

Briefing to the Incoming Minister

Minister Responsible for the GCSB and
Minister Responsible for the NZSIS

2017



Contents

Welcome	4	PART 4:	
Overview	7	International partnerships	19
PART 1:		PART 5:	
New Zealand's threatscape	8	Our support to you	21
Cyber threats	8	Directors-General	21
Violent extremism	9	Private Secretary	22
Espionage	10	Joint Directors-General Office	23
Regional stability – the South Pacific	11	Decisions in the first three months	23
PART 2:		GCSB	24
Transforming how we work	12	About GCSB	24
A community approach to intelligence and security	12	GCSB Strategic Plan 2016-2020	25
Core components of investment in GCSB and NZSIS	13	GCSB's functions	25
Collaborative intelligence collection and analysis	14	Intelligence collection and analysis	26
PART 3:		Information assurance and cyber security ...	30
Intelligence and Security Act 2017	17	Additional statutory functions	33
Your statutory role under the ISA	17	Co-operation with other entities to facilitate their functions or respond to an imminent threat	34
Oversight	17	GCSB's people	35
		Senior Leadership Team	35

NZSIS38

About NZSIS..... 38

NZSIS Operational Strategy **S6(a)** 38

NZSIS's functions..... 40

Intelligence collection and analysis..... 40

Protective security services and vetting 42

NZSIS's people 44

NZSIS's Senior Leadership Team..... 45

Welcome

Dear Minister

Congratulations on your appointment as the Minister Responsible for the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS).

GCSB and NZSIS are New Zealand's security and intelligence agencies. Our new legislation, the Intelligence and Security Act 2017 (ISA), confers three key objectives on the agencies. These are to contribute 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.

At their core, these objectives are concerned with three main things. The first is keeping New Zealand and New Zealanders safe from significant national security threats. These threats include cyber attacks, terrorism, espionage (both against the New Zealand Government and New Zealand businesses and institutions), and offshore political or civil unrest that New Zealanders may be caught up in. Our functions allow us to covertly identify, investigate and report on these threats and risks. Sometimes we do this alone, but often our role

is to support New Zealand's law enforcement agencies and the New Zealand Defence Force.

Our agencies' second area of focus is preserving New Zealand's competitive advantage. This means using intelligence to help make sense of New Zealand's position in the world – this assists decision makers to manage risks and maximise opportunities relevant to New Zealand's interests.

Our agencies also play a key role in keeping secure the information, assets and personnel of the New Zealand Government and nationally significant organisations such as key economic generators, operators of critical infrastructure and owners of valuable intellectual property. Safeguarding these areas is an important enabling factor in New Zealand's economy and international relations.

NZSIS and GCSB are Public Service departments. Accordingly, we are accountable to the Government of New Zealand and act in the interests of New Zealand and New Zealanders. Everything we do needs to be in accordance with New Zealand law and our international human rights obligations. We are subject to a high level of independent oversight and scrutiny, primarily from the Inspector-General of Intelligence and Security, but also from the Commissioner of Intelligence Warrants,

the Chief Ombudsman, the Privacy Commissioner and the Auditor-General. The Intelligence and Security Committee of Parliament also scrutinises our expenditure, policy and administration.

GCSB and NZSIS, together with the Security and Intelligence Group within the Department of the Prime Minister and Cabinet (DPMC), operate as “the New Zealand Intelligence Community” (NZIC).

The NZIC is just over one year into a four year transformational change programme. The foundations of this change can be found in the 2015 Independent Review of Intelligence and Security in New Zealand and a review of our agencies’ resourcing and capability.

Together, these reviews required the NZIC to go back to first principles and consider how we could rebuild ourselves as modern, connected, customer-centric, and effective security and intelligence agencies that have earned the trust and confidence of New Zealanders.

Our work towards this aim is now well underway:

- GCSB and NZSIS have new joint empowering legislation - the ISA. The ISA was passed with bipartisan support from across the House;
- As part of the New Zealand Government’s 2016 Budget, we received significant new funding spread over four years. This funding is critical to our ability to deliver our functions and stay ahead of New Zealand’s evolving threatscape;
- GCSB and NZSIS are working together more closely than ever before from a corporate standpoint; for example, the increased investment in our agencies is jointly governed and we share all corporate functions;
- Operationally, we are also much more connected, particularly in relation to our intelligence collection

functions, protective security and management of insider threats; and

- We are implementing a joint programme of work to improve the value that Ministers and relevant government departments receive from our intelligence products.

While much of the work referenced above concerns organisational health, we are also building capability in support of New Zealand’s National Intelligence Priorities (NIPs), which are set every twelve to 24 months by the Government. We have made progress against each of the NIPs, with particularly strong performance improvements in the areas **S6(a)**

S6(a) Feedback from our domestic and international partners on the results they are seeing from increased investment in the NZIC has been positive.

We continue to maintain a high operational tempo. We plan to provide you and the Prime Minister, as the Minister for National Security and Intelligence, with a series of more in depth briefings about our operational activities over the coming weeks.

We are growing in a careful and sequenced way, but the scale and pace of change, together with the nature of the threats New Zealand faces mean that risks will always remain.

We could not do our job without the support we receive from our Five Eyes partners. **S6(a)**

[REDACTED]

This briefing is intended to provide 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 GCSB and NZSIS. Finally, it suggests how we can support you, subject to your preferences. We will work with you and your office to tailor a series of more detailed briefings on our functions and current operations.

We look forward to working with you.

Yours sincerely



Andrew Hampton

Director-General, GCSB



Rebecca Kitteridge

Director-General of Security, NZSIS

Overview

The purpose of this briefing is to provide you with a high level overview of:

- New Zealand's threatscape;
- How our agencies use their lawful functions under the ISA 2017, and other legislation, to respond to that threatscape and generate national advantage; and
- How we are maximising the investment that has been made in the New Zealand Intelligence Community.

This briefing will be supplemented with more detailed and operationally focused briefings over the coming months. We have outlined a proposed briefing schedule in Part 5 of this briefing.

The first five parts of this briefing are focused on how GCSB and NZSIS work together. The later sections of this briefing are focused on GCSB and NZSIS as individual agencies. Included in these sections is the "how, what and why" of our intelligence collection, analysis and advisory functions.

PART 1:

New Zealand's threatscape

This section sets out the context for our agencies' work. It outlines four core national security threat areas (cyber, violent extremism, S6(a) and espionage) which together provide an overview of New Zealand's threatscape. We will provide more in depth briefings on each of these areas over the coming weeks.

As Directors-General, we are making a concerted effort to raise, in a responsible way, public awareness about New Zealand's threatscape, particularly in relation to cyber and the counter-terrorism profile.

Cyber threats

New Zealand is dependent on information and communication technology. Maintaining the integrity, availability and confidentiality of information in the networks and systems that make up cyberspace is vital to modern life.

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 mutating and

multiplying to adapt to new technology or security measures.

New Zealand faces both direct and indirect cyber threats. Direct threats deliberately target New Zealand, such as cyber espionage targeting New Zealand government departments. Indirect threats include, for example, indiscriminate cyber operations that do not target New Zealand but can harm us nonetheless.

The past year has been notable for the number and breadth of high profile global cyber incidents:

WannaCry, S6(a)

NotPetya S6(a)

These incidents were among the largest of their nature ever seen. In these instances, the impact on New Zealand was limited but the potential for future events of this kind to have a domestic impact is high.

S6(a)

Direct threats

S6(a)



Indirect threats

New Zealand is exposed to indiscriminate phishing and scanning by state-sponsored actors including

S6(a)



Violent extremism

The counter-terrorism environment in New Zealand is still dominated by the influence of the so-called Islamic State of Iraq and the Levant (ISIL). At any one time over the past three years, between 30 and 40 people have been listed on NZSIS's counter-terrorism risk register. These individuals are assessed to represent an actual or potential threat to New Zealand related to terrorism, for example, those seeking to carry out a domestic terror attack, foreign terrorist fighters, or individuals providing financial or facilitation support.

Violent extremist ideology and messaging, primarily accessed through online content and social media platforms, continues to resonate with a small number of individuals in New Zealand. NZSIS continues to investigate individuals for supporting or attempting to join ISIL in Syria and Iraq. NZSIS also provides security information to support passport cancellations. The provision of this information helps to support United Nations resolutions preventing travel by foreign terrorist fighters.

