

The importance of leadership and customer focus in a dynamic security and intelligence environment

Introduction

Thanks so much for having me. I have been looking forward to doing this sort of thing. It's time to start the process of opening up the NZSIS to the wider New Zealand public sector and eventually the public in general, but until now, it hasn't been possible. So this is my first outing and I am really pleased to be here.

Can I start by thanking you all at Customs for the fantastic help you give to the NZSIS across a range of work. At an operational level, and particularly at the border, we get great cooperation from you guys. So while I will be talking about the importance of working together collaboratively and in different ways, there is a good starting point, which is great.

I want to talk for a few minutes about the things that are on my mind about the NZSIS and the broader security sector, and then I want to open it up to hear what interests you, so there will be plenty of time for questions and answers.

I have three key messages:

- Geopolitically and domestically the threats that we face are becoming more complex.
- In this challenging context, we must work together or we will not keep New Zealand safe.
- Leadership exists at every level of any organisation, and showing collaborative, customer-focused system leadership is what will get you ahead in the public service environment now and in the future.

I know this is an unclassified forum, but I will be speaking frankly and openly, so can I just ask upfront that you respect that.

I took on the role of Director of Security on 1 May – 133 days ago. It is an exciting challenge to lead a team of people who are focused on a mission – to protect New Zealand and New Zealanders from harm and enhance New Zealand’s opportunities by enabling well informed decisions. This is done in the true kiwi way - with well-meaning people, making do with fairly limited resources, striving to do the best they can for New Zealand. But, it is clear to me - and it is clear to my staff – that we cannot succeed on our own. We can only succeed in partnership with others, so perhaps the title of this presentation from the importance of leadership and customer focus in a dynamic security and intelligence environment – something of a mouthful – could be summarised as “Better Together”.

I thought I would start by giving a little overview of the global and domestic threatscape from the NZSIS perspective – to give a sense of the complexity which I know you too see through your Customs lens.

The global threatscape is complex and constantly changing, and our place in the world is not immune from these issues. While the New Zealand threatscape is relatively benign, it is changing. Traditionally, the most significant threats to our national security have resided offshore – so what crosses the border (be it physical or cyberspace) has always and will continue to be really important to us.

If we look at that threatscape - we are faced with a range of significant issues: violent extremism (which the Americans call terrorism), espionage and efforts by some states to obtain weapons of mass destruction – particularly nuclear capabilities.

Terrorism has developed over the decades. It started with isolated incidents of violence in the 1970s and 80s, where individuals or small groups were targeted with hijackings or the threat of small attacks to extract a political concession. In the 1990s and early 2000s we saw a dramatic shift to larger scale, mass casualty attacks, where the motivation was more about seeking change through instilling a deep-rooted fear in a population for a longer term gain, rather than any immediate political concessions.

In the past decade we have seen the maturing of the franchised terrorist group model. There has been a shift, from a strong centre (core Al Qaeda) directing traffic, to the proxy group approach. Under this approach, franchise groups such as Al Shabaab, AQAP, etc] operate virtually autonomously in ungoverned spaces around the world, undertaking attacks locally or being used as a platforms to strike further afield. The IED in toner cartridges was a good example of a franchise group – in this case AQAP – picking up the mantle of taking the fight to the enemy in an asymmetric way. Their expenditure of a few thousand dollars by AQAP probably caused a billions dollars worth of security response.

We have seen the threat evolve further to a crowd-sourcing model where, through the mechanisms of social media, individuals are encouraged to fight wherever they are, with whatever they have available – such as the Boston marathon bombing. In these circumstances, threat is less a function of intent and capability. It is all about intent, as capability can come in any form.

Syria, however, has moved terrorism in another, more disturbing direction. The numbers of individuals involved and the complexity of the situation mean that it is different from previous conflict zones like Afghanistan, Yemen and Somalia, or Iraq and the Balkans in the 1990s – 2000s.

The concept of foreign fighters rushing in to protect Islam from Western aggression has been replaced by a borderless aspiration of establishing what I see as a perverted version of the Islamic Caliphate. While the establishment of a Caliphate was an underlying goal of Al Qaeda, the current approach has more to do with the traditional power play between the Sunni and Shia than it does in countering Western influence in the Middle East. So the battles are still waged on multiple fronts, but there is now more than one category of enemy. This complexity has led to some surprising alliances, mainly to counter Iranian dominance and influence.

Another disturbing issue in the current evolution of global terrorism is the apparent lack of discipline and control, and even the lack of humanity, that characterises some of the actions by those fighting in the name of the so-called "Islamic State" – a name which I utterly reject, as this group is neither representative of Islam nor a state. Random acts of extreme violence and the subsequent glorification of that in some media, changes the dynamic by moving the centre towards the margins. The risk is that what is acceptable and normal may shift. I am reminded of a recent DomPost cartoon in which Mao, Stalin and Hilter were lamenting that their legacy for horrific crimes was being overshadowed by ISIL – which is pretty close to the mark.

It is a real concern to me when individuals hold extreme or radical views, and these views are combined with a propensity for violence and a desensitisation of what is normal human behaviour. As for most Western democracies, the risk for New Zealand when our citizens are exposed to this type of behaviour (either directly or vicariously) is how that plays into their intentions and behaviours on the street in Auckland or Christchurch or Hastings. We regard the impact of a so-called foreign fighter returning to NZ as a potential game changer.

Countering terrorism is not the only thing that concerns me. Proliferation remains a global security issue and New Zealand is committed to ensuring that we are not a source country for components, technology or knowledge ^{6(a)} [REDACTED]
[REDACTED]. Again, New Zealand has not been immune to efforts by individuals and cover companies to procure items here or by exploiting New Zealand's good reputation elsewhere.

And then there is the world of espionage. I was a little surprised to find out the extent of spying that goes on in New Zealand. I was probably one of the many people in New Zealand who wondered whether it really went on after the end of the cold war. Who would target New Zealand? Where is the evidence, where's the smoking gun? I could see this on a Tui billboard – Espionage is the real threat to New Zealand, Yeah Right. But you know, the sceptics are wrong. The thing about espionage is that good spies don't get caught, so it is difficult to estimate the size of the problem. What I can say, is that espionage represents one of the greatest areas of long-term harm to this country. Some espionage activity is subtle, undertaken assiduously over time. Some takes the form of blatant cyber attacks, but there should be no doubt that espionage and foreign interference in the democratic system of government is ongoing and of deep, enduring concern.

So those are some of the things I worry about in terms of the geopolitical and domestic threatscape. There are many ways of countering these types of threats, but human source coverage is often the only way to filter information and determine the truth. That is what NZSIS does, but again, we rely on the cooperation and support of others to identify leads and assist with investigations that, more often than not, have elements that traverse the NZ border.

This is not rocket science, we instinctively know that with most things, the total is always greater than just the sum of its parts. The Service and Customs have a long history that recognises this fact. In 2002, the NZ Customs Service joined forces with NZSIS and GCSB to form the Counter Proliferation Joint Section - a team-based approach of bringing people together from their home agencies, with their skills, information and technology, and putting that in a room together with others doing the same thing. This model has been very successful over the years in identifying, investigating and preventing NZ being used as a source of proliferation of weapons of mass destruction or the means of their delivery.

6(a) [REDACTED]

[REDACTED] We work closely with Internal Affairs to make recommendations to cancel the passports of New Zealand citizens seeking to travel abroad to fight in Syria.

6(a) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Another challenge facing NZSIS is how to maintain collection in the face of advancing technology. (b)(a) [REDACTED]

[REDACTED]

(b)(a) [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

I encourage this type of initiative 100% as we seek to bring different perspectives to bear in a complementary way to refine assessments and avoid group think.

The reality is, though, that great systems, great collection and great analysis will still not be enough to tackle the challenges we face. What we need is partnerships between our agencies, and that is mostly about people – making it work. In a small country we can only succeed if our default setting is to share and work together, based on relationships of trust.

I don't know why it is so hard to share and collaborate. I guess humans may tend towards territorialism. The public sector reforms of the 1980s entrenched that tendency because of the very siloed nature of the departmental accountabilities and funding. And I think in the uniformed and operational services like Customs and the NZSIS there is an even stronger culture favouring clear command structures. None of these factors help us to share and collaborate – even when the threats faced by the nation demand that we do so.

The government, through the Better Public Services reforms, has been insisting for several years now that we get over ourselves and behave differently – cluster around issues, focus on results. We must respond to that challenge. We must get it right without waiting for a major disaster to be the catalyst for reinvestment or change. Our agencies (particularly in the intelligence area) have no excuse for continuing the historical pattern of intelligence agencies all around the world – failing to reinvent themselves or to change their operating models and capabilities until forced to change by a terrible event. Not only does it signal a failure to meet our obligation to protect New Zealand, it has a far less than optimal outcome in terms of capabilities. If an agency has fallen behind in terms of capabilities, investment after a crisis only tends to bring it up to today's standards, not position it to face the problems of the future.

So what does this mean for all of us?

Leadership to me is about working together at every level to deliver on our respective missions. There should be no daylight between operational agencies with common goals and objectives.

While we look to invest in technology and tools to help with collection and analysis, we also need to be investing in people.

I really support the concept of sharing our people across the security sector. 6(a)

[REDACTED]

[REDACTED]

6(a) [REDACTED]

[REDACTED]

[REDACTED]

More broadly, we are working in the NZIC on a standardised talent management and career development structure, which could be broadened into a sector workforce strategy. I would love it if there were a systematic way of ensuring that NZSIS staff get the broader experience that Customs and other agencies would offer them. It will help us to stop being so “spooky.” I also think you would get a huge amount out of living in our world for a while.

