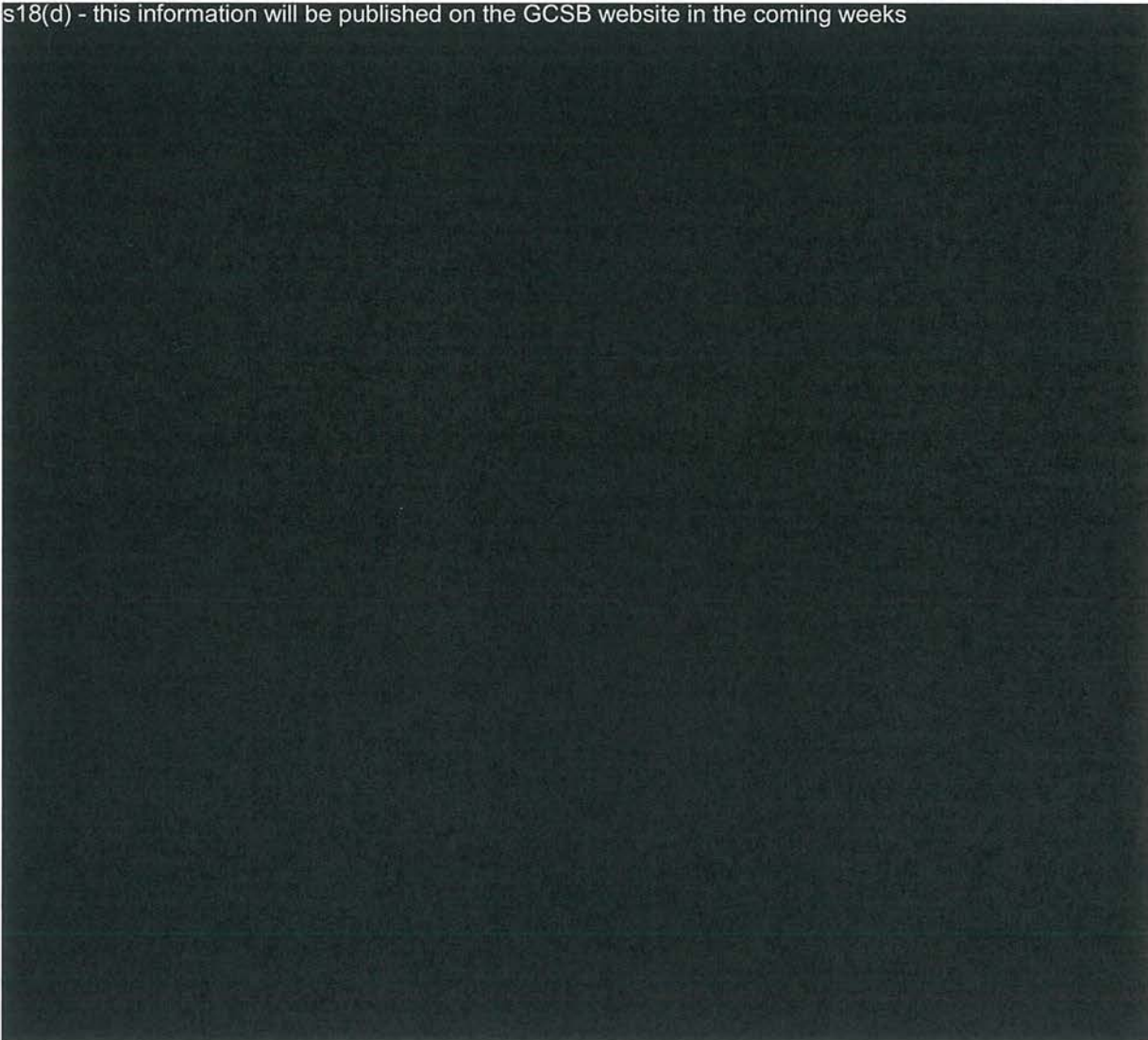
2024-2029

s18(d) - this information will be published on the NZSIS website in the coming weeks

GCSB Strategy 2023-2027

GCSB has developed a new organisational strategy, which took effect from 1 July 2023. The GCSB Strategy sets out the contribution GCSB can make to Aotearoa New Zealand's national security and economic wellbeing over the next four years, guiding activities between now and 2027.

s18(d) - this information will be published on the GCSB website in the coming weeks



GCSB Strategy 2023-2027

s18(d) - this information will be published on the GCSB website in the coming weeks

Ministerial Policy Statements

Provided for by the ISA, Ministerial Policy Statements (MPSs) are a mechanism that enables the responsible Minister to set out their expectations about the appropriate conduct of lawful activities by the GCSB and NZSIS. As MPSs only apply to lawful activities, they do not serve to authorise the activities but rather provide guidance as to the parameters of appropriate behaviour.