S6(a)



S6(a)

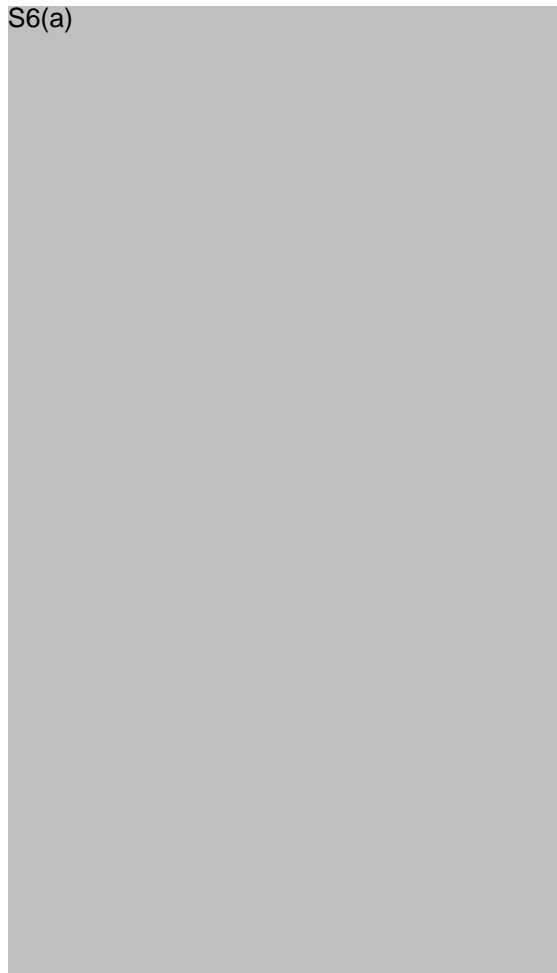


Terrorist attacks have continued - especially in Europe and the UK. These have been both sophisticated and rudimentary, often targeting places

of mass gathering and busy city streets, using weapons which are easily acquired. S6(a)



S6(a)

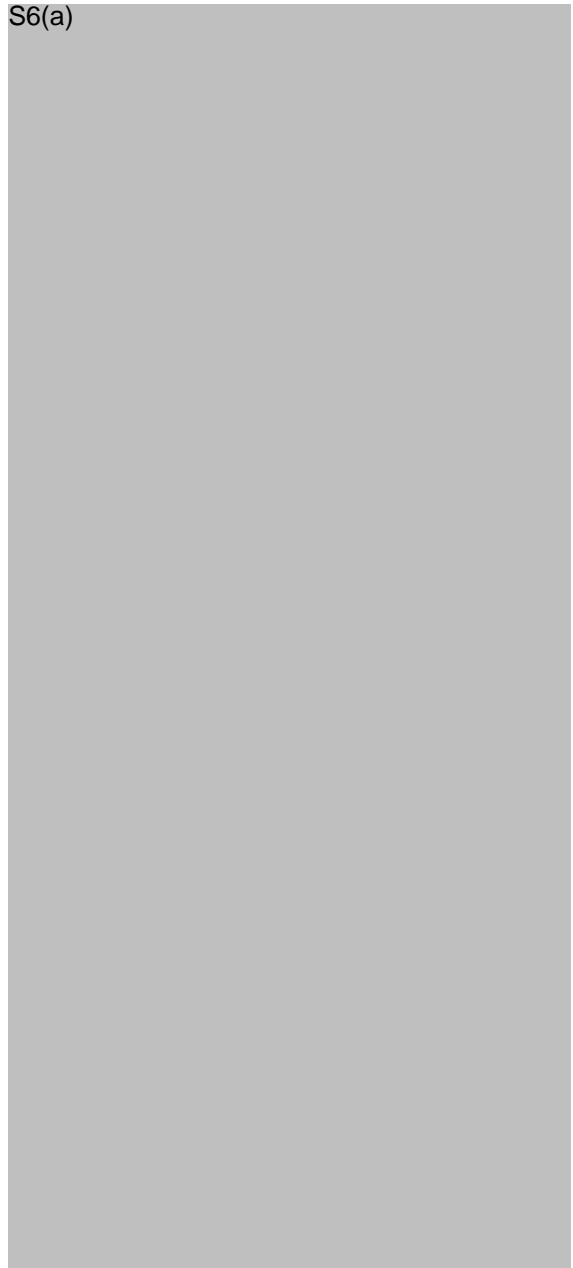


Espionage

New Zealand is not immune to the threat of espionage by foreign states, nor to foreign efforts to interfere with the normal functioning of government or the rights of

New Zealand citizens. Such activities in New Zealand over the past year have included attempts to access sensitive government and private sector information, and attempts to unduly influence expatriate communities.

S6(a)



S6(a)

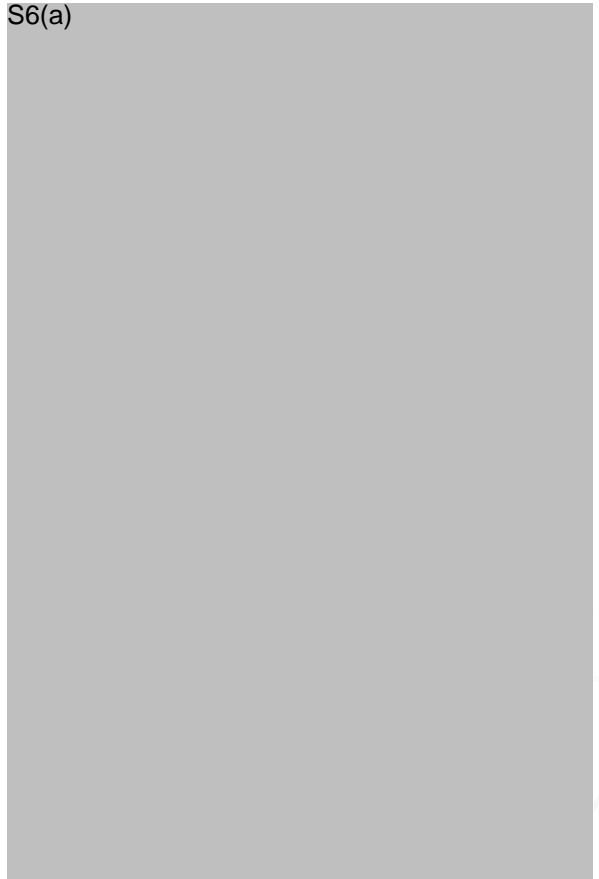


Regional stability – the South Pacific

S6(a)



S6(a)



PART 2:

Transforming how we work

To effectively respond to New Zealand's threatscape, and to generate national advantage, GCSB and NZSIS must work very differently from how we have traditionally operated. Since World War II, intelligence and security arrangements for New Zealand, and many of our closest partners, have been governed by traditional Signals Intelligence (SIGINT) / Human Intelligence (HUMINT) distinctions. These distinctions are becoming less important as the complexity of the threatscape in Western democracies continues to rise. **S6(a)** we are increasingly finding that multi-disciplinary responses are required to keep pace with those who seek to harm New Zealand and New Zealanders' interests.

We also need to be much more responsive to those we are here to serve, including Ministers and other decision makers. What matters to users of our intelligence and advice is high quality, tailored intelligence and advice that reaches the right decision makers at the right time.

This section outlines how we are transforming our agencies to meet these challenges. It includes the core components of the 2016 Budget investment in our community, how we are spending that investment and

the critical impact it has on our ability to effectively perform our functions and keep New Zealand safe.

A community approach to intelligence and security

The investment the NZIC, including DPMC, received as part of Budget 2016 was based on delivery of clear community-wide outcomes – not on individual agencies continuing to do what they have always done.

By taking a community approach to intelligence and security, GCSB and NZSIS can better ensure:

- Each agency's unique skills and approaches are brought to bear on intelligence and security issues in a co-ordinated way;
- We achieve efficiencies and increase value;
- We reduce the risk of an intelligence failure through missed threats or opportunities lost; and
- We apply a consistent and best practice approach to our governance, legal, and compliance obligations.

DPMC's role in the NZIC

Our agencies also work very closely with the Security and Intelligence Group (SIG) in DPMC, which exercises a

collaborative leadership role within the NZIC. As part of the core NZIC, SIG's primary functions are to lead and coordinate the wider national security system, including the Officials Domestic & External Security Committee (ODESC). SIG also leads on cybersecurity policy, national security policy and risk management and, as detailed elsewhere, SIG leads and coordinates the NIP priority setting process.

The National Assessments Bureau, which forms part of SIG, provides assessments to the Prime Minister, senior Ministers, and senior officials on international developments and events relevant to New Zealand's interests. The Director of Intelligence and Assessment, who heads the National Assessments Bureau, is responsible for coordinating intelligence assessment and promoting standards of intelligence analysis across the wider intelligence community. Additional investment was provided to DPMC in Budget 2016 to expand the National Assessments Bureau and expand the resources available to cross-government intelligence coordination.

SIG, through the National Security Policy Directorate, also 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. This arrangement is similar to that by which the Ministry of Justice provides policy advice in respect of the operations of the New Zealand Police. It ensures that there is separation and independence between the intelligence and security agencies and the policy framework in which we operate. For example, the Directorate led the development of the Government's response to the 2015 Independent Review of Intelligence and Security in New Zealand and the legislative process for the ISA.

Core components of investment in GCSB and NZSIS

GCSB, DPMC and DPMC were subject to significant reviews in recent years, including the 2014 State Services Commission-led Performance Improvement Framework (PIF) Review, the 2015 Independent Review of Intelligence and Security in New Zealand, and a first principles review of our capability and resourcing. These reviews identified a number of areas of under-performance and risk. In response to these reviews, and the changing threatscape facing New Zealand, Budget 2016 included a significant increase (\$178.7 million) in investment in the agencies, spread over four years.