We can also cluster together in other ways. One model is the ITOC in Auckland, in which the Service has participated for some time. That seems like a really impressive example of working together, and it is something I hope to see much more of.

At the same time as we as look to strengthening our connections with other agencies across the government sector, we can look to a stronger core that has developed in the Department of Prime Minister and Cabinet. Howard Broad, a former Police Commissioner, is now the Deputy Chief Executive for National Security. Howard brings a wealth of experience and gravitas to this role and one of his catch cries is “total cohesion”. I think you get the message that there is common theme going on here.

Carolyn may have mentioned to you that she and I attended a public sector CEs’ retreat last week. We were given a challenge, which I will put to you, because the reality is that every single person in this room has an opportunity to lead this change. The challenge we were given was to try to practice these three simple habits every day:

- To ask curious questions – questions that are genuinely open, and to which you do not know the answer.
- To take multiple perspectives – at the end of a discussion, to ask the question “whose perspective have we not taken into account?”
- To always try to think about a problem or a situation at a system level.

Apparently studies show that these three simple habits can make a huge difference to organisational leadership – and they are available to every person here.

And of course that is my challenge too. Like you, I am part of a system to which I need to contribute and from which I need help. NZSIS has its own customers and relationships, and I want to make sure that the stakeholder and customer interaction with NZSIS is a delightful experience. Even in vetting! That is an obvious area where gains can and must be made if we are to retain the confidence and support of those we serve.

So that's a quick gallop around the traps. As mentioned at the start, I have covered three main points:

- Geopolitically and domestically the threats that we face are becoming more complex.
- In this challenging context, we must work together or we will not keep New Zealand safe.
- Leadership exists at every level of any organisation, and showing collaborative, customer-focused system leadership is what will get you ahead in the public service environment now and in the future.

To conclude, the value proposition that we offer to the New Zealand Government is that the security and intelligence sector works together to provide the right knowledge, at the right place and at the right time. We can only do this in partnership and we are always going to be 'better together'.

Talking Points for NZDF Command and Staff College

Tuesday 20 October, 9.00am – 9.30am

Topic: "How the GCSB and NZSIS contribute to the safety and security of New Zealand"

Una:

[welcome etc]

We are pleased to speak to you today about GCSB and NZSIS contribute to the safety and security of New Zealand.

In summary, the reason New Zealand has an intelligence community is to:

- Help keep Kiwis safe (for example, identifying terrorist threats at home and abroad)
- Help protect and grow the economy (for example, providing or enabling cyber security)
- Provide foreign intelligence and assessment (so the Government knows more about the capabilities, intentions and activities of foreign persons and organisations).

Rebecca:

How do we help keep Kiwis safe?

In order to keep our country secure and protect our citizens, we have to be able to intercept private communications in some exceptional and legally authorised circumstances.

NZSIS investigates and communicates information relating to threats to our national security.

These threats include terrorism, proliferation of weapons of mass destruction, and espionage, both against the Government and against economic entities in New Zealand.

NZSIS investigates individuals whom who may pose a threat to security and can monitor individuals under warrant.

An example of how NZSIS advice might be used is in the cancellation of passports. NZSIS can recommend the cancellation or refusal of a New Zealand passport on national security grounds. We've made recommendations that have resulted in passport cancellations where individuals intend to travel to the Middle East for the purposes of fighting.

The Combined Threat Assessment Group, or CTAG, is an inter-agency capability which sits within NZSIS. CTAG is made up of staff from a range of NZ government agencies, including NZSIS, GCSB and NZDF.

CTAG assess threats posing physical harm to New Zealand, its citizens and its interests, both domestically and overseas.

It ensures assessment advice of these threats is given to the appropriate people, often other government agencies, so that risks can be mitigated.

It also sets the New Zealand domestic terror threat level.

NZSIS and GCSB also use our capabilities to underpin and support the activities of law enforcement agencies and the NZDF.

This can be through the provision of core intelligence or by helping them to better undertake their work^{6(a)}

6(a)

6(a)

Una:

We protect and grow the New Zealand economy by helping Government and key economic companies to protect their information, assets and people.

New Zealand government and private sector entities are targets and victims of malicious actors.

Project CORTEX, run by the GCSB's National Cyber Security Centre, is a key initiative for countering these threats.

Its sole purpose is to counter cyber threats to organisations of national significance by applying a number of layers of technical protections.

At the heart of these capabilities is the detection of foreign-sourced advanced malware.

CORTEX is in the process of being rolled out, and so far it's going really well.

GCSB also makes sure that national security buildings are physically secure and that we have secure communications. We do this across Government, including for NZDF.

6(a)

We also have to be able to keep the confidences of other countries we work with, and who share information with us, otherwise they will not work with us.

Rebecca:

The NZSIS leads a multi-agency programme to strengthen New Zealand's protective security arrangements and behaviours.

This programme is known as the Protective Security Requirements, or PSR.

It aims to strengthen security across government, with a focus on protecting the key elements of people, places and information.

One of the first lines of defence in protecting New Zealand's information, assets and people is the vetting system run by NZSIS.

It ensures that the people who can see the most sensitive information the Government holds can be trusted. This includes the foreign intelligence that we provide to Government

Una:

GCSB and NZSIS provide foreign intelligence to assist the Government to understand what others are doing or intending to do and trying to keep from us.

Foreign intelligence, and the assessment of it, is vital for knowing what is going on in the world, whether that be strategic challenges, political and economic instability, or security issues.

New Zealand is a global trader and New Zealanders are global travelers. We need to be fully informed about international issues that matter to us.

This includes the security our 'backyard', the South Pacific.

Of course, New Zealand's international interests extend beyond the South Pacific, and foreign intelligence makes an important contribution to our understanding of both the broader trends at work and the specific issues decision-makers are confronted with on a daily basis.

Rebecca:

We hope that we've given you some insight today into how the GCSB and NZSIS, through their many functions, contribute to the safety and security of New Zealand.

I expect that some of the other speakers today will talk more about some of the things we've touched on.

In the meantime, we'd be happy to answer any questions you have.





Speech: 6(a)

Monday 7 May, 1pm in Room 6(a)

Introduction

[Andrew]

Good afternoon. I'm Andrew Hampton the Director-General of the GCSB and this is Rebecca Kitteridge the Director-General of Security at the NZSIS.

We've got about an hour with you this afternoon to talk on Building Trust and Confidence. We thought we would talk for around 20 minutes about the journey both of the agencies have been on, and how that journey has helped build public trust and confidence in the agencies as well as brought us to be much closer at both an operational and organisational level. Followed by questions.

I think it's fair to say that the New Zealand Intelligence Community has recently completed a period of significant change and growth.

New Zealand is an open country in a globalised world. This benefits us significantly and is reflected in our values, institutions and economy.

As is the often the case, these benefits and opportunities come with risks and threats.

The role of the NZSIS

[Rebecca]

So what does the NZSIS actually do? Like the GCSB we collect, access and report on intelligence in accordance with priorities set by the Government and in the line with New Zealand's laws and its human rights obligations.

While the GCSB is focused on electronic communications, the Service is focused on HUMIT. We also provide protective services including security vetting for all of government and personnel security advice.

6(a) [Redacted]

[Redacted]

6(a) [Redacted]

Threatscape: Espionage

[Rebecca]

[This section is based on talking points developed to support MFAT – this is the first time they’ve been incorporated into our messaging]

We are vigilant against foreign interference intended to undermine New Zealand’s national interests.

This is not new, but we are concerned by the increasing scope and scale of foreign interference activity.

6(a) [Redacted text block containing multiple lines of blacked-out content]

Threatscape: Terrorism

The counter-terrorism environment in New Zealand is still dominated by the influence of ISIL.

At any one time between 30 and 40 people are listed on the NZSIS’s counter-terrorism risk register. These individuals are assessed to represent an actual or potential threat to New Zealand related to terrorism.

Looking ahead, New Zealand is concerned about the effect of retuning foreign fighters and regional security more broadly should ISIL’s attention turn to South East Asia.

The role of the GCSB

[Andrew]

The GCSB is a SIGINT or signals intelligence agencies meaning we specialise in intelligence derived from electronic communications. We also have a statutory role in cyber security an information assurance.

6(a) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

Threatscape: Cyber

New Zealand's cyber threat environment is increasingly complex.

A key way that the GCSB protects organisations of national significant is through a system we call CORTEX. It's focused on detecting and disrupting complex and persistent foreign-sourced malware that is typically beyond the capabilities of commercial available tools.

In November 2017 the GCSB released its second unclassified cyber threat summary. It found of the 396 serious incidents recorded nearly a third had indicators of connection to foreign intelligence agencies.

New Zealand organisations are subject to both direct and indirect threats, and are being used as staging points by threat actors to target systems in other countries.

Motivation varies from espionage to revenue generation and seeking to secure political outcomes.

Cyber-attacks are relatively cheap and effective, and to date the implications of getting caught have not been great.

In February I added New Zealand's voice to the international condemnation of the NotPetya cyber-attack which international partners have now attributed to the Russian Government. It targeted the Ukraine but also had a global impact.

In December I also joined international partners to express concern about the international reports which link North Korea to the major WannaCry ransomware campaign.

While New Zealand was not significantly impacted by NotPetya or WannaCry, we are not immune from this type of threat. That's why it's important that like minded countries continue to publicly condemn reckless and malicious activity.

The journey we have been on

[Rebecca]

To respond to this threatscape and to overcome the impediments of our size and spread, we are transforming how we operate as an intelligence community.

The theme of Building Trust and Confidence is appropriate when reflecting on the journey of change the agencies has been on.

For me this journey started in 2012 when I was to carry out an independent review of the GCSB's compliance.

The Kitteridge Report found that there were long-standing, systemic problems with the GCSB's compliance systems and aspects of its organisation and culture. It also highlighted the need for the GCSB to have a clear legal framework to operate within.

