

~~SECRET // NZ, REL FVEI~~



GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

GCSB Strategy 2018–2022

3/08/2018

www.gcsb.govt.nz

New Zealand Government

Table of Contents

Our Place In The New Zealand Government	3
Why We Carry Out Our Work	3
What We Do	3
The Environment We Work In	4
What We Want To Achieve	4
What We Will Focus On	4
Products And Services That Are Used And Valued	6
Relationships With Purpose	6
Retain, Develop, And Recruit The Best People	10
Government's Information Security Authority	11
Specialist Intelligence Access And Tradecraft	14
Trusted Technology	16

Our Place In The New Zealand Government

(U) We are the New Zealand Government's specialist in applying technology to produce intelligence that informs decision makers and information security services and advice that protects New Zealand's most important information and information infrastructures.

Why We Carry Out Our Work

Protecting and enhancing New Zealand's security and wellbeing.

(U) Under the Intelligence and Security Act 2017, the GCSB's principal objectives are to contribute to the protection of New Zealand's national security, the international relations and well-being of New Zealand, and the economic wellbeing of New Zealand. We pursue these objectives in accordance with the policy and priorities set by the New Zealand Government.

(U) We contribute to these objectives by supporting:

- (U) The safety of New Zealanders at home and abroad.
- (U) New Zealand's domestic and foreign policy objectives.
- (U) Reducing strategic surprise.
- (U) The protection and advancement of New Zealand's economic interests.
- (U) The ability of New Zealand and New Zealanders to go about their daily lives free from hostile foreign political interference.

What We Do

(U) The work we do that contributes to these objectives includes:

- (U) Providing the Government and other authorised recipients with intelligence to inform their decision making.
- (U) Services, advice and assistance to protect New Zealand's most important information and infrastructure from technology-borne compromise.
- (U) Services that enable the government to operate while protecting its most sensitive information.
- (U) Specialist assistance to the New Zealand Security Intelligence Service (NZSIS), the New Zealand Defence Force (NZDF), and the New Zealand Police (NZP) in the performance of their functions.
- (U) Regulating telecommunications network operators to ensure the security of nationally significant infrastructures.

The Environment We Work In

(U) We continue to work in a world of increasing change and complexity. Rapid developments in technology and the way it is used have consequences for domestic and international politics, public safety, the security and sovereignty of New Zealand's institutions and economy, and day-to-day relationships within society more broadly. International affairs are becoming more volatile after a period of relative calm and as a consequence we are seeing an increasing amount of flow-on effects impacting New Zealand and New Zealanders.

(U) New Zealand's population is older, more diverse, more technically literate, and more internationally connected than ever before. Their expectations and understanding of national security, technology, the collection and use of information, fairness, equality, and New Zealand's role in the world are correspondingly contested and evolving.

(U) We are a small and agile agency, experts in communications technology and have strong international relationships, and a highly trusted, motivated, and skilled workforce. These characteristics mean we are unique within the New Zealand Government and amongst our foreign partners.

(U) We are also an agency that has grown significantly as a result of the increased investment the Government made in the New Zealand Intelligence Community (NZIC) as a result of the 2015/16 Strategy, Capability and Resourcing Review (SCRR). Under SCRR we will continue to grow significantly over the next two to four years. We are also redefining and strengthening our role as an agency in the domestic and international system. The nature of our work can rapidly change, the demands on us are increasing, and we are now spread across more locations.

(U) Our profile with Ministers, other New Zealand Government agencies, and the public is greater than it has ever been before. The expectation that we demonstrate our value and share our story publically is, and will continue to grow. But in contrast, the work we do still frequently relies on exploiting circumstances, technology, and accesses that must remain secret for us to be effective. This is against a challenging and rapidly changing technological landscape that we must keep pace with to remain effective.

What We Want To Achieve

(U) GCSB has two ideal end-states we are seeking to achieve over the next four years:

- **(U) Indispensable Intelligence** – Our intelligence products and services consistently generate unique policy and operational impacts for New Zealand.
- **(U) Impenetrable Infrastructure** – Our services, advice and assistance means New Zealand's most important information infrastructures are impenetrable to technology-borne compromise.

What We Will Focus On

(U) To achieve these end-states, we will focus on building our capability and capacity in the following areas over the next four years.