The investment was designed to help the Government mitigate its most critical (non-natural hazard) national security risks, stabilise the NZIC in the face of pressures it faced and build a solid foundation for the NZIC to prioritise operational effort to keep

New Zealanders safe, to protect and grow the economy, and to provide foreign intelligence and assessment about issues that matter most to New Zealand.

We are now a little over a year into the four year investment programme. Overall we consider good progress has been made against the expectations that came with the increased investment, with marked improvements in our organisational health (for example, legal compliance, recruitment and staff engagement), protective security standards across government and operational outcomes. Early indications are that our domestic and international partners are beginning to see benefits of the investment as well.

In broad terms, our emphasis over the remaining three years will be on:

- Continuing to build capability in the areas of intelligence collection, information security and investing in information technology;
- Recruiting, developing, and retaining the best and brightest people; and
- Ensuring we embed and capitalise on the opportunities the new legislative framework creates – particularly in respect of our operational work.

S6(a)



We see the key strategic challenges for our agencies as being in the areas of:

- Keeping up with adversaries, staying ahead of the curve from a capability and personnel perspective;
- Realising the benefits of the investment in GCSB and NZSIS;
- Managing the risks that come with growth – and come with the territory; and
- Maintaining a bi-partisan approach to national security, improving public trust and confidence in the agencies and continuing to become more transparent.

Some of these challenges, for instance, keeping up with adversaries, will remain constant. This is because, as described earlier in this report, New Zealand's threatscape and threat actors are constantly evolving. Other areas, such as absorbing growth in a sustainable way, are being managed. However, the careful way in which the investment in the NZIC was sequenced means that these areas may not all be addressed until the latter part of the four-year investment programme.

We will provide you with a more detailed briefing on organisational risks.

Governance of investment

A significant amount of work has been done to ensure the investment programme is well governed. We have established:

For the whole of the NZIC:

- A shared NZIC Four-Year Plan – this acts as a platform for aligning strategic intent and prioritising resources towards common goals;
- A Joint Leadership Team, through which senior representatives from the three agencies govern several NZIC-wide work programmes;

For NZSIS and GCSB:

- Joint workforce planning based on common remuneration, job families and a shared recruitment campaign;
- Shared security, finance, human resources and facilities services; and
- A Joint Directors-General Office, including strategic planning, policy, international engagement and communications functions.

NZSIS and GCSB are also in the process of establishing a joint ICT function to accompany existing shared services for our security, finance, facilities and people capability functions.

Collaborative intelligence collection and analysis

GCSB's and NZSIS's intelligence collection and analysis efforts are also becoming much more joined up.

Mechanisms we are using to drive collaboration include

the National Intelligence Priorities, the Customer Engagement Project and our outreach functions. These are outlined below.

National Intelligence Priorities

Since 2015, shared National Intelligence Priorities (NIPs) have been set to drive the collection and assessment activities of all of New Zealand's intelligence and security agencies including GCSB and NZSIS. The purpose of the NIPs is to ensure relevant government agencies, including GCSB and NZSIS, focus intelligence collection, reporting, and assessment activities on what matters most to the Government. The Intelligence Coordination Unit of DPMC provides high-level oversight of and support to groups bringing together collectors, assessors and customers of each of the **S6(a)** NIPs (see below).

The Cabinet National Security Committee, via a DPMC-led process, reviews and agrees to the NIPs every twelve to 24 months. Subject to ministerial decisions, the next refresh of the NIPs is currently set for March 2018.

S6(a)

S6(a)

S6(a)

S6(a)



Ensuring we are customer focused

S6(a)



Intelligence is only useful, however, if we understand and meet the needs of our customers, including Ministers agencies in the State services.

Customer Engagement Project

As part of improving the utility of our foreign intelligence products, we are working with the Ministry of Foreign Affairs and Trade (our primary policy customer) to trial a new, joint approach to the way our intelligence products are tailored, delivered and used by customers. GCSB, NZSIS and DPMC are currently working with two MFAT divisions, trialing improvements in all of these areas. The lessons learned from these trials will be evaluated and, as appropriate, applied more broadly – including to our engagement with

Ministers and Ministers' offices – and made sustainable across GCSB and NZSIS and the National Assessments Bureau (DPMC). Early indications from the initiative are that significant gains will be made through better education of customers on how to access and use intelligence, and through improved dissemination of intelligence.

Outreach functions

Our information assurance and cyber security functions also require a high level of customer-focused engagement. GCSB's National Cyber Security Centre (NCSC) has positive, responsive relationships with organisations of national significance, including those receiving CORTEX cyber protection services. NCSC shares appropriately classified threat information through a customer portal and sector briefings (Security Information Exchanges), and provides one-on-one advice and more general guidance on information security standards. GCSB also works closely with customers requiring our technical inspection and cryptographic services.

The Protective Security Requirements (PSR) Team within the NZSIS similarly has a strong outreach function and works with public sector agencies to ensure they are operating to best practice personnel, information and physical security protective security standards. Government agencies are responding positively to the 'trusted, critical friend' role of the PSR team and the number of agencies that the PSR team engage with has grown markedly to include the 35 PSR mandated agencies plus 70 other prioritised agencies. Interest from private sector organisations is also growing.

PART 3:

Intelligence and Security Act 2017

The Intelligence and Security Act 2017 (ISA) came fully into force on 28 September 2017.

The ISA replaces the four statutes that previously applied to the NZIC and its oversight bodies with a single, modern and cohesive statute. The ISA contains:

- Shared objectives, functions and powers for NZSIS and GCSB;
- A single authorisation regime covering both agencies' intelligence collection and protective security functions; and
- Significant enhancements to NZSIS and GCSB's oversight institutions and their roles.

The Act allows NZSIS and GCSB to work more closely together where previously our different legislative frameworks created unnecessary confusion and complexity when conducting joint operational work.

This section outlines some of the key features of the ISA. We will provide you with more detailed briefings on the ISA and its operation, including the Act's authorisation and warranting regime.

Your statutory role under the ISA

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

These include:

- Receiving intelligence;
- Authorising others to receive intelligence;
- Issuing of intelligence warrants and removal and practice warrants;
- Authorising the provision of protective security services, advice and assistance by NZSIS or GCSB to any public authority or person / class of persons;
- Issuing Ministerial Policy Statements, a unique legislative tool, which provides guidance to GCSB and NZSIS on how they exercise a range of functions; and
- Providing a response to inquiries undertaken by the Inspector-General of Intelligence and Security (IGIS).

We will cover these responsibilities in more detail in our first meeting with you.

Oversight

The ISA reinforces NZSIS and GCSB'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 main oversight bodies are the IGIS and the Intelligence and Security Committee (ISC):

- The IGIS is a statutory officer providing independent external oversight and review of the intelligence and security agencies. The IGIS is responsible for reviewing issues of legality and propriety, which includes the agencies' compliance with human rights and privacy obligations. The IGIS is supported to perform her role by a statutorily appointed Deputy IGIS and a team of approximately six employees.
- The ISC is the parliamentary oversight committee for the intelligence and security agencies. It is established by statute and examines issues of effectiveness and efficiency, budgetary matters and policy settings.

Our overarching oversight and accountability framework has multiple layers:

Executive/Ministerial

- The Minister Responsible for the GCSB and Minister in Charge of the NZSIS oversees day-to-day business and approves warrant applications made by the respective agencies
- The Minister for National Security and Intelligence (Prime Minister) oversees the National Security System

- The Cabinet National Security Committee provides Cabinet oversight on national security matters
- There is a legislative requirement to review the intelligence agencies within five years of the commencement of the ISA and periodically thereafter; and
- The State Services Commissioner employs the Directors-General of the GCSB and the NZSIS, manages their performance and provides leadership and oversight of the State sector.

Parliamentary

- The ISC is our parliamentary oversight committee (as above); and
- The agencies are required to brief the Leader of the Opposition.

Judicial

- The Minister and the agencies are subject to the courts, including through judicial review.
- Independent authorities
- The participation of a panel of Commissioners of Intelligence Warrants in the warranting process
- The IGIS and the advisory panel to the IGIS
- The Privacy Commissioner
- The Ombudsman
- The Auditor-General; and
- The Human Rights Commission.

PART 4:

International partnerships

Everything GCSB and NZSIS do needs to be in accordance with New Zealand law and human rights obligations, and in alignment with our national interests, as determined by the government of the day.

International intelligence-sharing arrangements are fundamental to how GCSB and NZSIS meet New Zealand's national interests. New Zealand could not hope to deliver the current level of security and intelligence activity alone. Our most significant relationship is with the Five Eyes partnership.

The Five Eyes partnership has been central to New Zealand's approach to intelligence and security since World War II.