The report was always written with the intention of releasing it publicly. The public release was brought forward by a week or so following an unauthorised disclosure.

Not surprisingly, there was wall to wall media coverage and debates in Parliament on both the unauthorised disclosure and the content of the report.

It was not only an incredibly tough time for the incredible staff here at the GCSB, but it also had a wider impact on the trust and confidence in the New Zealand intelligence agencies as a whole.

It was a result of my experience working with the GCSB I was motivated to apply for the top job at the Service a year later.

Soon after arriving at the Service I kicked off a review similar to the one I had carried out at the GCSB. Not surprisingly I found similar issues at the Service and it was clear that a huge amount of work was needed to turn things around.

It's around this point that the journey of change for both of the agencies really kicked up a gear.

To maintain public trust and confidence, as much as to maintain the social license to function, we have to strike the balance very carefully when it comes to our security and intelligence agencies.

To briefly summarise some of the key changes:

- The agencies were subject to a couple of reviews, including the Independent Review of Intelligence and Security in New Zealand and our Strategy Capability and Resourcing Review;
- As part of the New Zealand Government's 2016 Budget, we again received significant new funding and we are investing in both people also capabilities;
- Our agencies are growing at pace - for example, the NZSIS is doubling in size over the six year period from 2014 to 2020; and
- Since last year, the NZSIS and GCSB have been operating under a new single statute - the Intelligence and Security Act 2017.

The new era

[Andrew]

For us the new legislation is incredibly important. I'm very strong believer in following not only the letter but also the spirit of the law and we needed a much cleared legal framework to operate within.

The Intelligence and Security Act replaces the four statutes that previously applied to the New Zealand Intelligence Community. We now have a single, modern and cohesive statute. The Act contains:

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

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

The legislative changes will not have an impact on existing information-sharing arrangements with Five Eyes partners. The Act does, however introduce a more explicit requirement for our Minister to take into account human rights considerations when authorising our agencies to share information with partners.

All of the changes we have outlined – to our funding and legislation – have been underpinned by significant efforts by Ministers and the leadership of both of our agencies to be more open and transparent – and to build public awareness of New Zealand's threatscape – particularly on cyber and terrorism matters.

Indications are that this approach is working; the Intelligence and Security Act passed through Parliament with near unanimous support. Unlike five years ago, New Zealand's Intelligence agencies are not the focus of negative media attention and polling indicates public perception of our agencies and awareness of the threatscape are lifting.

Building joint capability

[Rebecca]

The New Zealand Government's investment in our community is based on delivery of clear community-wide outcomes - not on individual agencies continuing to do what they have always done.

To improve how GCSB and NZSIS work together as a community, we have:

- A shared Four Year Plan – a platform for aligning strategic intent and prioritising resources towards common goals;
- A Joint Leadership Team, with senior representatives from both agencies to govern shared work programmes including work to improve the value our customers receive from intelligence products;
- Joint workforce planning based on common remuneration, job families and a shared recruitment campaign; and
- Shared security, finance, human resources and facilities services.

We also established a Joint Office of the Director's-General and are reviewing ICT enablement with a view to determining the benefits of a joint – or at least more closely aligned ICT function.

All of these changes set us up to deliver – both in terms of the New Zealand Government's very clear intelligence requirements - and our ability to contribute to the Five Eyes partnership.

Our focus is now on growing as quickly and as safely as possible.

Our emphasis as a community over the next couple of years is on:

- continuing to build capability in the areas of collection, cyber defence, and investing in information management technology;
- recruiting, developing, and retaining the best and brightest people;
- ensuring we embed and capitalise on the opportunities our new legislative framework has created for us – for example allowing the NZSIS and GCSB to work more closely together on national security issues.

Translating change into trust and confidence

[Andrew]

Ensuring the agencies have the right mechanism in place to ensure that they are lawful and compliant has been incredibly important in building trust and confidence.

I'm pleased to say that for three years in the row the Inspector-General of Security Intelligence has found the GCSB's systems and processes to be fully compliant and that our staff have a strong culture of legal compliance.

In recent years Rebecca and I have been actively pushing our agencies towards greater transparency and openness where possible.

Where we can we're keen to release official documents to increase the public understanding of what we do and why we need to do it.

For example, our recent unclassified Annual Reports included more information than ever before; our joint Briefing to the Incoming Minister was released with a small number of reductions; and I believe our responses to Official Information Requests have greatly improved.

Being able to engage more with the public about the risks New Zealand is facing, and the role the Service and the GCSB has in mitigating those risks in fundamental to building trust and confidence.

Rebecca and I are also engaging with the public more than ever before. An area we're actively pushing the boat out is around our promoting the unique career paths the agencies offer.

For example, the GCSB has been championing the need to encourage more women into science, math, engineering and technology background into techy care paths. We're doing this through our Women in STEM tertiary scholarship programme. This scholarship has enabled me to speak at Universities around the country and a wide variety of media outlets.

The Service in the last few weeks had an active Surveillance Officer interviewed about their role to kick off a recruitment campaign for SOs.

Closing Remarks

[Rebecca]

As we've outlined the agencies have been through a massive journey in recent years.

It has been a busy time, we remain resolutely focused on delivering against the priorities set for us by the government while continuing to build on the public trust and confidence and maintain our social license to function.

Thank you.

NZDF Staff College speech

5 May 2017, 9.15 to 9.30am, Room 2,19, PHoP

AH is speaking first and will hand over to you.

Thank you Andrew. Good morning everyone

I am very pleased to be invited to speak to you all today. I see this as a great opportunity to increase your understanding about my organisation - the New Zealand Security Intelligence Service - and the ways in which we work with the Defence Force.

I have been Director of the NZSIS for three years and it's fair to say that the organisation has been on a steep journey of transformation to bring us to a place where we are more proactive and planned, more future-focused and much more collaborative. I think it is a really exciting time to be part of the New Zealand Intelligence Community.

Today, I would like to talk about:

- who we are and the work that we do,
- our organisational growth and development programme,
- recent legislation changes that enable our work, and
- the importance we place on having strong, healthy and productive working relationships with Defence and Security agencies.

So who we are and what we do:

The New Zealand Security Intelligence Service focuses on keeping New Zealand and New Zealanders secure. Our work can be broadly split into **three functions**:

1) We provide protective security advice and security screening services

- The NZSIS's role is about providing advice and support to New Zealand state sector agencies and to outline the Government's expectations of the public sector for **managing personnel, physical and information security**, and supporting agencies to better manage risks and assure continuity of delivery.
- This area includes our **vetting services** which you will have come across when you applied for a security clearance.
- My agency also **screen people visiting or seeking residency** who may pose a risk to national security. We do this by gathering information about them from police records, travel information, interviews and other sources.

2) We are a Security Service

- We use a wide variety of **sources and methods** to identify, and provide advice to counter threats to national security to New Zealanders at home and abroad.
- The **threats** include terrorism and violent extremism, espionage conducted by other states, the proliferation of weapons of mass destruction, and hostile cyber activities.
- We **work closely with partners** such as the New Zealand Police, the New Zealand Customs Service, the Department of Internal Affairs, Immigration New Zealand and the New

Zealand Defence Force to prevent threats to security progressing to acts of violence or espionage.

6(a)

3) We provide Foreign Intelligence advice

- 6(a)
- Foreign intelligence, and the assessment of it, is vital for **knowing what is going on in the world**, whether it is strategic challenges, political or economic instability, or security issues.
- Based on the information we gather, we provide **advice to other government agencies** such as NZDF or the Ministry of Foreign Affairs and Trade or to our international partners.
- In this role, the fundamental business of intelligence is about **helping decision makers manage risks** to New Zealand's interests.

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, we are nearing the end of a journey of change which started in 2014. This leads me onto my second point - **development and growth programme.**

In 2014, we launched our organisation-wide development and growth programme which focuses on five different areas - match fit leadership; outstanding people; systems that enable; delivery excellence; and powerful profile.

In the last two years, the NZSIS has also developed a new operational strategy which looks to a ten year horizon. The operational strategy answers the questions - what are the NZSIS's key outcomes and strategic goals, and how should NZSIS best go about achieving these?

For most organisations, there is a straight-forward path between mission and vision. For the NZSIS success will not, ultimately, be measured by what the organisation does individually, but rather how it is able to contribute to wider security and intelligence sector outcomes. National Security is a team sport. As such, the priorities outlined in our operational strategy are designed to enable the NZSIS to meet the intelligence priorities and the security outcomes of the government.

You may be aware that in Budget 2016 the Government announced an increased funding package for the New Zealand Intelligence Community of \$178.7m over four years. This was the result of a significant amount of work to review **NZIC Strategy, Capability and Resourcing**. This was very similar to the Defence Mid-point review. One of the key priorities for my organisation is to work with the NZIC and the wider Defence and Security sector over the coming four years to grow our capabilities and resources.

I know Andrew has already spoken about the ways in which we are working together to build joint capability.

Another component of our strengthened working relationship is our **new legislation**.

In 2015, Dame Patsy Reddy and Sir Michael Cullen commenced an independent Review of Intelligence and Security which reported back to government in early 2016. The review proposed new legislation.

Our previous legislation, the NZSIS Act was enacted in 1969, and as I'm sure you can appreciate, there have been significant changes in technology and capability since then.

On 28 March this year, the Intelligence and Security Act 2017 was given Royal assent and on 1 April the first provisions came into force. The remainder of provisions, including the NZSIS becoming a government department, will come into force on 28 September. From that date, the NZSIS and GCSB will operate under that new single statute.