Eleven MPSs (required under sections 206 and 207 of the ISA) came into effect in March 2022 for a period of three years. They relate to:

- Information assurance and cybersecurity activities
- Assumed identities
- Legal entities
- Collecting human intelligence
- Conducting surveillance in a public place
- Publicly available information
- Section 121 requests
- Information management
- False or misleading representations about employment
- Road user rule exemption
- Cooperating with overseas public authorities.

The responsible Minister may amend, revoke or replace a Ministerial Policy Statement at any time (subject to the consultation requirements under the ISA)³. You are also able to issue Ministerial Policy Statements to provide guidance about any additional matter.

³ When issuing, amending, revoking or replacing a Ministerial Policy Statement, the responsible Minister must consult with the Inspector-General of Intelligence and Security, any other Minister of the Crown whose area of responsibility includes an interest in the proposed Ministerial Policy Statement, or any other person the Minister considers appropriate.

GCSB's and NZSIS's oversight and accountability framework

The ISA sets out the key parts of GCSB's and NZSIS's oversight and accountability framework. Through independent oversight, a balance is struck between the secrecy necessary for the agencies to operate effectively and the public's expectations of accountability and transparency. Our overarching oversight and accountability framework has multiple layers, which are described below.

Executive / Ministerial


The Minister Responsible for the GCSB and NZSIS oversees day-to-day business and approves warrant applications brought by the agencies.

The Minister for National Security and Intelligence oversees the national security community. There is a legislative requirement to review the intelligence agencies and the ISA five years after the commencement of the ISA and periodically thereafter.

As outlined earlier in this briefing, the first review of the ISA was completed on 31 January 2023. The Government response to the report is being jointly led by the Prime Minister, as Minister for National Security and Intelligence and the Minister Responsible for the NZSIS and the Minister Responsible for the GCSB. DPMC administers the ISA and is the lead agency for responding to the review. We are supporting them with this work.

In the previous administration, the Cabinet External Relations and Security Committee (ERS) provided oversight on national security matters on behalf of Cabinet. ERS was chaired by the Prime Minister and had responsibility for a wide range of issues, including foreign affairs and defence deployments.

s9(2)(g)(i)



Parliamentary

The Intelligence and Security Committee (ISC) is our parliamentary oversight committee. The Committee is established by the ISA, with members appointed by the Prime Minister and Leader of the Opposition, in consultation with other party leaders in Parliament. DPMC will advise the Prime Minister on establishing the ISC early in the Parliamentary term. The functions of the ISC are outlined in section 193 of the ISA.

Accountability documents ordinarily presented to the House of Representatives (annual reports, Estimates of Appropriations, statements of strategic intent) are instead provided with classified material to the ISC.

Inspector General of Intelligence and Security (IGIS)

The IGIS is a statutory officer providing independent external oversight and review of the intelligence and security agencies.

The IGIS' work involves:

- Investigating complaints about the NZSIS and the GCSB
- Conducting inquiries and reviews into the activities of the agencies
- Reviewing all warrants and authorisations issued to the intelligence and security agencies
- Receiving protected disclosures relating to classified information or the activities of the intelligence and security agencies
- Providing advice on matters relating to oversight of the intelligence and security agencies, including input into the development of relevant government policy

The full functions of the IGIS are detailed in section 158 of the ISA.

The Minister Responsible for the GCSB and the NZSIS, the Prime Minister, or the ISC can ask the IGIS to conduct an inquiry into the matters provided for in the ISA; however the IGIS mostly initiates inquiries on their own initiative.

The Inspector-General will generally conduct an inquiry if a matter requires in-depth investigation, such as interviewing witnesses. The IGIS may also decide to conduct an inquiry into a complaint received about the agencies.

A review will generally be less formal than an inquiry and will usually involve the IGIS selecting an area of an agency's work for examination and assessment.

A classified report is produced at the end of an inquiry or review and provided to the relevant agency and the Minister responsible for the agency. The report may include findings and recommendations about actions that the IGIS considers the agencies should take. A public report will also usually be prepared that does not involve classified information, for publication on the IGIS website.

The IGIS is supported to perform their role by a statutorily appointed Deputy IGIS and a team of approximately six employees. The current Inspector-General is Brendan Horsley. He was appointed in June 2020 for a five year term.

General

The Minister and the agencies are subject to the courts, including through judicial review. The agencies are also subject to oversight and review by:

- The Privacy Commissioner;
- The Ombudsman; and
- The Auditor-General.

PART SIX

ORGANISATIONAL HEALTH

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

In recent years we have faced workforce disruptions from COVID-19, building remediation and increased competition from public and private sectors for the skills and expertise of our people.