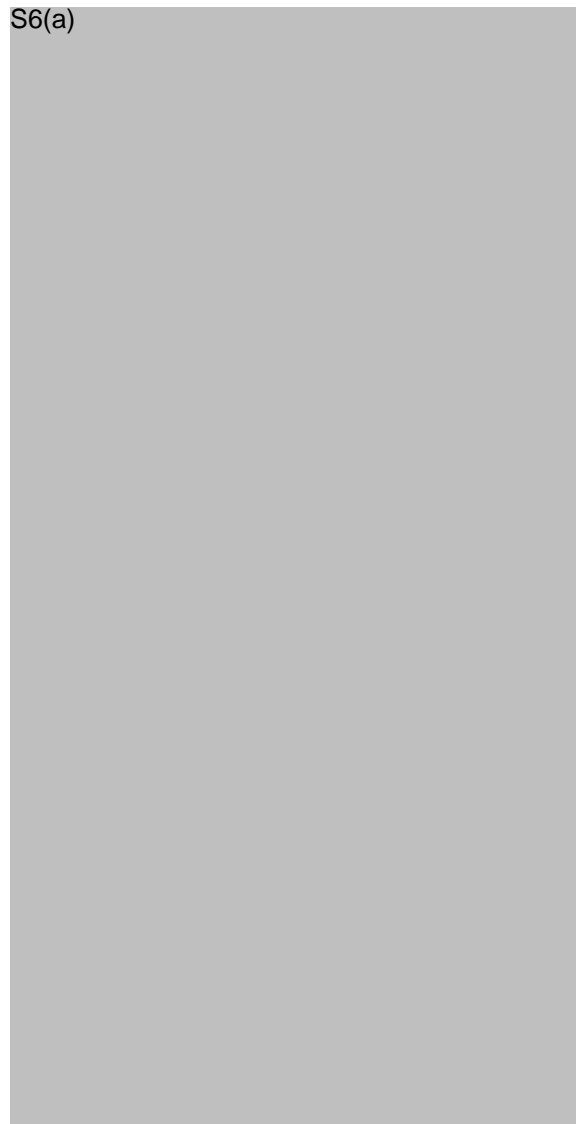
S6(a)



S6(a)




S6(a)



S6(a)



We also share intelligence with a range of other international counterpart agencies, including S6(a)



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

PART 5: Our support to you

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

The Executive Wing of Parliament Buildings does not have facilities necessary to brief you on material classified above RESTRICTED. As a result, we propose to hold the majority of meetings with you at our headquarters, Pipitea House. Pipitea House is a Sensitive Compartmented Information Facility (SCIF).

S6(a)

Directors-General

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

Initial briefing programme

We have developed a briefing programme aimed at providing an initial overview of our agencies, their functions and work. We will discuss our proposal with you during our first meeting and will then tailor it to meet your expectations.

Regular meeting schedule

NZSIS and GCSB's recent practice has been to hold separate fortnightly meetings with the responsible Minister. These meetings are attended by the relevant Director-General and members of our Senior Leadership Teams. The meetings tend to cover emerging policy and operational issues, matters coming before Cabinet committees, upcoming publicity or media issues, and matters relating to the organisational health of the agencies. We recommend this arrangement continue.

Warrants and authorisations

Because of your statutory role, we regularly request meetings to discuss warrants and authorisations. From time to time fast-moving or urgent operational matters may mean we need to brief you at short notice. There may also be joint meetings with the Commissioner of Intelligence Warrants.

The Minister of Foreign Affairs also has a statutory role in relation to warrants and authorisations that have foreign affairs implications or involve activities with an international dimension. We seek meetings with the Minister of Foreign Affairs on an ad hoc basis,

depending on the warrants that are being sought. You will know that these meetings are occurring. There is no need for you to attend as well, but you are welcome to attend if you wish.

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

Prime Minister

As previously noted, we have responsibilities to the Prime Minister, as Minister responsible for National Security and Intelligence. Our relationship with the

Prime Minister is independent of her portfolio responsibilities for DPMC's national security function.

In terms of our engagement with the Prime Minister, both Directors-General attend the Prime Minister's weekly intelligence briefing. The Director-General of Security also briefs the Prime Minister on a monthly basis, which you are also likely to attend. Both Directors-General also brief the

Prime Minister on a case-by-case basis on sensitive operational matters.

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 NZIC.

In accordance with our statutory responsibilities, our recent practice has been to brief the Leader of the Opposition on a monthly basis. We keep the Leader of

the Opposition informed on the same security matters on which we brief the Prime Minister, with some exceptions.

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 of 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. The Minister for Communications has also held the cyber policy portfolio, so may receive briefings from us in this respect from time to time.

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

Private Secretary

NZSIS and GCSB currently provide a NZIC Private Secretary to the Office of the Minister Responsible for the GCSB and the NZSIS. 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.

Joint Directors-General Office

The Joint Directors-General Office (JDGO) is responsible for providing day-to-day service to staff in your Office. The JDGO comprises three teams: Strategy, Performance & Policy, International Engagement, and Communications. JDGO 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 1993 requests, oral and written questions etc.

Decisions in the first three months

We anticipate the following issues may arise during your first three months in the role. We will provide full briefings on each, as issues arise:

Warrants and authorisations

S6(a)

Implementation issues associated with the commencement of the Intelligence and Security Act

As mentioned earlier in this briefing, the ISA is now fully in force. All of the necessary Ministerial Policy Statements are in place and training for staff has been complete. Implementation of the ISA has been a significant piece of work for our agencies and we are still working to ensure all necessary arrangements are in place to give effect to the Act. A few areas

may require ongoing decisions including

S9(2)(f)(iv)

Malware-Free Networks

In December 2017, GCSB is scheduled to report back to Cabinet with a recommendation about taking the Malware-Free Networks component of CORTEX out of pilot and scaling it.

S9(2)(f)(iv)
S6(a)

CORTEX and Malware Free Networks are described later in this briefing.

S6(a), S9(2)(f)(iv)

S9(2)(f)(iv)

GCSB

ABOUT GCSB

In 1977, Prime Minister Robert Muldoon approved the formation of the GCSB to fulfil the functions of Signals Intelligence (SIGINT), Communications Security (COMSEC) and Technical Security (TECSEC) for government. However the origins of the GCSB go back more than sixty years to the early days of World War I when the New Zealand Post and Telegraph Department in conjunction with the Royal Navy, operated intercept stations within New Zealand and the South Pacific. They operated again in the lead up to and during World War II, providing a small but useful input to Allied SIGINT efforts.

The intercept stations were disbanded in late 1945, ironically the same time as US and UK authorities were discussing continuation of the successful SIGINT partnership typified by the achievements at Bletchley Park. The UKUSA agreement was signed in 1946, and the then New Zealand Prime Minister agreed that New Zealand should maintain a peace-time SIGINT effort. However over the next 10 years there was little progress until the establishment of the New Zealand Combined Signals Organisation (NZCSO) in 1955 and New Zealand's formal signature of the UKUSA

agreement in 1956. **S6(a)**



In the mid-1970's two reviews were conducted into the SIGINT and COMSEC activities of the New Zealand Government, and these identified a need for changes to improve the effectiveness and governance of both functions. The outcome was a recommendation to the Prime Minister to establish a new national authority for signals intelligence, technical and communications security. Initially the GCSB was part of the Ministry of Defence and its functions and activities were kept secret but by 1980 it was decided that the existence of GCSB could be disclosed on a limited basis, leading to the first briefings of Cabinet and the Leader of the Opposition. These briefings acknowledged GCSB's TECSEC and COMSEC functions, but not its SIGINT function. Prime Minister Muldoon publicly acknowledged the existence of GCSB and its SIGINT function in 1984. In 1989, following a range of state sector reviews, the GCSB was established as a standalone crown agency.

In early 2000, a legislative process to place GCSB on a statutory footing began. In 2003, the Government Communications Security Bureau Act 2003 (the GCSB Act) took effect and GCSB became part of the Public Service. In June 2003, Cabinet formalised the role of GCSB as the national authority for signals intelligence and information systems security.

In May 2014, the Telecommunications (Interception Capability and Security) Act 2013 (TICSA) came into effect. Under TICSA, GCSB acquired responsibility for administering the network security provisions set out in Part 3 of the Act.

GCSB is a Public Service department with its head office in Wellington, an office in Auckland, a high frequency radio interception and direction-finding station in Tangimoana near Palmerston North, and a satellite communications interception station at Waihopai near Blenheim. **S6(a)**

GCSB STRATEGIC PLAN 2016-2020

GCSB's Strategic Plan outlines what GCSB will achieve over the next four years. The Strategic Plan focuses our actions on our aim that by 2020:

- a. New Zealand's most important information infrastructures are impenetrable to technology-borne compromise. We call this aim **impenetrable infrastructure**; and
- b. New Zealand's intelligence generates unique policy and operational impacts for New Zealand. We call this aim **indispensable intelligence**.

Underpinning these aims are eight priority objectives:

- Recruit and retain the best people;
- Implement the new legislative regime;
- Renew and extend GCSB's core IT infrastructure;
- Replace New Zealand's high-grade cryptographic infrastructure;
- Embed and scale GCSB's cyber defensive capabilities;
- Radically improve the utility of our intelligence product;
- Continue to modernise GCSB's accesses and tradecraft; and
- Overhaul how highly classified communications are delivered.