The Intelligence and Security Act replaces the four statutes that previously applied to the New Zealand Intelligence Community. We will now have a single, modern and cohesive statute. The Act contains:

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

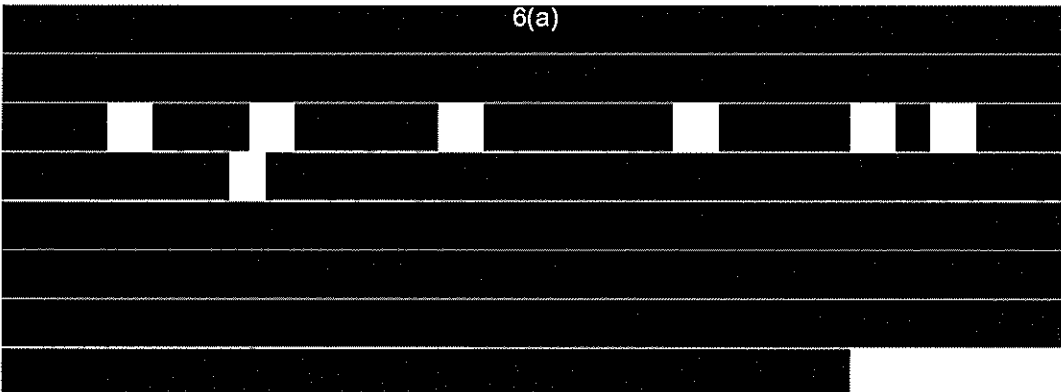
The Act allows GCSB and the NZSIS to work more closely together. Previously our different legislative frameworks created unnecessary confusion and complexity when conducting joint operational work.

We also believe in the importance of having working closely together with organisations across the Defence and Security sector. This leads me onto my fourth point.

My agency **works closely with both the Ministry of Defence and the New Zealand Defence Force** to either provide you with advice, seek your advice, or to work collaboratively on issues.

For example –

- **NZSIS provides protective security advice** through our Protective Security Requirements programme. This programme is publicly available through our website and is a standardise approach to protecting New Zealand’s people, systems, and premises. The impact of the Snowden leak has been felt across our community so we need to take all reasonable protection measures to ensure the classified information held by New Zealand isn’t part of an unauthorised leak either to the public or through espionage to our of foreign adversaries.

- 6(a)

We value our close working relationships very highly.

I hope I have given you a good sense of who the NZSIS is, what we do and how we work collaboratively with the GCSB and wider New Zealand Intelligence community.

I wish you the best for the rest of the day.

Keeping New Zealand and New Zealanders safe – the role and focus of the NZSIS

Presentation to Auckland University students and staff

Background

Date	14 June 2017
Location	Auckland University
Timing	Thirty minute presentation, 30 minutes of questions from the audience
Audience	25 students and staff (list will be supplied)
Topics	<ul style="list-style-type: none"> • The role of the NZSIS • The NZ threat picture in NZ with a focus on counter terrorism

Speaking notes

Thank you very much for the opportunity to deliver this guest lecture and to talk with you about the NZSIS and the important work that we do to keep New Zealand and New Zealanders secure.

As you can imagine there are aspects of our work that is classified as sharing it could compromise safety and security, or our ability to carry out our work.

My goal today is to be sufficiently interesting that you will be glad you came, but not so interesting that security is compromised. So, all the examples that I am using to illustrate my points are already publicly available.

I am happy to take questions at the end, but please forgive me if I am conservative about what I answer. I am sure that you understand.

I'd like to talk with you today about:

- Who the NZSIS is, the work that we do to make a difference for New Zealand and New Zealanders, and the legal framework we operate under that contributes to transparency and accountability, and

- The threat environment we operate in, with a specific focus on counter terrorism.
- I'll then open the floor up for questions.

So first of all, who is the NZSIS and how do we make a difference for New Zealand and New Zealanders?

The NZSIS is a civilian government agency. We aim to achieve three main outcomes:

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

To achieve those outcomes, we work alongside other agencies in the New Zealand Intelligence Community and with our international partners to maintain New Zealand's national security.

There are three main aspects to the NZSIS's work.

Security intelligence

Security intelligence consumes the greatest part of our resources. Our efforts in this area include identifying and providing advice on a number of different national security threats.

Generally threats fall into four categories:

- violent extremism,
- espionage conducted by state or non-state actors,
- the proliferation of weapons of mass-destruction, and
- hostile cyber activities.

The NZSIS works closely with other agencies like the New Zealand Police, and with international partners, to investigate individuals and groups who would harm New Zealand and New Zealanders.

The NZSIS's aim is to prevent security threats escalating to acts of violence here or off-shore, and to mitigate the threat of espionage activity in New Zealand or against New Zealand interests.

The NZSIS also works with other government agencies to identify potential visitors and people seeking residency or citizenship who may pose a risk to national security. As well as our own efforts to investigate these risks, we also provide advice to Immigration New Zealand and the New Zealand Customs Service to support their work to protect New Zealand's borders.

Foreign intelligence

The NZSIS's foreign intelligence activities largely focus on ensuring the security and stability of the Pacific. We do this by using information shared by individuals and other governments to identify people and states representing a threat to regional security.

The NZSIS sets out to discover what these actors are doing or intending to do, and what their hidden agendas might be in relation to New Zealand and our Pacific partners. Based on the intelligence we gather, the NZSIS provides advice to other government agencies such as the New Zealand Defence Force, the Ministry of Foreign Affairs and Trade, the New Zealand Police, or to our international partners.

Protective security advice

The NZSIS provides protective security advice to government. We do this by implementing and promoting the Protective Security Requirements, or PSR, across the public sector.

The PSR sets out the government's requirements for managing personnel, physical and information security. That includes providing formal guidelines and ongoing support to so that agencies can better manage business risks and assure continuity of service delivery. The NZSIS also conducts 'vetting' checks on individuals seeking security clearances within government, including for New Zealand Intelligence Community. That includes gathering information from police records,

travel information, interviews and other sources to determine, and make a recommendation about, a person's suitability to gain access to classified material.

Given the particular nature of the work that we do, our legal framework is really important, especially in ensuring we are as accountable and transparent as possible.

It is this legal framework that establishes the outcomes we need to deliver both as an agency and as a community, and the powers that we have to deliver these outcomes.

Originally formed in 1956, the New Zealand Security Service was only placed on a legislative footing in 1969. That Act, still in force, has been amended over time but had never been comprehensively reviewed.

On 28 March this year, the Intelligence and Security Act was passed with the first provisions coming into force on 1 April. The remainder of the provisions, including the NZSIS becoming a government department, will come into force later this year on 28 September.

The new legislation was developed as a result of the first Independent review of Intelligence and Security carried out by Dame Patsy Reddy and Sir Michael Cullen. The review, which began in 2015, reported back to the Intelligence and Security Committee in 2016 and recommended the new legislation. The review is a good primer to the Act, but also provides some useful context to intelligence, its uses, the New Zealand and international environment and how they influenced the recommendations. It is well worth reading.

A key objective of both the Intelligence and Security Review and the subsequent legislation was to ensure that the public would be better informed about the intelligence and security agencies work and their legal parameters. From my perspective, greater clarity and transparency in the law can only be a good thing, both for NZSIS and the public.

Another important element of the Act is that it enables closer working relationships across the New Zealand Intelligence Community and particularly between the NZSIS and the GCSB. For example, the new legislation creates a common set of purposes, objectives and functions for the NZSIS and GCSB.

I thought it might be helpful to outline these so you get a feel for the responsibilities of the NZSIS and the Intelligence Community and how these fit into the broad outcomes I talked about earlier.

The purpose of the new Act is to protect New Zealand as a free, open, and democratic society. The legislative mechanisms for this are:

(a) Establishing intelligence and security agencies that will effectively 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;

(b) Giving the intelligence and security agencies adequate and appropriate functions, powers, and duties;

(c) Ensuring that the functions of the intelligence and security agencies are performed -

- in accordance with New Zealand law and all human rights obligations recognised by New Zealand law;
- with integrity and professionalism; and
- in a manner that facilitates effective democratic oversight;

(d) Ensuring that the powers of the intelligence and security agencies are subject to institutional oversight and appropriate safeguards.

The NZSIS really welcomed the new legislation including the transparency it provides.

So, let's explore the work we do and threat environment we operate in a little more, focusing on counter terrorism.

New Zealand faces security threats just like any other country. Terrorism and the threat from violent extremism continue to be of very real concern and New Zealand is not immune. Counter-terrorism is therefore an important part of the work that the NZSIS and the wider New Zealand Intelligence Community does.

The international environment continues to evolve and while the threat from the so-called Islamic State, or Da'esh, remains a key focus for the NZSIS, al-Qaida and related extremist groups continue to be of concern. NZSIS needs to be in a position to have an understanding of the overall threat environment and, in particular, to be able to highlight any emerging threats.

Some key changes that have impacted on the New Zealand environment are:

- the increasingly sophisticated and pervasive social media presence of extremist groups, but in particular Da'esh and their ability to reach and influence individuals across the world;
- the nature of the messages from those types of groups. Those messages include encouraging individuals to travel to Syria or Iraq, and if that is not possible to commit attacks in their own countries; and
- the nature of attacks, which have become increasingly unsophisticated. For example, in recent months we have seen attacks committed overseas using vehicles and knives.

The NZSIS and the GCSB collect intelligence related to terrorist activity and, through our links with overseas security and intelligence organisations, monitor movements of known terrorists around the world.

The strategic aim of New Zealand's counter-terrorism effort is that New Zealand is neither the victim nor the source of an act of terrorism, and

that New Zealand plays an appropriate role in international efforts to combat terrorism.

This means NZSIS has a focus not only on the threat within New Zealand but also the wider international context. One way in which we do this is by preventing “wannabe terrorists” from travelling to the Middle East.