- **(U) Products & services that are used and valued:**
(U) Customers consistently use and value our intelligence products, cyber security services, and information security advice and assistance to inform their decisions.
- **(U) Relationships with purpose:**
(U) We plan, prioritise, and pursue relationships with New Zealand Government agencies, international partners, and private sector agencies with a clear understanding of how those relationships contribute to our work. The strength of our relationships means we are trusted, valued, and influential.
- **(U) Recruit and retain the best people:**
(U) GCSB's profile as an employer of choice will allow us to recruit, develop, and retain the most skilled people. Recruiting and retaining the best people ensures we have the skills, experience, and diversity to allow us to respond to the security and intelligence challenges New Zealand and New Zealanders face on a daily basis.
- **(U) Government's information security authority:**
(U) We are trusted as the New Zealand government's authority on information security. We lead on risk management for the New Zealand Government, with respect to information security. The New Zealand government's information security consistently improves because of GCSB's work.
- **(U) Specialist intelligence accesses and tradecraft:**
(U) GCSB's access and analytical posture mean we have a portfolio of intelligence accesses and analytical tradecraft that protects New Zealand and New Zealanders and promotes New Zealand's national advantage.
- **(U) Trusted technology:**
(U) Our technology enables our work, and facilitates better collaboration with our domestic and international partners. GCSB and other agencies in the sector have access to infrastructure and platforms that are reliable and resilient, and are delivered efficiently.

(U) Each of the focus areas are discussed in more detail in the following pages.

Products And Services That Are Used And Valued

Why this matters?

(U) The value of our products and services comes from them being used by the people who receive them; products and services are not an end in themselves. Our products need to be used and valued by our customers. Customers and stakeholders must have trust and confidence in our products and services and see the real-world outcomes and impacts they can bring.

(U) "Used" means our products and services inform the decision-making process and guide actions – rather than simply being "useful" – which may not include *actual* use.

(U) "Valued" means our customers recognise our products and services make a meaningful contribution. We know this because they let us and others know of that contribution.

What we intend to achieve?

(U) Customers consistently use and value our intelligence products, cyber security services, and information security advice and assistance to inform their decisions.

What success will look like in four years?

- (U) GCSB's work will be aligned with our customers' priorities, including the governments National Intelligence Priorities and the cyber security risk environment.
- (U) Ministers and officials will recognise our contribution to New Zealand's security, prosperity, and international affairs.
- (U) GCSB defensive cyber capabilities will be able to protect New Zealand's critical national infrastructure and key national institutions from harm.
- (U) Our customers will trust in and be highly satisfied with our products and services as well as recognising their real world impact.
- (U) Customers will be able to easily access and consume our products and services and experience low barriers to their use in their work.
- (U) We will be able to measure and understand our customers' views on our products and services, which we will use to continually improve our performance.
- (U) Our customers and the public will be confident that we deliver our products and services legally and consistently with the values of New Zealanders.

What we will do to achieve this?

- (R) We will have established mechanisms for understanding customers and their needs. This will inform our decisions about what products and services to offer and the value of their real world impact.

- (b) We will have reliable and easily accessible mechanisms for customers to seek, and us to supply, our products and services.
- (b) We will provide customers with training and support about the products and services we offer and how they can be used.
- s6(a) _____
- (b) We will establish and implement a plan for increasing public understanding of our intelligence function.

Relationships With Purpose

Why this matters?

(U) GCSB, working alone, can only do so much. We use our relationships with other organisations so we can be more effective and work at a greater scale than we could alone. Many of these organisations have expertise, capabilities, and relationships that GCSB (and the NZIC) could not easily replicate. We can draw on and use these (and vice versa) to improve the outcomes we provide to New Zealand and New Zealanders.

(U) Building and maintaining relationships requires work. We need to ensure we direct our effort at those relationships of greatest value to us and New Zealand. Poor systems and processes can reduce the value we get out of our relationships, meaning it is important the systems and processes supporting our engagement with others are efficient and effective as possible.

What we intend to achieve?

(U) We plan, prioritise, and pursue relationships with New Zealand government agencies, international partners, and private sector agencies with a clear understanding of how those relationships contribute to our work. The strength of our relationships means we are trusted, valued, and influential.

What success will look like in four years?

- (U) We will be able to understand the status of our relationships with other New Zealand government agencies, international partners, and private sector entities.
- (U) We will be able to prioritise our relationships according to their relative costs and benefits.
- (U) Our operational relationships with NZSIS, NZDF and NZP will be well-defined and highly effective and efficient.
- (U) We will be seen as easy to work with by domestic and international partners.
- (U) Our relationships across the government will mean we are included in all policy matters relevant to us, and we can draw on the expertise and influence of others.
- (U) Five Eyes partners will be able to identify specific contributions we make to the partnership and the international security environment.
- (U) Our relationships mean we will have options available to us to work more closely with academia and industry e.g. R&D.
- (U) Our work with international partners will be consistent with New Zealand law and human rights obligations.

What we will do to achieve this?