In order to deliver on these outcomes and objectives, GCSB is making changes to have a higher level of customer interaction, use its resources more collaboratively and build public trust and confidence in the agency. In the next section of this briefing, which outlines GCSB's functions, we provide practical examples of how we are addressing these challenges.

GCSB'S FUNCTIONS

Under the ISA GCSB has five core functions:

- Intelligence collection and analysis;
- Information assurance and cyber security activities;
- Protective security services, advice and assistance;
- Co-operation with other public authorities to facilitate their function; and
- Co-operation with other entities to respond to imminent threat.

A high level description of each function is set out below.

Intelligence collection and analysis

GCSB's enduring mission is to enable customer outcomes through the collection and exploitation of communications intelligence in a lawful manner consistent with

New Zealand's national interest and national security. Our intelligence products enhance New Zealand's policy development, geo-political decision making, as well as

S6(a)



This has a direct bearing on New Zealand's security and national advantage.

The ability to interpret and make best use of intelligence depends on the tradecraft, experience and unique capabilities applied to it. Increasingly important is GCSB's ability to understand the intended customer outcome and conduct intelligence activities to best meet the need.

S6(a)



How does GCSB collect intelligence?

GCSB is a communications intelligence agency. We collect intelligence using several methods:

S6(a)



S6(a)



S6(a)



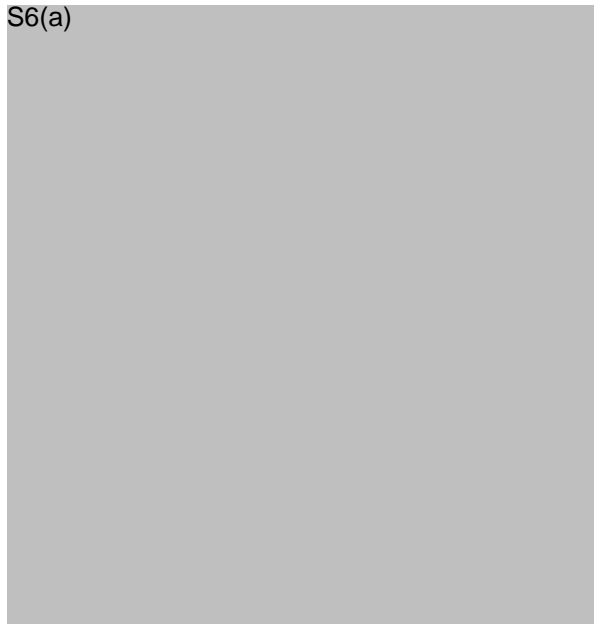
What does GCSB produce intelligence on?

All of GCSB's intelligence collection activities are governed by the ISA and aligned with the NIPs. These are described earlier in this briefing.

S6(a)



S6(a)



Counter-terrorism

GCSB's counter terrorism efforts are focussed on two zones of effort:

- i. Domestic: Support NZSIS and the New Zealand Police in countering actual or planned acts of terrorism within New Zealand; and
- i. S6(a) to identify and counter global actors that seek to project influence into New Zealand, with a view to inspiring or conducting acts of terror within New Zealand.

S6(a)



S6(a)



S6(a)



S6(a)

GCSB's New Zealand Security Operations Centre (NZSOC)

GCSB's New Zealand Security Operations Centre (NZSOC) provides a "Watch and Warn" service on a 24/7 basis in support of major events, NZDF operations and to travelling VIPs.

S6(a)

Targeting of New Zealanders

New Zealand does not undertake any "mass surveillance" of New Zealanders, such as the active monitoring of emails, phone calls and internet use of the populations. We do not have the legal authority, capability or interest to undertake such activity. Both the 2015 Independent Review of Intelligence and Security in New Zealand, and the IGIS have looked at the matter and confirmed this to be the case.

The previous legal position, under the GCSB Act 2003, was that in pursuing its foreign intelligence function, GCSB could not do anything for the purpose of intercepting the private communications of New Zealand citizens or permanent residents, except where they were acting as agents or representatives of a foreign person or organisation. The ISA amends this position but puts in place strict warranting requirements before this can occur. We will brief you on these provisions of the ISA.

Modernising GCSB's capability and tradecraft

S6(a)

Radically improve the utility of our intelligence product

GCSB provides regular delivery of intelligence to 19 government agencies and to appropriate Ministers, their offices, the Leader of the Opposition and international partners. Our intelligence is only worthwhile, however, if it generates insight and decision-making advantage, or is put into operational use.

In February 2017 NZSIS, GCSB, and DPMC launched the Customer Engagement Programme. This initiative, which is focused on foreign intelligence, is described earlier in this briefing.

GCSB is also increasing the utility of the cyber security threat information we collect to get it to a declassified form that is useful for our organisations of national significance customers. We have a portal where customers can access a range of governance and technical information to help them manage and mitigate their information security risks. We also provide monthly classified and unclassified threat summaries, which are widely distributed to customers.

S6(a)



Information assurance and cyber security

Under its information assurance and cyber security functions, GCSB works with significant public and private sector organisations to protect information systems and communications critical to New Zealand's

national interests from sophisticated security threats. GCSB is the lead agency for information security for government. This section provides an overview of the different aspects of GCSB's information assurance and cyber security functions.

National Cyber Security Centre

Through the NCSC, GCSB provides cyber security services and advice to nationally significant public and private sector organisations. These include government departments, key economic generators, niche exporters, research institutions and operators of critical national infrastructure. NCSC works with these organisations to detect and disrupt advanced malicious cyber activity, helping find and remove network compromises and providing advice and support on remediation and prevention. While NCSC's efforts are concentrated on New Zealand's most significant information systems, NCSC may also get involved in other serious incidents if required.

The NCSC's Incident Co-ordination and Response team is on call to victims of cyber incidents and ready to deploy 24/7. The NCSC triages, refers and/or responds to these public-derived incidents.

The NCSC recorded 396 incidents in 2016/17, an increase of 58 on the previous year. This is in part a reflection of our increasing insight into the activity occurring on networks of national significance, due to the delivery of CORTEX capabilities across a wider range of customer networks.

NCSC works closely with CERT NZ (Computer Emergency Response Team). NCSC takes the lead in responding to significant cyber events – particularly those that may affect national security and nationally

significant systems and information. CERT NZ meanwhile, helps businesses, organisations and individuals wanting prevention and mitigation advice on day-to-day online security issues. CERT NZ has primary responsibility for cyber threat reporting and a coordination role in threat response.

S6(a)



CORTEX

CORTEX is a programme to counter cyber threats to both public and private sector organisations of national significance. It involves GCSB utilising tools and threat information to protect these organisations from advanced persistent malicious software (malware). CORTEX cyber protection services operate in respect of a highly targeted, consented and authorised range of communications and are only deployed with the express agreement of the organisation involved.

S6(a)



Of the 396 incidents recorded by NCSC in the past year, S6(a) were detected using CORTEX capabilities. Over

the past six months, some of the types of incidents detected and disrupted by CORTEX capabilities include:

S6(a)



In addition to providing cyber defence services to its CORTEX customers, GCSB uses CORTEX threat information to inform cyber threat alerts and advisories, which it distributes to all government departments and a large number of private sector organisations. Damages avoided by CORTEX in the 12 months to 30 June 2017 have been assessed at \$39 million.

Malware-free Networks

As part of CORTEX, GCSB piloted a capability in partnership with Vodafone called Malware-free Networks. This involved sharing cyber threat information and technology with Vodafone so they could use the information to help protect a subset of their customers, all of whom consented to receive the service.

S6(a)



Although the pilot has officially ended, service will continue to be provided to the S6(a) pilot customers until at least December 2017 when GCSB will report back to Cabinet

with a recommendation about how the capability should be taken out of pilot **S9(2)(f)(iv)**

S6(a)

is accompanied by an unclassified Cyber Threat Report, which is designed to inform and support discussion amongst a wider range of decision-makers, and to shine light on the work that the NCSC carries out.

Information assurance

GCSB acts as the New Zealand national authority for communications security (COMSEC) – the technology and processes used to protect our most sensitive data through advanced encryption. COMSEC ensures that our deployed forces can securely communicate

in hostile areas, that we can receive and disseminate valuable intelligence, and that our diplomatic and trade activities can be effective on the world stage. COMSEC is the primary means of maintaining the integrity of highly classified New Zealand **S6(a)**

Critical elements of our current infrastructure will soon reach the end of their supported life **S6(a)**

The Cryptographic Products Management Infrastructure (CPMI) project replaces the equipment, hardware, software, networks, facilities and support arrangements currently used by GCSB to protect highly classified New Zealand Government information systems **S6(a)**

The new infrastructure will affect several other government agencies in the sector, **S6(a)**

This is a significant project, which received \$120.2 million over four years in Budget 2016. **S6(a)**

It is currently on time and on budget.