We also need to do our best to assure the protection of New Zealanders who are deployed overseas, for example police, military, and foreign affairs. And we have a role in mitigating the risk posed to overseas locations or events where New Zealanders are likely to gather.

A key way we approach this is through the Combined Threat Assessment Group, known as CTAG. CTAG is an independent, inter-agency group located in NZSIS. It assesses terrorist threats of physical harm to New Zealanders and New Zealand interests. CTAG ensures that assessment advice about threats is reported to the appropriate domestic and international partners in an accurate, timely and relevant way, so risk can be mitigated.

While the threat level in New Zealand is low, there are individuals and groups with links to overseas organisations that are committed to acts of terrorism, violence and intimidation. This includes a small number of New Zealanders who remain in ISIL-occupied parts of the Middle East. There are also home-grown and self-radicalised individuals and groups. I have a few examples for you.

I'll start with a couple of examples that demonstrate how we work to secure New Zealand from threats.

- ***Example one***

In 2015, NZSIS identified a foreign citizen on an international watch list attempting to travel to New Zealand. NZSIS advised Immigration New Zealand who made further enquiries about the person and found he had served a prison sentence overseas for terrorism-related charges. Immigration New Zealand did not allow the person to board their flight to New Zealand as their convictions meant they did not meet the Immigration Act character requirements. The information provided by NZSIS enabled Immigration New Zealand to make an informed decision and manage the risk to New Zealand while the individual was still overseas.

- ***Example two***

A foreign citizen in New Zealand was identified as being directly associated with people responsible for a terrorist attack overseas. The person had entered New Zealand under a variation of his name. NZSIS decided the person was a threat to New Zealand's national security because of that and their activities since arriving in New Zealand, and the person was deported for security reasons.

We also contribute to international efforts to combat terrorism. We do this by collecting intelligence about terrorist activity and monitor, as far as we can, the movements of known terrorists around the world. I have a few examples of how we go about doing that.

- **Example three**

A New Zealand citizen based offshore had their passport cancelled by the Minister of Internal Affairs. This followed a classified briefing by NZSIS indicating the individual sought help from a jihadi facilitation network to enter Syria and engage in militant jihad alongside a terrorist group. The New Zealander was subsequently arrested and convicted by foreign authorities on terrorism charges.

- **Example four**

NZSIS identified a New Zealander who was in contact with someone in a European country. The two had discussed plans to meet in a third country in order to travel and participate in militant jihad. NZSIS shared this intelligence with the intelligence service of the European country. That country started their own investigation and discovered the European-based individual had obtained items that could be used to make explosives. The person was arrested and charged with terrorism offences.

- **Example five**

6(a)
[REDACTED]

So those are a few examples of how what we do makes a difference in terms of counter-terrorism.

I hope I have given you a good sense of who we are and the work that we do, and the checks and balances that are in place around that work.

Before I open up the floor to questions I want to thank you for inviting me here to speak with you today.

The NZSIS has not always had a very visible public presence. While the NZSIS handles secret information, we need not be a secret organisation. New Zealanders rightly feel they have a stake in the discourse on national security. And as I have already said, greater clarity and transparency is a really good thing, both for NZSIS and the public.

This presentation, and presentations like it, is all part of helping to tell the story of what we do and the contribution that we make to New Zealand.

Thank you.

Acting Director-General's speech

To new Ministry of Defence staff

Friday 23 February 2018: 1000 – 1100

Main themes:

- Introduction on NZIC and NZSIS – roles and functions
 - The threats facing New Zealand
 - Working with partners
 - Case study of NZSIS activities
-

I am very pleased to be invited to speak to you all today. I see this as a great opportunity to increase your understanding about - the New Zealand Security Intelligence Service - and the ways in which we work with our partners, including the Defence sector.

The organisations in the Defence and the security and intelligence sectors are essential parts of keeping New Zealand and New Zealanders safe.

To do our jobs effectively and keep New Zealand safe, we need to be working together. New Zealand is too small, and our job is too important to be un-coordinated or focusing our efforts in different places.

I would like to discuss four things with you today:

- Introduction on NZIC and NZSIS – roles and functions
- The threats facing New Zealand
- Working with partners
- Case study of NZSIS activities

No powerpoints! Just me! I'm planning on holding your interest for the next 30 minutes or so.

The New Zealand Intelligence Community

The core New Zealand Intelligence Community (NZIC) is made up of NZSIS, GCSB and the National Assessments Bureau (NAB), which is a part of DPMC (SIG). First sentence – 6 acronyms! Welcome to the NZIC! We are all co-located in Pipitea House.

Our three agencies work together (consistent with legal parameters) to more effectively meet the government's security and intelligence priorities.

Collectively we have a vision of an agile, coordinated and customer focused community that can sustainably meet the Government's security and intelligence priorities.

We also work with other intelligence partners wherever we need to – this includes NZDF, as well as civilian organisations like Customs, Immigration New Zealand, Department of Internal Affairs and Police.

In addition to providing joined up, co-ordinated advice to Ministers, NZIC works together on major projects.

This includes:

- Making sure that all three agencies are making the best use of the extra resources the Government allocated to security and intelligence in 2016. This is essentially our joint budgets for building capacity and our growth path over a 4 year period.
- Implementation of the Intelligence and Security Act 2017 – a major legal overhaul that gives a single piece of legislation for

intelligence and security. This was fantastic for our agency, but implementation is a big job.

As I mentioned, all three organisations are based together in Pipitea House and we are constantly working to integrate, align and streamline what we do so we can be as effective and efficient as we can. The Senior Teams meet together three times a week so this helps set the tone of collaboration. We also have shared corporate arrangements that support both organisations i.e. finance; HR; comms; International Engagement; and strategy, performance, policy teams.

The ultimate aim is to keep New Zealand safe and get the most benefit out of every dollar we have in our funding.

So who are we and what do we do?

The New Zealand Security Intelligence Service exists to protect New Zealand's National Security, international relations and reputation of New Zealand, and the economic wellbeing of New Zealand.

NZSIS's vision is to be *ahead of the curve: providing indispensable security and intelligence services underpinned by high public confidence and trust.*

Everything we do is governed by the Intelligence and Security Act and is in alignment with the National Intelligence Priorities.

As an organisation we have three primary outcomes we seek to achieve on behalf of New Zealand and New Zealanders :

New Zealanders Are Safer

We identify, and provide advice to other agencies about countering, a number of threats including: terrorism and violent extremism, espionage conducted by other states and the proliferation of weapons of mass-destruction. We work with other agencies, such as the Police, to prevent threats to security progressing to acts of violence or espionage.

We work closely with partners such as the Department of Internal Affairs and Immigration New Zealand to screen people visiting our country who may present a security risk, or seeking residency or citizenship who may pose a risk to national security.

We also help protect Government officials and representatives posted overseas or attending events and conferences. Overseas postings or trips like this can expose New Zealanders to security risks like terrorist attack or espionage.

This extends to supporting NZDF operations, mostly through force protection and keeping deployed New Zealanders safe and secure overseas.

Secondly, Key institutions are protected

Through the Protective Security Requirements (PSR) we help agencies to meet the Government's expectations of the public sector for

managing personnel, physical and information security and support agencies to better manage risks.

We also vet people seeking security clearances to ensure they are trustworthy given the range of classified material they will see in their roles. We do this by interviewing them, checking information they provide about themselves and by contacting referees.

Each of you will have been through this process.

How was it for you?

Out third outcome..... National advantage is promoted

We work to identify people or states which threaten our regional security, work out what they are doing or intending to do, and what their true agenda towards New Zealand or our partners might be.

Based on the intelligence we gather, we provide advice to other government agencies such as the NZDF or the Ministry of Foreign Affairs and Trade or (where appropriate) to international partners.

Robust Oversight

We have some quite intrusive powers and, by necessity, most of what we do is not seen by the public.

To give New Zealanders confidence that what we are acting legally and in the interests of New Zealanders we are subject to robust oversight.

This includes:

- Strong internal checks and controls. *(Compliance Framework underpinned by policies, SOPs, training, audit processes)*
- Intelligence can only be gathered in accordance with a warrant. Every warrant must be approved by the Minister responsible for

the NZSIS, Minister Little and a Commissioner of Warrants – an independent statutory office holder.

- The current Chief Commissioner of Warrants is Sir Bruce Roberston
- The Inspector-General of Intelligence and Security – an independent statutory office holder who has the power to review the legality of our activities, undertake inquiries and review complaints from the public. The OIGIS has right of access to NZSIS staff, premises and records to carry out their functions.
 - The current IGIS is Cheryl Gwyn
- The Intelligence and Security Committee, a Parliamentary oversight committee for the Intelligence agencies. Our annual review by the ISC is coming up in March, this includes a section that is open and a classified section that is behind closed doors.

Human Intelligence

More about who we are and what we do.

We are a Human Intelligence agency – HUMINT in the sector jargon, as opposed to COMINT – which is Communications Intelligence and SIGINT – which is Signals Intelligence.

In simple terms we gather intelligence from people.

This could involve:

- Working with the community
- Getting people to tell us things or give us access to information or documents
- Surveillance – watching what people do and who they meet with
- Screening and spotting individuals of security concern

Threats to New Zealand

We are fortunate that New Zealand is a safe country – especially relative to many parts of the world. This is what we are here to protect. That does not mean that we don't face threats.

The environment and 'threatscape' is not benign.

Constantly evolving and advancing technology and faster, easier international travel are very beneficial to our country, but they also present challenges for security.

Terrorism:

ISIL remains a threat despite the loss of most of its territory. While it has lost most of its territory – its supporters are still around and are still trying to influence people to commit violent acts.

There is a watch list of around 30-40 individuals. Individuals come on and off that list depending on their activities.