- (R) We will develop and begin applying criteria to guide how we prioritise our relationships.
- (R) We will create and review operational policies and procedures that govern our work with NZSIS, NZDF and NZP to ensure they are efficient and effective.
- (R) We will ensure that GCSB and its leaders can engage effectively at the policy and technical level across government on current and future technology areas of interest, risks, and opportunities.
- (R) We will finalise and implement an international engagement strategy that will guide the GCSB in terms of how we think about our international relationships and how we invest in them.
- (R) We will establish a long term plan that clarifies the purpose of our secondments with international partners and other New Zealand government agencies. This plan also includes improving the systems and processes of our secondment programme.
- (C) We will improve GCSB's relationships with domestic academic and intelligence and security communities to bolster our - and their - understanding of the threats and opportunities facing New Zealand and New Zealanders.

Retain, Develop, And Recruit The Best People

Why this matters?

(U) Our people deal with some of the most complex security and intelligence, technology, and geopolitical challenges and issues on a daily basis. We need people with world-leading skills, experience, and diverse perspectives and backgrounds to allow the GCSB to meet and keep ahead of these challenges and changes. As an agency specialising in technology, we also need all our people to be able to engage with technology and technology-related topics.

(U) The GCSB operates in a competitive labour market, a rapidly evolving technology sector, and faces high costs and long lead times to get new staff on board. Over the next four years we want to focus on continuing to invest in and develop the staff that already work for the GCSB. Recruitment of new people will still remain important as we continue growing under SCRR, but our focus needs to shift to the development and retention of our people and giving them great career and learning experiences.

(U) There continues to be increasing competition for technologists in government and the private sector. GCSB needs to be able to access this market to recruit, but also recognises it has a role in helping to develop and upskill New Zealand's wider technology and cyber security sector.

What we intend to achieve?


(U) GCSB's profile as an employer of choice will allow us to recruit, develop, and retain the most skilled people. Recruiting and retaining the best people ensures we have the skills, experience, and diversity to allow us to respond to the security and intelligence challenges New Zealand and New Zealanders face on a daily basis.

What success will look like in four years?

- (U) GCSB will be seen as an employer of choice within New Zealand - particularly in technological fields.
- (U) GCSB will rank in the top 25% of Public Sector agencies for staff engagement.
- (U) Our technology specialists will be seen as the experts in New Zealand.
- (U) Our people will have access to tools and systems that enable rather than hinder them in their work.
- (U) We will be able to grow and develop our people in whatever field, and at whatever level, they choose to operate in.
- (U) GCSB will be a diverse and inclusive organisation that represents the communities we serve. We value and respect that diversity and inclusivity.
- (U) Our leaders will be seen by our people as drivers of success and change, and will empower their people and the wider organisation.

- (U) Our people will be given the opportunities and space to experiment and think about the future needs of the GCSB, NZIC, and our domestic and international partners.

What we will do to achieve this?

- (U) We will know the current and future development needs of our people and be active in upskilling and developing our workforce.
- (U) We will have initiatives in place to increase the diversity and inclusivity of our workforce.
- ~~(R)~~ We will know what the retention pressures are for the GCSB and the NZIC and have a plan in place to address these.
- ~~(R)~~ We will improve the accuracy and impact of our recruitment campaigns to ensure the people we hire come with a broad range of experiences, profiles, and skills that deepens our diversity and promotes better intelligence and security outcomes for New Zealand.
- ~~(R)~~ We will continue to improve the GCSB and NZSIS career progression framework and ensure our people a healthy mix of career opportunities across multiple disciplines – both internal and external to GCSB.
- ~~(R)~~ We will put effort into developing our leaders so they can meet the challenges the future holds for GCSB and New Zealand.
- s6(a) 

Government's Information Security Authority

Why this matters?

(U) The New Zealand Government is increasingly recognising the importance of information security and for New Zealand's security experts and decision makers to be well informed about intelligence and security risks, threats and vulnerabilities. The consequences of the New Zealand government having poor information security could be catastrophic – potentially impacting the security of New Zealand and government personnel, the trust of our international partners, the New Zealand economy, the privacy of New Zealanders, and the provision of public services.

(U) Our expertise and capabilities mean we are best suited to lead system-wide improvements in the government's information security. We have technical expertise, a multi-layered cyber defence capability, a regulatory function, relationships throughout the New Zealand government and private sector, and strong relationships with information security leaders internationally.

What we intend to achieve?

(U) We are trusted as the New Zealand government's authority on information security. We lead on risk management for the New Zealand government, with respect to information security. The New Zealand government's information security consistently improves because of GCSB's work.

What success will look like in four years?

- (U) We are recognised and trusted as the government's expert advisor and trusted rule-maker on information security.
- (U) We will be able to understand the scale and nature of current and emerging threats to the security of the government's information and infrastructure.
- (U) The New Zealand government will be using our advice, guidance and policy to make measurable improvements to their information security.
- (U) We prioritise the delivery of advice, guidance and policy based on our specialist expertise, technical accesses, and relationships with partners.
- (U) The New Zealand government's information security standards will form a coherent part of the broader protective security framework, and supports government's digital transformation initiatives.
- (U) Our COMINT security role will be recognised, understood and respected within the New Zealand government and by foreign partners.