GCSB also provides technical inspection services, ensuring that sensitive areas or those that contain classified material are free from interception devices or vulnerabilities. **S6(a)**

To protect government agencies from information security risk, the GCSB publishes the New Zealand Information Security Manual (NZISM). It contains minimum standards along with guidance for agencies to protect information from threats to its confidentiality, integrity or availability. The NZISM is part of the PSR delivered by the NZSIS and GCSB.

For locations or computer systems that store or process highly classified information, the Director-General, GCSB is the operating authority, responsible for reviewing agency risk mitigation and granting an accreditation that allows the agency to deploy the location or system.

New Zealand Top Secret Network

New Zealand government agencies operate a wide variety of technology capabilities at the TOP SECRET level, some of which are shared, but the majority of which are operated by individual agencies. The diverse arrangements across the sector result in a number of inefficiencies, duplication of capabilities and limited integration of mission endeavours. The New Zealand Top Secret Network programme was established to address these challenges and opportunities, and to deliver an integrated set of capabilities for the whole Top Secret community. Through the adoption of common technology, barriers to co-operation will be removed.

S6(a)



S6(a)



Additional statutory functions

GCSB also has functions under the TICSAs and the Outer Space and High Altitude Activities Act 2017 (OSHAA).

Under Part 3 of TICSAs, the Minister Responsible for the GCSB and the Director-General, GCSB have a range of regulatory responsibilities concerned with keeping New Zealand's public telecommunications networks secure. TICSAs require public telecommunications network operators to notify the GCSB if they are planning a major network change within certain areas of specified security interest (such as lawful intercept equipment and network operations centres). Notifiable changes within the areas of specified security interest include the purchase or acquisition of equipment or services, changes to network architecture, or changes in ownership of control.

If a network security risk is raised by a notification, the Director, 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. TICSAs set out a process for making such a direction, which includes consultation with the Minister for Communications and the Minister of Trade.

TICSA has now been in place for three years. As of 18 September, S6(a) cases have been received from New Zealand operators. The majority of notifications raised a minimal or no network security risk (meaning a risk to New Zealand's national security, including its economic well-being), S6(a)



Outer Space and High-altitude Activities Act

In July 2017, the New Zealand Parliament passed the OSHAA, the purpose of which is, amongst other things, to facilitate the development of a safe and secure space industry in New Zealand, and to ensure that space activities preserve New Zealand's national security and national interests. OSHAA comes into force on 21 December 2017, though transitional provisions apply to launches by Rocket Lab for a period of six months after the Act comes into force.

GCSB and NZSIS, working in conjunction with NZDF and the broader NZIC, have formed a Space Activity Risk Assessment Group to conduct national security risk assessments on outer space launches, launch facilities, payloads and high altitude vehicles. This assessment is required under OSHAA.

Rocket Lab's first launch, conducted in May 2017, provided a first test of the national security review

process in New Zealand. S6(a)



Co-operation with other entities to facilitate their functions or respond to an imminent threat

Under section 13 of the ISA, GCSB can cooperate and provide advice and assistance to the New Zealand Police and NZDF for the purpose of facilitating the performance of those entities' lawful functions. S6(a)



Similar provisions applied under section 8C of the GCSB Act. During the past year, under section 8C of the GCSB Act, GCSB provided cooperation and advice to NZSIS, NZDF and NZ Police in support of national security investigations. S6(a)



Section 14 of the ISA provides a new but limited ability for GCSB and NZSIS to co-operate with and provide advice and assistance to, a person, class of persons, or public authority (whether in New Zealand or overseas) that is responding to an imminent threat to life to those in New Zealand or an area for which New Zealand has search and rescue responsibility, New Zealand citizens and permanent residents overseas, and those outside the jurisdiction of any country (e.g., parts of the oceans). This ability can only be used for activities which could

not be authorised by an ISA warrant. GCSB and NZSIS have not yet acted under this provision.

GCSB'S PEOPLE

This section outlines at a high level overview of GCSB's composition as well as a brief introduction to the Senior Leadership Team.

GCSB is a Public Service department with slightly over 400 employees. **S6(a)**

GCSB is an organisation of experts drawn from an increasingly competitive market. We recruit from a wide range of disciplines including foreign language experts, communications and cryptography specialists, engineers, technicians, and corporate staff.

Over the long term it is staff, more than our technology, that generate the unique value GCSB's customers are seeking. It is therefore critical that we can attract, and provide fulfilling career options, for New Zealand's top talent. We have put in place a number of initiatives to meet this challenge including a graduate recruitment programme, a recruitment campaign called "Beyond Ordinary" and a Career Pathways Framework.

We believe this investment is paying off, with our most recent staff engagement survey positioning GCSB in the top 25% of public sector agencies.

We are also bringing a clear focus to gender and ethnic diversity. While women are well represented in GCSB at senior level, and our gender pay gap is less than the wider State sector average, overall only 36% of our workforce is female. We recently agreed

an action plan to increase female representation in GCSB and reduce our gender pay gap by half within a year. As part of this work, GCSB recently announced a \$10,000 tertiary scholarship for women students in their second year of study or above taking a STEM qualification. The objective is to attract more women into computer technology, computer science and engineering roles where there is a marked gender imbalance. We received 80 high quality applications for this scholarship and are considering ways to ensure those who don't receive a scholarship remain engaged with our recruitment efforts.

The GCSB (and wider NZIC) workforce is generally less ethnically diverse than the wider public service, in part because it is more difficult to confirm the personal information of people who have not been resident in New Zealand for a long period of time (a requirement of the vetting process). The NZIC recognise this as an issue and is actively seeking to mitigate any negative impacts on potential employees, staff and the NZIC.

Senior Leadership Team

In your new role, you are likely to have a significant amount of contact with GCSB's Senior Leadership Team. A brief introduction to each team member is set out below.

Andrew Hampton – Director-General

Andrew Hampton is the Director-General, GCSB. He has been in this role since April 2016.

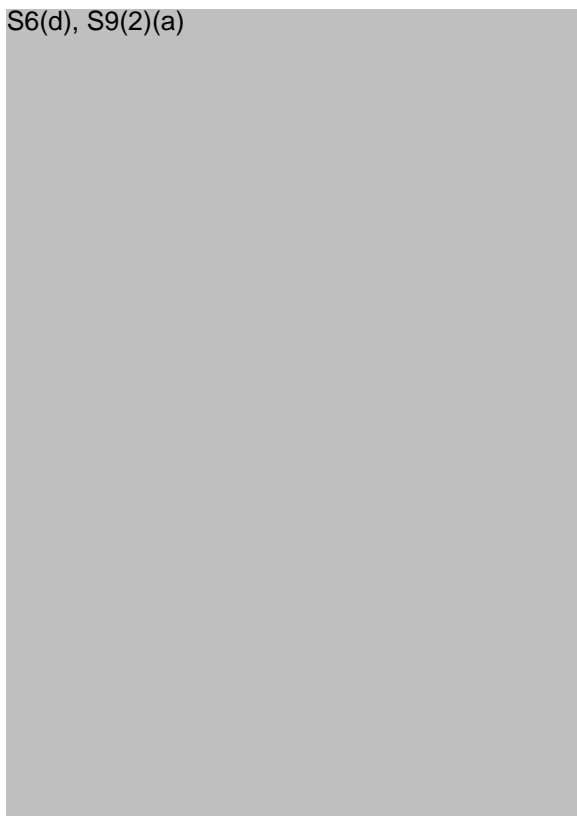
Prior to joining the GCSB, Andrew spent much of his career in the justice sector, including Treaty settlement negotiations, courts administration and leading various

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. He was also the Government Chief Talent Officer at the State Services Commission, a new role responsible for leadership development, workforce strategy and employment relations across government.

S6(d), S9(2)(a) – **Director of Strategy, Governance and Performance**

S6(d), S9(2)(a)



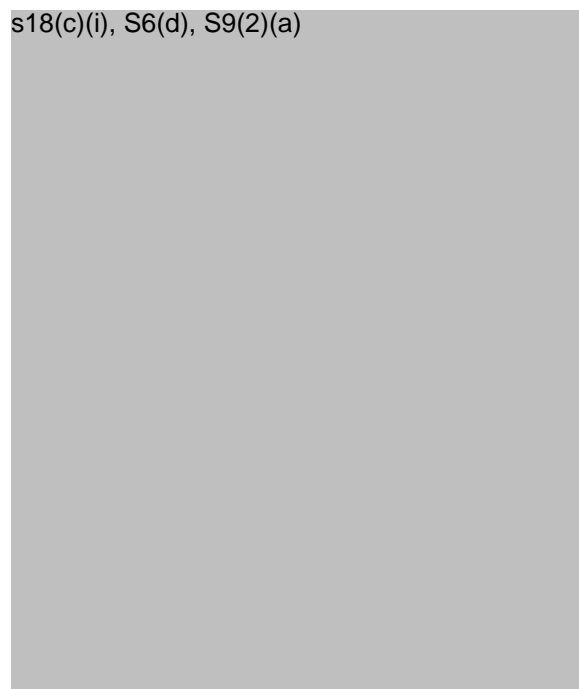
Lisa Fong – Director Information Assurance and Cyber Security

Lisa is Director Information Assurance and Cyber Security. She also holds the roles of Chief Information Security Officer and National COMSEC Officer.