Espionage

Other countries try to find out information we don't want them to have.

This can target government agencies, New Zealand businesses or individuals.

Cyber Attack

This is online attacks designed to disrupt computer systems.

These acts may be carried out by foreign governments, state sponsored actors, private sector companies or individuals.

The Director-General of the GCSB recently joined international condemnation of Russia over the NotPetya cyber attack that caused

wide spread damage and disruption to computer systems around the world in June 2017.

Proliferation of Weapons of Mass Destruction:

This could include New Zealanders unwittingly supplying highly sensitive technology, materials or equipment to a foreign WMD development programme.

Regional instability

Political and social disorder in a Pacific state or across the region could threaten the security of the region and impact on New Zealand's interests.

This could include a political crisis, such as a coup, that could create tension between states in the region, including New Zealand.

Arrival:

An individual (or group) who might be of national security concern (particularly terrorism) could present at the border and requires an immigration decision about eligibility to enter New Zealand

What do we do about threats?

So when a threat is identified, what then?

If you are thinking helicopters, fast cars and explosions – I have to disappoint you!

NZSIS is not a law enforcement agency, we don't take action ourselves. We provide information to other organisations for them to take action where they need to.

Partnerships

We have extensive engagement with Police, NZDF, Customs, Ministry of Primary Industries Immigration and other agencies that includes

two-way sharing of intelligence, direct support for operational activities, and the sharing of capabilities and training.

The 5-Eyes partnership comprising our “allies” post-World War II is our most significant intelligence relationship. We also work with overseas partners.

We also provide advice to a range of other organisations on matters of security, including: providing protective security advice and security screening services to government, advising officials about the risks with being posted overseas and providing advice to other agencies about national security.

So how does it actually work?

To give you a sense of NZSIS' role and help you understand how it works, I'm going to briefly take you through the process around a counter-terrorism investigation.

I'll be illustrating that with a case study.

To avoid compromising any actual operations or people, this is realistic but doesn't actually relate to a real investigation.

Step 1: The initial lead

The NZSIS is notified of a new threat.

The source could be a foreign liaison partner, a member of the public could come in through a walk-in, our telephone line, email, through a government department or even a previous investigation.

The lead is assessed for reliability and priority before it is referred to an Intelligence Officer.

Case study

A trusted foreign liaison partner tells NZSIS that:

- a Syria-based individual called Dave, who has a kiwi accent, has been in contact with a facilitator for ISIL and has been living in an ISIL camp
- Dave is seeking to travel to New Zealand “at the direction of the ISIL leadership”, and
- Dave has a New Zealand mobile number, which is not being used in Syria.

The Intelligence Officer must consider what this information means for New Zealand.

Does Dave intend to undertake activities that could impact New Zealand’s security?

Step 2: Initial enquiries

The Intelligence Officer decides the initial investigative steps.

They must consider the necessity and proportionality, legality and propriety of every step before it is taken.

If initial enquiries show there is no threat, the investigation will be discontinued.

If further investigation is required, the Intelligence Officer will talk to a manager about the next steps.

Case study

6(a) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

After Dave returns to New Zealand, further enquiries indicate that he is in regular contact with John, a New Zealand citizen known to NZSIS.

John has previously expressed interest in extremist ideology and is assessed as very susceptible to radicalisation.

This may indicate that Dave is recruiting others, such as John, to join ISIL or even attempt to harm people in New Zealand.

Step 3: Intelligence collection

(a) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

Case study:

6(a) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

6(a)

The text '6(a)' is followed by three large black rectangular redaction boxes covering the majority of the page's content.

Based on this information and what is already known, the Intelligence Officer assesses that Dave may be seeking to encourage or direct John to travel to Syria and join ISIL.

Step 4: Warrant application if required

If more intrusive investigative activities are required, such as intercepting a person's communications, the Intelligence Officer will begin an application for a warrant.

Managers and legal staff will review the proposal before the application is submitted for external approval in accordance with legislation.

Case study

The Intelligence Officer determines that further information is required ^{6(a)} [REDACTED]

[REDACTED]

The Intelligence Officer and their manager decide it is necessary and proportionate to seek a warrant on both Dave and John for this purpose.

Both Dave and John are New Zealanders so a Type 1 intelligence warrant is required under the Intelligence and Security Act 2017.

After a rigorous internal process, the application is presented to the Minister responsible for the NZSIS and a Commissioner of Intelligence Warrants.

The warrant is approved and NZSIS begins exercising its warranted power ^{6(a)} [REDACTED]

(b) (7)(C) [Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(C) [Redacted]

[Redacted]

Step 5: Assessment and action

Once all the necessary collection has been undertaken, the Intelligence Officer will determine what risk a particular individual poses.

If the person does not pose a threat, the investigation is concluded.

If a threat is posed, NZSIS will send a report to political decision-makers and/or an enforcement agency, such as the New Zealand Police.

Case study

The Intelligence Officer is now highly confident in their assessment that Dave and John intend to travel to Syria imminently to join ISIL.

This poses risks to New Zealand since Dave and John may commit terrorist acts overseas and/or may return to New Zealand and commit terrorist acts.

The Intelligence Officer and their managers determine it is necessary to issue formal advice to relevant officials and partner agencies to mitigate the threat posed by Dave and John, including advice recommending the cancellation of Dave and John's passports to prevent them travelling to Syria and joining ISIL.

This is not the end of the investigation

6(a) [Redacted]

[Redacted]

[Redacted]

[Redacted]

This may lead to further investigation.

So, in closing, like all organisations we have a range of suitably qualified and experienced people performing a range of roles.

We collect and analyse intelligence in accordance with the Government's National Intelligence Priorities. Much of our work is done in secret and therefore, our robust oversight arrangements help give New Zealanders confidence that we conduct our activities lawfully and in the interest of New Zealanders.



Speech: NZDF Staff College Director-General of the GCSB Friday 1 June 2018, 0900-0930, ^{6(a)} PHOP

Introduction

[Andrew]

Good morning. I'm Andrew Hampton the Director-General of the GCSB and this is Rebecca Kitteridge the Director-General of Security at the NZSIS.

We've got about 30 minutes with you this morning to talk on Building Trust and Confidence. We thought we would talk for around 20 minutes about the journey both of the agencies have been on, and how that journey has helped build public trust and confidence in the agencies as well as brought us to be much closer at both an operational and organisational level. Followed by questions.

I think it's fair to say that the New Zealand Intelligence Community has recently completed a period of significant change and growth.

New Zealand is an open country in a globalised world. This benefits us significantly and is reflected in our values, institutions and economy.

As is the often the case, these benefits and opportunities come with risks and threats.

The role of the NZSIS

[Rebecca]

So what does the NZSIS actually do? Like the GCSB we collect, access and report on intelligence in accordance with priorities set by the Government and in the line with New Zealand’s laws and its human rights obligations.

While the GCSB is focused on electronic communications, the Service is focused on HUMIT. We also provide protective services including security vetting for all of government and personnel security advice.

Threatscape: Espionage

[Rebecca]

We are vigilant against foreign interference intended to undermine New Zealand’s national interests.

This is not new, but we are concerned by the increasing scope and scale of foreign interference activity.

6(a) [Redacted text block]

Threatscape: Terrorism

The counter-terrorism environment in New Zealand is still dominated by the influence of ISIL.

At any one time between 30 and 40 people are listed on the NZSIS's counter-terrorism risk register. These individuals are assessed to represent an actual or potential threat to New Zealand related to terrorism.

Looking ahead, New Zealand is concerned about the effect of retuning foreign fighters and regional security more broadly should ISIL's attention turn to South East Asia.

The role of the GCSB

[Andrew]

The GCSB is a SIGINT or signals intelligence agencies meaning we specialise in intelligence derived from electronic communications. We also have a statutory role in cyber security and information assurance.

Threatscape: Cyber

New Zealand's cyber threat environment is increasingly complex.

A key way that the GCSB protects organisations of national significance is through a system we call CORTEX. It's focused on detecting and disrupting complex and persistent foreign-sourced malware that is typically beyond the capabilities of commercial available tools.

In November 2017 the GCSB released its second unclassified cyber threat summary. It found of the 396 serious incidents recorded nearly a third had indicators of connection to foreign intelligence agencies.

New Zealand organisations are subject to both direct and indirect threats, and are being used as staging points by threat actors to target systems in other countries.

Motivation varies from espionage to revenue generation and seeking to secure political outcomes.

Cyber-attacks are relatively cheap and effective, and to date the implications of getting caught have not been great.

In February I added New Zealand's voice to the international condemnation of the NotPetya cyber-attack which international partners have now attributed to the Russian Government. It targeted the Ukraine but also had a global impact.

In December I also joined international partners to express concern about the international reports which link North Korea to the major WannaCry ransomware campaign.

While New Zealand was not significantly impacted by NotPetya or WannaCry, we are not immune from this type of threat. That's why it's important that like minded countries continue to publicly condemn reckless and malicious activity.

The journey we have been on

[Rebecca]

To respond to this threatscape and to overcome the impediments of our size and spread, we are transforming how we operate as an intelligence community.

The theme of Building Trust and Confidence is appropriate when reflecting on the journey of change the agencies has been on.

For me this journey started in 2012 when I was to carry out an independent review of the GCSB's compliance.

The Kitteridge Report found that there were long-standing, systemic problems with the GCSB's compliance systems and aspects of its organisation and culture. It also highlighted the need for the GCSB to have a clear legal framework to operate within.

The report was always written with the intention of releasing it publicly. The public release was brought forward by a week or so following an unauthorised disclosure.

Not surprisingly, there was wall to wall media coverage and debates in Parliament on both the unauthorised disclosure and the content of the report.