What we will do to achieve this?

~~SECRET~~ We will be established as the functional lead for information security within New Zealand and exert system leadership to improve the New Zealand government's incident response and deterrence preparedness.

- (R) We will implement a risk management framework, which allows GCSB to inform stakeholders and customers of information security threats and vulnerabilities, and enable customers to manage the impact of security risks.
- (R) We will bolster and grow GCSB's information security policy unit within IACD, and support the continuous improvement of the New Zealand Information Security Manual, and information security guidelines.
- (R) We will support closer alignment with the NZSIS PSR engagement team to support improvements in wider protective security matters.
- s6(a) [Redacted]
- s6(a) [Redacted]

Specialist Intelligence Access And Tradecraft

Why this matters?

(U) Through its unique access, GCSB contributes to the safety and well-being of New Zealand and New Zealanders by providing intelligence and security products and advice. Given the changing domestic and international environment, and the rapid change in the technological landscape, the GCSB must ensure that it has the right accesses, tradecraft, and domestic and international relationships to be able to keep decision makers well informed about matters of importance.

(U) GCSB also occupies a unique position within the government that means we can, and should, provide specialist support and capabilities to other agencies that enables them to fulfil their roles and functions e.g. NZSIS, NZP, and NZDF.

~~(S)~~ New Zealand, via GCSB's relationship with Five Eyes agencies, benefits significantly from the Five Eye's SIGINT system – in the intelligence products we receive, the information, technology, and skills we have access to, and in the international relationships New Zealand has (via the GCSB) with Five Eyes governments more broadly.

s6(a)
[Redacted]

What we intend to achieve?

(U) GCSB's access and analytical posture mean we have a portfolio of intelligence accesses and analytical tradecraft that protects New Zealand and New Zealanders and promotes New Zealand's national advantage.

What success will look like in four years?

- (U) We will provide domestic and international partners with unique security and intelligence insights.
- (U) We will develop cutting edge capabilities and analytical postures across all GCSB missions allowing us to contribute unique access that cannot be provided by partners.
- (U) NZSIS, NZDF, NZP, and others will be benefiting from our specialist SIGINT accesses in carrying out their operations.
- Our tradecraft will be seen as world leading.
- s6(a)
[Redacted]

- s6(a) [Redacted]

What we will do to achieve this?

- s6(a) [Redacted]
- s6(a) [Redacted]
- s6(a) [Redacted]
- s6(a) [Redacted]

[Redacted] (P) We will foster a culture and systems that promote innovation.
[Redacted] (P) Our policies, procedures and compliance mechanisms will support our people in their activities and be easy to apply.

Trusted Technology

Why this matters?

(C) GCSB and wider sector outcomes fundamentally depend on technology. Over the next four years, we will invest to ensure that our platforms and core infrastructure meet mission and organisational requirements, today and in the future. s6(a)

[REDACTED]

(R) Two programmes – Cryptographic Products Management Infrastructure (CPMI) and the New Zealand TOP SECRET Network (NZTSN) – will be key focus areas over the next two years in particular. Through these programmes, GCSB will take on an increased role for technology delivery within the intelligence sector. This will have benefits for the GCSB's mission, but we will also measure our success in terms of the excellence of our service delivery to NZSIS and other sector agencies.

What we intend to achieve?

(U) Our technology enables our work, and facilitates better collaboration with our domestic and international partners. GCSB and other agencies in the sector have access to infrastructure and platforms that are reliable and resilient, and are delivered efficiently.

What success will look like in four years?

- (U) GCSB has modern applications and tools to support and enhance the delivery of our mission objectives and outcomes.
- (U) Our technology infrastructure and its performance will be match-fit and meet demanding performance standards. It also means we will be able to keep pace with future change.
- (U) GCSB provides applications, tools, and infrastructure to support and enhance the delivery of other government agencies mission objectives and outcomes.
- (U) Our technology will allow us and others to easily collaborate with our domestic and international partners e.g. the NZSIS, NZDF, Police and Five Eyes.
- (U) Our compliance and legal obligations will be made easy through our application of technology e.g. smart data and data retention and destruction that promotes good practice.

- (U) Duplication of technology solutions will be reduced within the GCSB, NZSIS, and wider New Zealand security and intelligence sector.

What we will do to achieve this?

• (R) Core NZTSN infrastructure and applications will be established and delivered to all relevant agencies.

• (R) Optional Top Secret Network infrastructure and applications will be available to relevant agencies.

• (R) Our new cryptographic infrastructure will be fully operational.

• (S) [Redacted]

• (R) New data transport mediums will support compliance and audit requirements and will enable intelligence and security outcomes.