The last few years presented their share of challenges for business continuity, with the building disruptions being a significant one. The seismic strengthening remedial work at Pipitea House on Pipitea Street in Wellington has been completed; with the building now back to full occupancy.

s6(a)



In response to high staff turnover, we revised the Joint Remuneration Policy this year, which introduced a number of new provisions to ensure our people can be paid fairly for their skills, experience, and performance in their role.

We continue to prioritise initiatives to attract and retain a diverse workforce, including competitive remuneration, closing gender and ethnic pay gaps, enabling more flexible working, investing in employee development and fostering an inclusive culture.

GCSB runs a graduate programme and the agencies both participate in the Ministry for Ethnic Communities Graduate Programme. GCSB also have a Women in Stem scholarship for students studying cyber security, technology, mathematics, data science, computer engineering or computer science. NZSIS has also commenced its own graduation programme this year.

More information on the organisational health of the GCSB and NZSIS, our diversity strategy and our ongoing efforts to ensure the health and safety of our employees is available in our annual reports. We can brief you on these initiatives in greater detail.

PART SEVEN

HOW WE WILL SUPPORT YOU

This section contains some suggestions based on current practice, for how we could provide day-to-day support to your office.

Directors-General

We are available at all times. We will inform you of any travel commitments that we have and when acting arrangements are in place.

Regular meeting schedule

The GCSB and NZSIS's recent practice has been to hold ~~s6(a)~~ meetings with the responsible Minister. These meetings are attended by the respective Director-General and members of our Senior Leadership Teams, as well as specialist

briefings as required. The meetings need to be held in ~~s6(a)~~

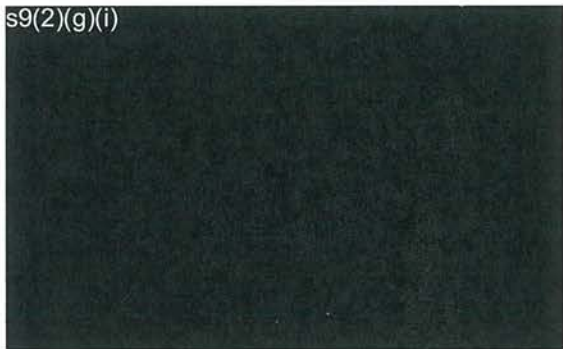
~~s6(a)~~ to ensure our classified information is protected. The meetings cover emerging policy and operational issues, matters coming before Cabinet committees, upcoming media issues, and matters relating to the organisational health of the agencies. They are also used to brief the Minister on warrant applications. We recommend these arrangements continue.

Responsibilities to the Prime Minister, Leader of the Opposition and Ministers

Prime Minister

We have responsibilities to the Prime Minister, as Minister for National Security and Intelligence. Our relationship with the Prime Minister is independent of their portfolio responsibilities for DPMC's national security function.

s9(2)(g)(i)



Minister for Digitising Government

We will also work with you in your role as Minister for Digitising Government. Cyber security is a core national security issue, and opportunities to enhance New Zealand's security and resilience against cyber threats need to be prioritised, given the potential impact of malicious cyber activity.

Cyber security policy is currently coordinated within the National Cyber Policy Office (NCPO), which sits within the National Security Group in DPMC. Cyber security operational services are provided by the GCSB's NCSC, and CERT NZ, which recently transferred to the GCSB. We would appreciate discussing the scope of this role at an early opportunity.

Leader of the Opposition

We have statutory responsibilities under the ISA to the Leader of the Opposition. This requirement strengthens bipartisan understanding of national security issues and reinforces the political neutrality of the security and intelligence agencies.

In accordance with our statutory responsibilities, our recent practice has been to brief the Leader of the Opposition s6(a) . We keep the Leader of the Opposition informed on the same national security matters on which we brief the Prime Minister, with some exceptions. The Director-General of Security also briefs leaders of political parties on any national security matters relevant to their party, such as foreign interference.

We propose to provide an initial brief to the Leader of the Opposition shortly after our first meeting with you and the Prime Minister.

Responsibilities to other Ministers

Our statutory functions also mean the Minister for Trade and the Minister for Communications may become involved in decisions made in accordance with the Telecommunications (Interception Capability and Security) Act 2013 relating to network security risks.

We also support the Outer Space and High-altitude Activities Act 2017 regulatory regime, which has been overseen by the Minister for Economic Development. You have a statutory role in respect of national security checks that are carried out on launch vehicles and payloads.