It was not only an incredibly tough time for the incredible staff here at the GCSB, but it also had a wider impact on the trust and confidence in the New Zealand intelligence agencies as a whole.

It was a result of my experience working with the GCSB I was motivated to apply for the top job at the Service a year later.

Soon after arriving at the Service I kicked off a review similar to the one I had carried out at the GCSB. Not surprisingly I found similar issues at the Service and it was clear that a huge amount of work was needed to turn things around.

It's around this point that the journey of change for both of the agencies really kicked up a gear.

To maintain public trust and confidence, as much as to maintain the social license to function, we have to strike the balance very carefully when it comes to our security and intelligence agencies.

To briefly summarise some of the key changes:

- The agencies were subject to a couple of reviews, including the Independent Review of Intelligence and Security in New Zealand and our Strategy Capability and Resourcing Review;
- As part of the New Zealand Government's 2016 Budget, we again received significant new funding and we are investing in both people also capabilities;
- Our agencies are growing at pace - for example, the NZSIS is doubling in size over the six year period from 2014 to 2020; and
- Since last year, the NZSIS and GCSB have been operating under a new single statute - the Intelligence and Security Act 2017.

The new era

[Andrew]

For us the new legislation is incredibly important. I'm very strong believer in following not only the letter but also the spirit of the law and we needed a much cleared legal framework to operate within.

The Intelligence and Security Act replaces the four statutes that previously applied to the New Zealand Intelligence Community. We now have a single, modern and cohesive statute. The Act contains:

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

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

The legislative changes will not have an impact on existing information-sharing arrangements with Five Eyes partners. The Act does, however introduce a more explicit requirement for our Minister to take into account human rights considerations when authorising our agencies to share information with partners.

All of the changes we have outlined – to our funding and legislation – have been underpinned by significant efforts by Ministers and the leadership of both of our agencies to be more open and transparent – and to build public awareness of New Zealand's threatscape – particularly on cyber and terrorism matters.

Indications are that this approach is working; the Intelligence and Security Act passed through Parliament with near unanimous support. Unlike five years ago, New Zealand's Intelligence agencies are not the focus of negative media attention and polling indicates public perception of our agencies and awareness of the threatscape are lifting.

Building joint capability

[Rebecca]

The New Zealand Government's investment in our community is based on delivery of clear community-wide outcomes - not on individual agencies continuing to do what they have always done.

To improve how GCSB and NZSIS work together as a community, we have:

- A shared Four Year Plan – a platform for aligning strategic intent and prioritising resources towards common goals;
- A Joint Leadership Team, with senior representatives from both agencies to govern shared work programmes including work to improve the value our customers receive from intelligence products;
- Joint workforce planning based on common remuneration, job families and a shared recruitment campaign; and
- Shared security, finance, human resources and facilities services.

We also established a Joint Office of the Director's-General and are reviewing ICT enablement with a view to determining the benefits of a joint – or at least more closely aligned ICT function.

All of these changes set us up to deliver – both in terms of the New Zealand Government's very clear intelligence requirements - and our ability to contribute to the Five Eyes partnership.

Our focus is now on growing as quickly and as safely as possible.

Our emphasis as a community over the next couple of years is on:

- continuing to build capability in the areas of collection, cyber defence, and investing in information management technology;
- recruiting, developing, and retaining the best and brightest people;
- ensuring we embed and capitalise on the opportunities our new legislative framework has created for us – for example allowing the NZSIS and GCSB to work more closely together on national security issues.

Translating change into trust and confidence

[Andrew]

Ensuring the agencies have the right mechanism in place to ensure that they are lawful and compliant has been incredibly important in building trust and confidence.

I'm pleased to say that for three years in the row the Inspector-General of Security Intelligence has found the GCSB's systems and processes to be fully compliant and that our staff have a strong culture of legal compliance.

In recent years Rebecca and I have been actively pushing our agencies towards greater transparency and openness where possible.

Where we can we're keen to release official documents to increase the public understanding of what we do and why we need to do it.

For example, our recent unclassified Annual Reports included more information than ever before; our joint Briefing to the Incoming Minister was released with a small number of reductions; and I believe our responses to Official Information Requests have greatly improved.

Being able to engage more with the public about the risks New Zealand is facing, and the role the Service and the GCSB has in mitigating those risks is fundamental to building trust and confidence.

Rebecca and I are also engaging with the public more than ever before. An area we're actively pushing the boat out is around our promoting the unique career paths the agencies offer.

For example, the GCSB has been championing the need to encourage more women into science, math, engineering and technology background into techy care paths. We're doing this through our Women in STEM tertiary scholarship programme. This scholarship has enabled me to speak at Universities around the country and a wide variety of media outlets.

The Service in the last few weeks had an active Surveillance Officer interviewed about their role to kick off a recruitment campaign for SOs.

Closing Remarks

[Rebecca]

As we've outlined the agencies have been through a massive journey in recent years.

It has been a busy time, we remain resolutely focused on delivering against the priorities set for us by the government while continuing to build on the public trust and confidence and maintain our social license to function.

Thank you.



Speech: 6(a)
2019

Introduction

[Andrew]

Hi everyone. I'm Andrew Hampton the Director-General of the GCSB and with me today is the Deputy Director-General of the NZSIS, 6(a), 9(2)(a), 18(c)(i).

We've got some time this afternoon to talk about the approach our intelligence agencies have taken to **Building Trust and Confidence**. This is a key enabler for us to be able to successfully deliver the positive security outcomes for Zealanders we are mandated to.

The New Zealand Intelligence Community has been through a significant period of change and growth. To provide some context for this, we will briefly talk about our roles, the threats we work to counter and the journey we've been on to modernise our agencies in order to increase our capabilities and build public trust and confidence.

Though geographically remote, New Zealand is an open country in an increasingly globalised world. This benefits us significantly and is reflected in our values, institutions and economy. But these benefits and opportunities equally come with risks and threats.

In the light of the dreadful events in Christchurch, the conversation about public trust and confidence is one that is perhaps more important than before.

The Christchurch terrorist attacks were an unexpected display of violent extremism completely at odds with the values of tolerance and openness that define New Zealand. To see New Zealanders rally in support of our Muslim communities in the way they have has made me so proud of our country.

In the days ahead following the attack, media and the public were asking hard questions of New Zealand's Intelligence Community and other domestic agencies – and rightly so! We were asking these questions of ourselves.

The condolence messages and offers of support we received from partner agencies overseas – many who have experienced an attack like this in their homeland –was comforting. Our Australian counterparts immediately offered resources, shared information and would end up sending people to work with our teams, who were operating at a heightened tempo. We are really grateful to have such supportive partnerships.

In the immediate aftermath of the attacks like the NZSIS and GCSB stood up a 24 hour operation.

As primarily a foreign intelligence and cyber security agency, the GCSB's role was to support the investigative efforts as required primarily our technical capabilities and pass on any relevant intelligence received from foreign partners to NZ Police and the NZSIS.

As the domestic intelligence agency, the NZSIS had a lead role in the investigation. I'll now hand over to 6(a), 9(2) for more on NZSIS's response to the attacks.

NZSIS role in response to the Christchurch attacks

6(a), 9(2)(a),

Like the general public, the NZIC was also shocked by the Christchurch mosque attacks. New Zealand has had a LOW national threat level for a long time; whereby the threat of an attack was always possible but not expected.

We were asking the same questions the New Zealand public were asking, "How could this happen? Could it have been stopped? Did anybody know about the attacker?"

While these questions are difficult, they present us with an opportunity to learn. A Royal Commission of Inquiry into the attacks is now underway and we welcome any recommendations that may come out of it. If there are things we can change to prevent this tragedy from happening again, we are certainly open to them. Such independent scrutiny matters hugely to agencies like ours and GCSB because we depend on public confidence, understanding and democratically sanctioned legal authority to do our work.

So, in the immediate aftermath of the attacks the NZSIS went into full-scale response mode. Our investigation broadly covered three areas:

- First, getting a complete picture of the alleged attacker, finding out everything possible about him and his plans, with an immediate focus on whether he was part of a group and whether any other attacks were planned.
- Second, reviewing everything we knew about extreme right-wing groups in New Zealand, to detect any potential "copycat attacks" inspired by the Christchurch attacks.
- And third, detecting any suggestions of a revenge attack either in New Zealand or against New Zealand interests offshore – and you may recall that ISIS quickly called for such revenge attacks.

In each of these areas we have worked closely with our Police colleagues, GCSB as well as foreign intelligence partners- partly because the alleged attacker was an Australian who had travelled widely before the attacks and partly because of the possibility of copycat or revenge attacks is an international issue.

The Christchurch attacks also prompted many New Zealanders to report concerns about people who had expressed racist, Nazi, identitarian, or white

supremacist views. In the days following the attacks the NZSIS received hundreds of calls and messages, as did Police. Each call was a lead that needed to be investigated and triaged into high, medium or low priority depending on the information to hand – a very challenging task given the level of public alarm and vague nature of much of the information provided.

In the public sphere, there was a demand for information about what NZSIS knew or did not know about the alleged attacker, and what work we had been doing in the area of violent right wing extremism before the attacks.

Releasing even a small amount of information was an important part of being open with the public. Where there is a void in information being provided, that space can quickly be filled with inaccurate speculations and judgements about the intelligence agencies. We have equally seen a lot of this in the last few weeks which has been challenging for our community.

We released some basic information – that the alleged attacker was not known as a person of national security concern to us, or to NZ Police, or our Australian counterparts; and that NZSIS had been looking specifically at violent right wing extremism for about nine months before the attacks. Though it didn't seem like much, but given the circumstances the fact that we were even acknowledging what we did or didn't know is more than we would have usually spoken about publicly.

Terrorism and Violent extremism

The Christchurch attacks were a realisation of the threats we work to counter. The NZSIS is concerned by all extremist behaviour which incites violence to advance their ideology.