Lisa has held a range of positions in the NZIC, including Chief Legal Adviser for the GCSB, and short periods as acting General Counsel for the NZSIS and acting Director of the GCSB. Before joining GCSB's Senior Leadership Team in 2013, she represented and advised the government on legal issues at Crown Law, specialising in public law litigation. She has a BA/LLB (Hons) from the University of Auckland and a Master of Laws from New York University.

s18(c)(i) **Director Intelligence**

s18(c)(i), S6(d), S9(2)(a)



S6(d), S9(2)(a) [REDACTED] - Chief Legal
Advisor

S6(d), S9(2)(a)

[REDACTED]

S6(d), S9(2)(a) [REDACTED] Director Technology

S6(d), S9(2)(a)

[REDACTED]

S6(d), S9(2)(a) [REDACTED] Chief People
Officer, Intelligence Community Shared
Services

S6(d), S9(2)(a)

[REDACTED]

S6(d), S9(2)(a) [REDACTED] Chief Financial
Officer, Intelligence Community Shared
Services

S6(d), S9(2)(a)

[REDACTED]

NZSIS

ABOUT NZSIS

NZSIS was founded in 1956. Until then, apart from a brief period during World War II, national security matters were handled by the Special Branch of the New Zealand Police. NZSIS's functions were legislated for in 1969. The ISA recently replaced the NZSIS Act 1969 and on 28 September 2017, the NZSIS became a Public Service Department.

NZSIS is a Human Intelligence or HUMINT agency. It conducts its operational activities and provides intelligence and advice to the government to ensure that:

- New Zealanders are safer;
- Our institutions are protected; and
- New Zealand's national advantage is promoted.

NZSIS's vision is to be ahead of the curve: providing indispensable security and intelligence services underpinned by high public confidence and trust. To ensure we are able to deliver this vision now and in the future, we have been on a significant journey of growth and development over the past three years.

To ensure the NZSIS can grow as quickly and sustainably as possible, we have put in place a ten-

year operational strategy – S6(a) provides clarity of purpose for NZSIS activities, allows us to prioritise our resources and take major strategic decisions including on investment in capabilities, recruitment and training.

S6(a) is now embedded and is guiding our decision making. We are now better positioned to deliver on investment committed in 2016, and meet the challenges of New Zealand's evolving national security environment. The nature of our work, and the significant amount still to be done, mean however that risks will always remain.

NZSIS's head office is based in Pipitea House on Pipitea Street in Wellington. NZSIS has regional offices in Auckland and Christchurch as well as S6(a)

NZSIS OPERATIONAL STRATEGY – S6(a)

S6(a) is focused on three primary outcomes we seek to achieve on behalf of New Zealand and New Zealanders. The link between these outcomes and NZSIS's long term strategic goals are set out overleaf.

Primary Outcome	Long-term Strategic Goal	Explanation
<i>New Zealanders are safe</i>	NZSIS has established an effective baseline picture of emerging terrorism threats.	S6(a)
	NZSIS has successfully mitigated domestic terrorism threats.	
	NZSIS has provided effective and sustainable support for a significant overseas deployment.	
<i>New Zealand's key institutions are protected</i>	The NZIC is a protective security exemplar.	
	NZSIS has assisted key institutions to mitigate their insider threat risks.	
	NZSIS has mitigated espionage and hostile foreign intelligence threats.	
<i>New Zealand's national advantage is promoted</i>	NZSIS has enabled better policy and geopolitical decision making.	
	NZSIS has meaningfully contributed to international security.	
	NZSIS has enhanced security in the Pacific.	

NZSIS'S FUNCTIONS

NZSIS exercises its functions under the ISA in support of its long term strategic goals. Under the ISA, NZSIS has the same functions as GCSB, specifically:

- Intelligence collection and analysis;
- Protective security services, advice and assistance;
- Information assurance and cyber security activities;
- Co-operation with other public authorities to facilitate their functions; and
- Co-operation with other entities to respond to imminent threats.

A high level description of each function is set out below.

Intelligence collection and analysis

How does NZSIS collect intelligence?

Many of NZSIS's collection methods are based on human intelligence activities – "HUMINT". HUMINT is intelligence obtained from people with knowledge of or access to information. HUMINT may come from a range of sources – from covert human intelligence sources at one end of the spectrum, to private individuals who may offer information, at the other end. We collect HUMINT through a range of methods **S6(a)**

NZSIS also uses a range of other collection methods including physical surveillance, tracking devices, technical interception, listening devices **S6(a)**

What does NZSIS collect intelligence on?

All of NZSIS's intelligence collection activities are governed by the ISA and are aligned with the NIPs.

Some key areas of focus are outlined below. These are intended to provide an initial overview of our work.

More detailed briefings on NZSIS operations will follow.

Keeping New Zealanders safe

Counter-terrorism

One important way that we help to keep New Zealanders safe is through investigating people who pose an actual or potential terror-related threat to New Zealand. At any one time over the past three years, between 30 and 40 people were listed on the counter-terrorism risk register. The ubiquity of ISIL's messaging is such that all but one of NZSIS's current counter-terrorism investigations concern ISIL-linked extremism, and we continue to investigate individuals for supporting or attempting to travel offshore to join ISIL. **S6(a)**

S6(a)

Border security

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

The role of analysis

The Analysis Branch of NZSIS works closely with domestic and international partners to provide threat assessment and strategic analysis to a range of decision makers. The branch provides time sensitive domestic threat reporting and assessment via the Combined Threat Assessment Group¹ (CTAG). It also covers a range of strategic and thematic topic areas relating to counter-terrorism and espionage and provides wider-ranging analysis of these topics.

CTAG also monitors terrorist threats globally and contributes threat advice to the Ministry of Foreign Affairs and Trade's Safe Travel capability where there is a possibility that New Zealand interests could be impacted.

¹ CTAG is a combined threat assessment group hosted by the NZSIS and made up by representatives from NZSIS, GCSB, NZDF, New Zealand Police, New Zealand Customs, and the Aviation Security Service.

New Zealand institutions are protected

Counter-espionage

NZSIS helps to detect, defend, and counter threats posed by foreign intelligence services to New Zealand and New Zealanders. Countering these threats requires a multi-disciplinary approach. NZSIS works closely with domestic and foreign intelligence partners, the most significant being GCSB.

NZSIS continues to see foreign powers conduct espionage activity and other hostile State-sponsored activities (including foreign interference) against New Zealand and New Zealanders. Foreign intelligence services pursue information, both classified and publicly available, to support the objectives of their respective governments. Key areas of focus for foreign intelligence services activity in New Zealand include:

S6(a)



New Zealand's national advantage is promoted

S6(a)



S6(a)

S6(a)

Protective security services and vetting

NZSIS has significant NZIC and all-of-Government leadership responsibilities in relation to counter-intelligence and protective and personnel security. As part of this work, NZSIS provides advice and assurance to government agencies and private sector organisations.

Protecting NZIC's people, information and assets

One of NZSIS's functions is to support a safe and secure NZIC. In co-operation with GCSB, NZSIS helps ensure the NZIC's protective security measures meet national and international standards. Our efforts ensure New Zealand's most sensitive information, people, facilities, and assets are protected.

Security clearance vetting

Having access to highly classified information allows the NZIC and the NZSIS to provide unique advice to decision makers. It also comes with a significant degree of responsibility and trust, however. Misuse, mishandling or the unauthorised disclosure of classified information can have significant consequences for the New Zealand Government, our international partners, and the work of the NZIC and NZSIS. People and other organisations place a lot of trust in the NZIC agencies to protect and respect their information.

Any individual who has access to classified government information requires a security clearance. NZSIS plays a cross-government role in vetting candidates for a range of security clearances ranging from RESTRICTED to TOP SECRET SPECIAL. NZSIS vetting officers undertake a range of duties, including interviewing candidates and referees, to make an assessment about an individual's suitability to hold a security clearance. A recommendation is then provided to the chief executive of the relevant sponsoring agency. NZSIS vetting recommendations form the basis for state sector agencies to grant personnel access to classified information.

Recent NZIC growth has significantly increased demand for security vetting services. We are actively working to improve our performance against our vetting targets as well as the overall experience of candidates going through the vetting process. Work plans have been developed and will be implemented during 2017/18 to reduce the current backlog of vetting applications and increase NZSIS's ability to meet our vetting performance targets.

All-of-Government Protective Security Requirements

The Protective Security Requirements (PSR) framework - led by the NZSIS - includes 29 mandatory requirements covering security governance and personnel, information, and physical security requirements that all government agencies are expected to meet. The PSR framework and the PSR support team provides a single source of truth, tools, and guidance for government agencies to ensure they are operating to best practice protective security standards. The PSR team is also

getting increasing interest from private sector agencies that are proactively looking to increase their security standards.

Government agencies are responding positively to the 'trusted, critical friend' role of the PSR team and the number of agencies that the PSR team engage with has grown markedly to include the 35 PSR mandated agencies plus 70 other prioritised agencies.