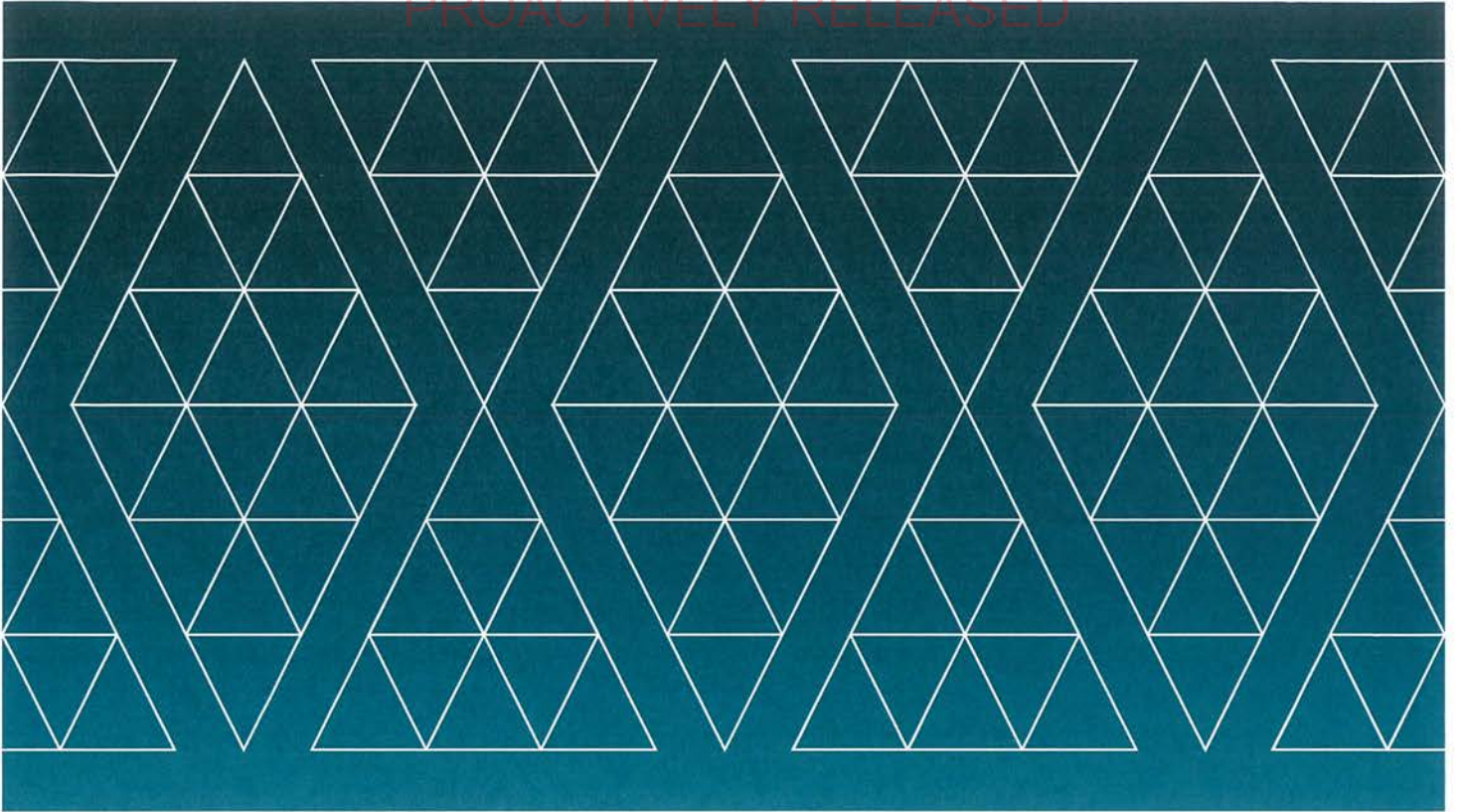
Private Secretary

GCSB and NZSIS currently provide a Private Secretary to the Office of the Minister Responsible for the GCSB and the NZSIS. Given the importance of this role, we ensure this person is an experienced staff member with knowledge and experience of our agencies. This arrangement means that you and your staff have an immediate source of advice and contact into our agencies. It also streamlines some of the security arrangements associated with handling highly classified material. We recommend this arrangement continue.

Strategic Direction, Governance and Policy Directorate

The Strategic Direction, Governance and Policy Directorate (SDGP) is responsible for providing day-to-day service to staff in your Office, and is led by Bridget White, who has regularly acted as Director-General for the GCSB. SDGP is a joint function and comprises three teams: Strategy, Policy and Ministerial Services; International Engagement; and Communications. SDGP will work with your office to establish your expectations about the frequency and nature of reporting we provide you, the management of Official Information Act 1982 and Privacy Act 2020 requests, and oral and written Parliamentary questions.

PROACTIVELY RELEASED



Te Tira Tiaki
Government Communications
Security Bureau



Te Pā Whakamarumarū
New Zealand Security
Intelligence Service