At any one time around 30 people are of particular interest to the NZSIS. These individuals are assessed to represent an actual or potential threat to New Zealand. The number fluctuates over time. As investigations into individuals of interest are resolved or their activities of concern diminish, other individuals of interest may emerge – as a result this number is not static.

ISIL remains the main global terrorist actor. Although the physical caliphate has significantly diminished, intelligence shows that ISIL continues to exert its extreme ideologies online. And as Andrew alluded to earlier, in the online space geographical dispersion does little to stop such ideologies spreading.

The role of the NZSIS

6(a), 9(2)(a),

So moving on to the role of NZSIS. what does the NZSIS do? The NZSIS is a human intelligence or HUMINT agency which means we use the human interest angle and relationships to meet our intelligence requirements. We collect, investigate and report on issues relating to New Zealand's national security- Counter terrorism, espionage, foreign interference and regional stability.

We undertake our role in accordance with priorities set by our Government and in the line with New Zealand's laws and its human rights obligations.

We also provide protective security services, advice and assistance to government with the goal of lifting the overall security culture and capability across government.

And we are responsible for security clearance vetting across government.

6(a)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

And partnerships are important because of the complex threat environment we are all operating in. In this highly globalized world, no one agency has all the answer and cooperation is the only way in which we can counter these threats.

Threatscape: Foreign Interference

In addition to countering violent extremism, the NZSIS is vigilant against the threat of foreign interference intended to undermine New Zealand's national interests. Espionage is an age old trade craft.

There is a difference between legitimate foreign influence and foreign interference. We are concerned by the increasing scope and scale of foreign interference activity in which state actors are purposely misleading, covert and deceptive in their activities. This kind of activity presents the greatest risk to New Zealand's democratic and economic institutions.

6(a) [REDACTED]

We undertake a wide range of investigative effort to counter foreign interference threats. We also play an important role in helping the New Zealand government and some private businesses protect themselves against the risk of foreign interference.

The role of the GCSB
[Andrew]

The intelligence agencies exist to protect New Zealand as a free, open and democratic society. The GCSB is a SIGINT or signals intelligence agencies meaning we specialise in intelligence derived from electronic communications. We also have a statutory role in cyber security an information assurance.

Like the NZSIS, everything the GCSB does needs to be in accordance with the objectives in the Intelligence and Security Act 2017, New Zealand’s human rights obligations and guided by our Government’s priorities.

6(a) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Monitoring the internet

In the aftermath of the Christchurch attacks, I was intrigued by a sentiment the public expressed, that the GCSB/NZSIS does or should monitor all internet traffic – which is of course not true.

We do not have the legal authority, technical means, resourcing, or the social license to monitor all of the country’s internet activity. This would also require an access programme to enable the bulk collection of internet traffic entering and leaving the country and New Zealand does not have such an access programme.

Increasingly internet traffic is encrypted or involves closed chat rooms, which means activity would not necessarily be easily detected. And in any case, all investigations need to start with a substantive lead, or compelling hypothesis. This is not a problem unique to New Zealand. Law enforcement and security intelligence agencies around the world are dealing with the extreme challenges encryption present.

Threatscape: Cyber
[Andrew]

New Zealand's cyber threat environment like most is complex.

New Zealand organisations are subject to both direct and indirect threats, and are being used as staging points by threat actors to target systems in other countries.

Motivation varies from espionage to revenue generation and seeking to secure political outcomes.

Cyber-attacks are relatively cheap and effective, and to date the implications of getting caught have not been great.

Last year, our Cyber Threat Report, recorded 347 cyber security incidents, of these 134 or 39% had indicators of connection to state-sponsored cyber actors.

A key way that the GCSB protects organisations of national significant is through a system we call CORTEX. It's focused on detecting and disrupting complex and persistent foreign-sourced malware that is typically beyond the capabilities of commercial available tools.

Over the last 18 months I have added New Zealand's voice to the international condemnation of cyber campaigns with clear links to state-sponsored actors. These have included:

- NotPetya - attributed to the Russian Government. It targeted the Ukraine but also had a global impact.
- WannaCry ransomware campaign linked to North Korea
- Last year a campaign of cyber-enabled intellectual property theft was attributed to China.

It's important that like minded countries continue to publicly condemn reckless and malicious activity.

Huawei - 5G

The last thing for me to mention is GCSB's regulatory function under TICSA. There has been considerable public focus on the GCSB's regulatory roles recently – in particular in relation to the country's telecommunications network.

GCSB is responsible for administering the network security provisions of the TICSA. Through TICSA, we engage with network operators to identify and mitigate potential risks to national security.

The TICSA applies a country and vendor agnostic framework. It requires the GCSB to make an independent assessment of potential network security risks, on a case-by-case basis.

Since TICSA came into effect in 2014, the GCSB has received several hundred notifications from network operators. For example, in the last financial year the GCSB received 123 notifications from network operators.

There was and continues to be plenty of interest in the media surrounding the first 5G notification which we received from Spark. Our assessment of their proposal uncovered some significant security risks and so we subsequently declined. There have been speculations about whether Five-Eyes partners had coerced me into refusing the notification - this is not the case. Our TICSA process is completely independent.

The ball is now in Spark's court to mitigate the risks we found or submit a new proposal for their 5G network.

The new era

[Andrew]

To respond to this changing threatscape, we have been on a journey of change to transform how we operate as an intelligence community which has been made possible by significant investment from the Government in 2016.

This change was spurred on by the independent reviews of both the GCSB and the NZSIS which found long-standing systematic problems with its compliance systems and organizational culture.

The reviews also highlighted the need for there to be a clear framework to operate in. For us the new legislation has been a much needed and clearer legal framework to operate within.

The Intelligence and Security Act replaces the four statutes that previously applied to the New Zealand Intelligence Community. We now have a single, modern and cohesive statute. The Act contains:

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

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

The legislative changes will not have an impact on existing information-sharing arrangements with Five Eyes partners. The Act does, however introduce a more explicit requirement for our Minister to take into account human rights considerations when authorising our agencies to share information with partners.

All of these changes we have outlined have been underpinned by significant efforts by Ministers and the leadership of both of our agencies to be more open and transparent – and to build public awareness of New Zealand's threatscape – particularly on cyber and terrorism matters.

Indications so far are that this approach is working.

Building joint capability

6(a), 9(2)(a),
18(c)(i)

The New Zealand Government's investment in our community is based on delivery of clear community-wide outcomes - not on individual agencies continuing to do what they have always done.

To improve how GCSB and NZSIS work together as a community, we have:

- A shared Four Year Plan – a platform for aligning strategic intent and prioritising resources towards common goals;
- A Joint Leadership Team, with senior representatives from both agencies to govern shared work programmes including work to improve the value our customers receive from intelligence products;
- Joint workforce planning based on common remuneration, job families and a shared recruitment campaign; and
- Shared security, finance, human resources and facilities services.

We also established a Joint Office of the Director's-General comprising strategy and policy, international engagement and communications. And our most recent shared enabling function is the joint IT Directorate.

All of these changes set us up to deliver – both in terms of the New Zealand Government's very clear intelligence requirements - and our ability to contribute to the Five Eyes partnership.

With increased government investment our focus has been on growing as quickly and as safely as possible. We are now heading into the 4th year of this increased funding.

Our emphasis as a community over the next couple of years is therefore on:

- continuing to build capability in the areas of collection, cyber defence, and investing in information management technology;
- recruiting, developing, and retaining the best and brightest people;
- And with this we have a specific focus on Diversity and Inclusion. It is really important in winning the public's trust and confidence that we reflect the community we serve. NZSIS and GCSB have a joint Diversity and Inclusion strategy with clear goals for the next two years.

- For example, the GCSB has been championing the need to encourage more women into science, math, engineering and technology background into techy care paths, through the Women in STEM tertiary scholarship programme. NZSIS will launch its scholarship programme in the coming year.
- ensuring we embed and capitalise on the opportunities our new legislative framework has created for us – for example allowing the NZSIS and GCSB to work more closely together on national security issues under a joint warrant.
- Importantly, as the Royal Commission of Inquiry seeks to deliver its Report by year end, a key focus for us will be addressing the learnings, findings and recommendations and ensuring both agencies continue to strengthen to deliver positive security outcomes for all New Zealanders.

Translating change into trust and confidence

[Andrew]

Ensuring the agencies have the right mechanism in place to ensure that they are lawful and compliant has been incredibly important in building trust and confidence.

I'm pleased that the Inspector-General of Security Intelligence has found the GCSB's systems and processes to be fully compliant four years in a row, and the NZSIS two years in a row; reflecting that our staff have a strong culture of legal compliance.

In recent years Rebecca Kitteridge, Director-General of the NZSIS, and I have been actively pushing our agencies towards greater transparency and openness where possible.

Where we can we're keen to release official documents to increase the public understanding of what we do and why we need to do it.

For example, our unclassified Annual Reports included more information than ever before; our joint Briefing to the Incoming Minister was released with a small number of reductions; and I believe our responses to Official Information Requests have greatly improved.

Being able to engage more with the public about the risks New Zealand is facing, and the role the Service and the GCSB has in mitigating those risks in fundamental to building trust and confidence.

With the Royal Commission in full swing there will be limitations about what we can say, but having independent review of our agencies, which we welcome should go a long way increasing public confidence in what we do.

Closing Remarks

6(a), 9(2)(a),
b(7)(C)

As we've outlined the agencies have been through a transformational journey in recent years.

It has been a busy time, we remain resolutely focused on delivering against the priorities set for us by the government while continuing to build on the public trust and confidence and maintain our social license to function.

Thank you.

Andrew and I are happy to take any questions you might have.