The New Zealand Information Security Manual, which sits within the PSR framework, is led and managed by the GCSB. It is the New Zealand Government's manual for practitioners on information assurance and information systems security. It includes minimum technical security standards for good system hygiene, and provides other technical and security guidance for government departments and agencies to support good information governance and assurance practices.

NZSIS's cyber security role

S6(a)



S6(a)



Co-operation with other public authorities to facilitate their function

NZSIS routinely works with other public authorities to facilitate their functions. This will continue under the ISA. Some recent examples of co-operation include:

S6(a)



Responding to imminent threats

As is the case for GCSB, the ISA sets out a new function which allows NZSIS and GCSB to cooperate with and provide advice and assistance to, a person, class of persons, or public authority (whether in New Zealand or overseas) that is responding to an imminent threat to

life to a range of people including those in New Zealand and New Zealand citizens. Given the ISA only fully came into force on 28 September and that this is a tightly defined, NZSIS has not yet acted under this provision.

NZSIS'S PEOPLE

This section provides an overview of the NZSIS's composition and structure as well as a brief introduction to the NZSIS's Leadership Team.

As at 30 June 2017 the NZSIS had close to 300 full time equivalent staff. S6(a)

Recruiting, developing, and retaining outstanding people is a critical aspect of NZSIS and the NZIC workforce development planning. NZSIS staff provide the skills, innovation, and the drive necessary to ensure we keep New Zealand and New Zealander safe and secure - often in very challenging and complex situations.

Continual investment in the capability of our staff is a key part of our aim to stay ahead of the curve. To this end, we have strengthened our security intelligence training through a sustained Intelligence Development Programme. We have also completely modernised our Investigator and Case Officer training courses as well as the selection process for people seeking to fill these roles S6(a)

We are also bringing a clear focus to gender and ethnic diversity. Like GCSB, the NZSIS workforce is generally less ethnically diverse than the wider Public Service, in

part because it is more difficult to confirm the personal information of people who have not been resident in New Zealand for a long period of time (a requirement of the vetting process). We are working to address this issue.

NZSIS's Senior Leadership Team

As with the GCSB Leadership Team, you are likely to have a significant amount of contact with the NZSIS Leadership Team, which comprises:

Rebecca Kitteridge – Director-General of Security

Rebecca Kitteridge was appointed in May 2014.

Before her appointment Rebecca was the Secretary of the Cabinet and Clerk of the Executive Council, within DPMC. She served under four Prime Ministers and four Governors-General in that role and in earlier roles in DPMC.

Rebecca worked as a lawyer in private practice from 1988-1997, and then became the Cabinet Office legal adviser, on secondment from the Crown Law Office. She moved to the Ministry of Foreign Affairs and Trade in early 2001, working in the Legal Division and advising on a range of issues including Pacific constitutional issues and international treaty making. In late 2003, she returned to the Cabinet Office as Deputy Secretary of the Cabinet (Constitutional), before taking up the role of Secretary of the Cabinet and Clerk of the Executive Council in 2008. In 2012/2013 she was seconded to the GCSB for seven months, to undertake a compliance review.

In March 2014, Rebecca was appointed as a Commander of the Royal Victorian Order, in recognition of her service as Cabinet Secretary and Clerk of the Executive Council.

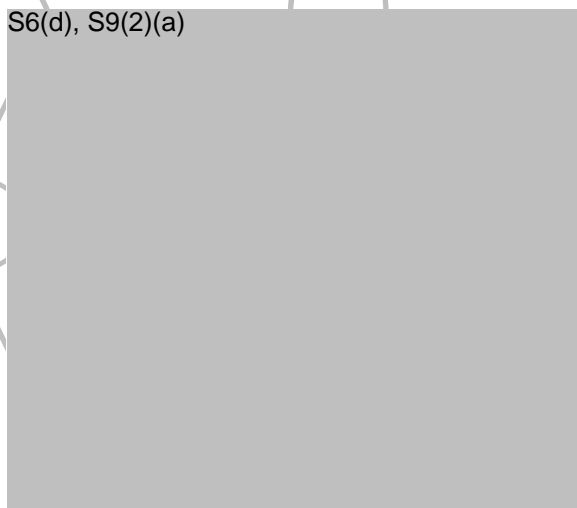
S6(d), S9(2)(a) **Deputy Director-General of Security**

S6(d), S9(2)(a)

S6(d), S9(2)(a) **Director Protective Security**

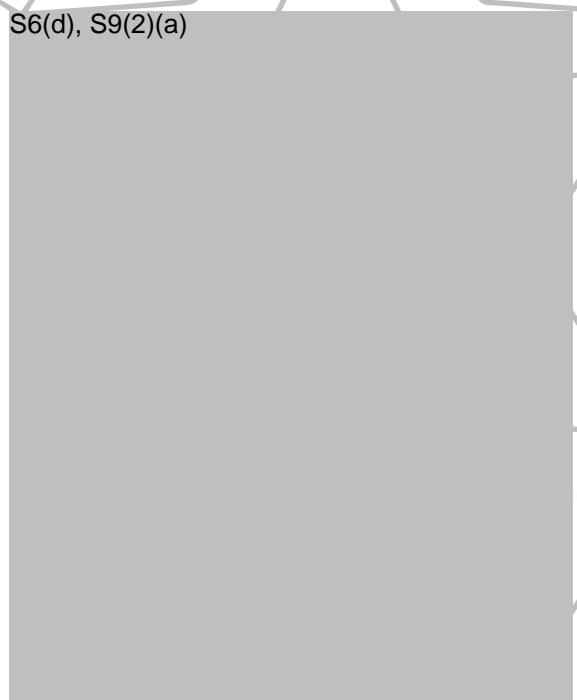
S6(d), S9(2)(a)

S6(d), S9(2)(a)




S6(d), S9(2)(a) **Director Intelligence**

S6(d), S9(2)(a)

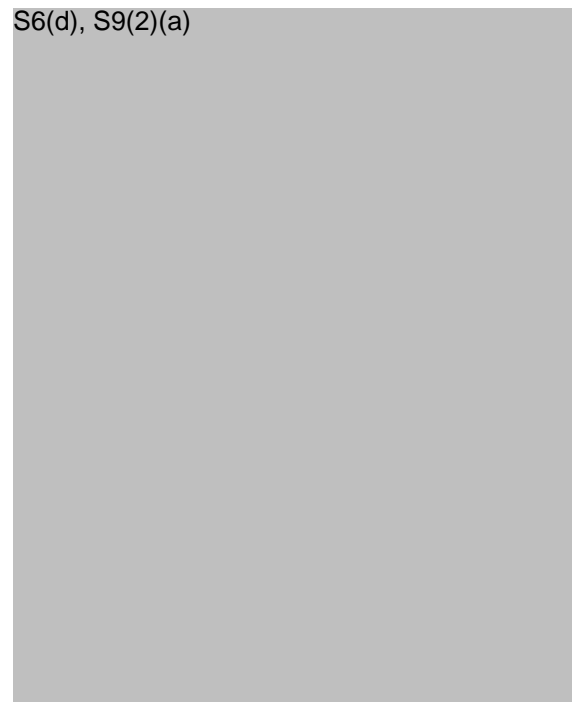


S6(d), S9(2)(a) **Director Capability**

S6(d), S9(2)(a)

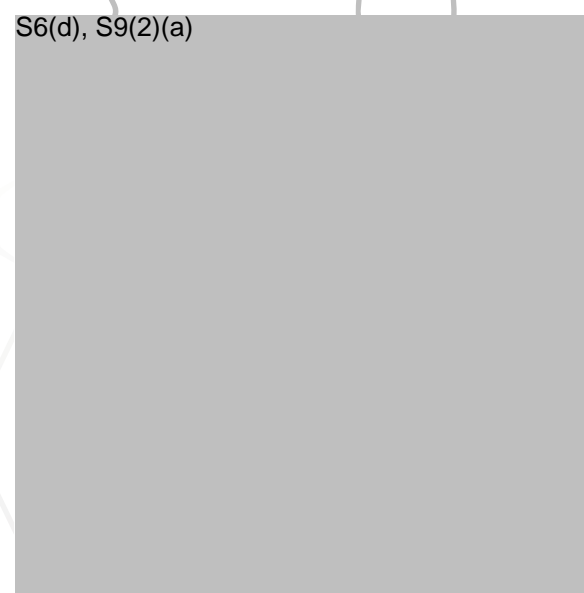


S6(d), S9(2)(a)



S6(d), S9(2)(a) **Chief Legal
Counsel**

S6(d), S9(2)(a)



Government Communications Bureau (GCSB)

PO Box 12209

Thorndon

Wellington 6144

Phone: 04 472 6881

New Zealand Security Intelligence Service (NZSIS)

PO Box 12209

Thorndon

Wellington 6144

Phone: +04 472 6170

UNCLASSIFIED

~~TOP SECRET // COMINT // NZEO~~



~~TOP SECRET // COMINT // NZEO~~

UNCLASSIFIED