



# **Follow-up Review for the New Zealand Intelligence Community (NZIC)**

## **Te Rōpū Pārongo Tārehu o Aotearoa**

August 2018



---

## Contents

<b>Executive summary</b>	<b>3</b>
<b>Accepting the future performance challenge</b>	<b>4</b>
NZIC's commitment	4
<b>The future performance challenge</b>	<b>6</b>
<b>Progress on performance improvement</b>	<b>8</b>
Context	8
The scale and pace of performance improvement	9
<b>Areas of focus</b>	<b>14</b>
The Intelligence and Security Act 2017	14
Demonstration of Value	17
Managing Growth	19
<b>Appendix</b>	<b>21</b>
Lead Reviewers' acknowledgement	21

## Introducing the NZIC's Lead Reviewers



### **Sandi Beatie, QSO**

Sandi is a Director on the board of Education Payroll Ltd, Chair of the Archives Council and a member of the Ministerial Advisory Committee on Public Broadcasting. She is a member of the Risk & Assurance Committee for the Department of Prime Minister and Cabinet, and Inland Revenue and a Trustee for Kāpiti Trade Aid.

In 2017, Sandi conducted an Inquiry into the treatment of staff at the Ministry of Transport who raised concerns about a former senior employee and, she then led the development of potential options for strengthening independent oversight of the Oranga Tamariki system.

She has worked in the private sector, local government and the public sector. Sandi's former public sector roles included Deputy State Services Commissioner, Deputy Chief Executive Department of Corrections, Deputy Chief Executive, Deputy Secretary Strategy & Corporate and Chief Information Officer Ministry of Justice.

Sandi holds a Masters in Public Policy, is a member of the Institute of Directors, and a Companion of the Queens Services Order.



### **Geoff Dangerfield, QSO**

Geoff works in governance and advisory roles in the public and private sectors.

He is an Independent Director of Payments New Zealand Ltd, Executive Chair of New Zealand Festival, Director of Wellington Water Ltd, Chair of the Audit and Risk Committee for Oranga Tamariki and Chair of the Major Outsourced Contracts Advisory Board for the Department of Corrections. Previous governance roles include Director of Auckland Transport and of NZ Transport Ticketing Ltd and Chair of the Leadership Development Centre.

Geoff's former public sector roles included Chief Executive of New Zealand Transport Agency, Chief Executive of Ministry of Economic Development and Deputy Secretary to The Treasury.

Geoff holds an MSc in Resource Management, is a Fellow of the Chartered Institute of Logistics and Transport, a Chartered Member of the Institute of Directors, and a Companion Member of Engineering New Zealand.

---

Published August 2018. ISBN 978-0-478-43490-3 (Online) Web address: [www.ssc.govt.nz/pif-reports-announcements](http://www.ssc.govt.nz/pif-reports-announcements)

© Crown copyright



This copyright work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International licence. In essence, you are free to copy and distribute the work (including in other media and formats) for non-commercial purposes, as long as you attribute the work to the Crown, do not adapt the work and abide by the other licence terms. To view a copy of this licence, visit <https://creativecommons.org/licenses/by-nc-nd/4.0/>. Attribution to the Crown should be in written form and not by reproduction of any such emblem, logo or Coat of Arms.

---

# The Performance Improvement Framework (PIF) enables State Service leaders to identify opportunities for improvement, building positive outcomes for New Zealand.

PIF is designed for agencies in the New Zealand State sector.

The PIF Review is a valuable tool that helps leaders drive organisational change. Change that will improve future agency performance, resulting in the delivery of better public services.

Independent reviewers lead each PIF Review. They have significant leadership experience across New Zealand's public and private sectors. Their fresh perspective helps to stimulate 'new thinking' amongst agency leaders as they grapple with the critical issues and challenges that lie ahead for their agency.

The Review is a future-focused exercise. The reviewers consider the questions: what is the contribution New Zealand needs from this agency and what is the performance challenge to make that contribution over the next four years? Taking a four-year horizon encourages medium-term strategic thinking and helps leaders and agency staff to understand what success would look like. Then, by considering current capability to meet future challenges, the reviewers evaluate the agency's preparedness for the future and describe its performance improvement priorities.

Each PIF Review delivers a published report, ensuring transparency and supporting accountability to New Zealanders.

At a suitable time after the PIF Review, the agency may commission a PIF Follow-up Review, in which Lead Reviewers examine the agency's progress on the performance improvement priorities and focus on specific areas agreed with the agency. The Lead Reviewers will also comment on changes in the critical issues and challenges for the next four-year period and may update the performance improvement priorities.



**Peter Hughes**  
State Services Commissioner

*The PIF Review is a valuable tool that helps leaders drive organisational change.*

## Performance Improvement Framework

### Four-year Excellence Horizon

What is the agency's performance improvement challenge?

#### Delivering Government Priorities

How well is the agency responding to government priorities?

#### Delivering Core Business

In each core business area, how well does the agency deliver value to its customers and New Zealanders?

In each core business area, how well does the agency demonstrate increased value over time?

How well does the agency exercise its stewardship role over regulation?

#### Organisational Management

How well is the agency positioned to deliver now and in the future?

 Leadership and Direction	 Delivery for Customers and New Zealanders	 Relationships	 People Development	 Financial and Resource Management
Purpose, Vision and Strategy Leadership and Governance Values, Behaviour and Culture Review	Customers Operating Model Collaboration and Partnerships Experiences of the Public	Engagement with Ministers Sector Contribution	Leadership and Workforce Development Management of People Performance Engagement with Staff	Asset Management Information Management Financial Management Risk Management

---

# Executive summary

This Review is a follow-up to the Performance Improvement Framework Review (PIF) conducted in 2014. The PIF Review came toward the end of a turbulent period for the core intelligence agencies and was accompanied by intense public scrutiny. Other reviews had pointed to the need for attention to professional operational practices and compliance with the law as well as learning from systemic failures<sup>1</sup>. The focus of the PIF was to set a four-year excellence horizon and to assess the agencies' delivery on Government priorities and core business. It also assessed how well the agencies were positioned to deliver then and into the future. Combined with the learnings from the other reviews it acted as a catalyst for galvanizing change.

Since 2014, the leadership of GCSB and the NZSIS underwent change and what has followed is an impressive catalogue of organisational transformation. The performance challenge set out by the PIF signaled the need for fundamentally re-thinking the approach to almost every dimension including leadership, direction and delivery, external relationships and people development.

The NZIC agencies in 2014 were also under both capability as well as severe financial pressures and one of the first acts of the new leadership was to

undertake an in-depth study of cost drivers and future capability requirements. This led to a significant increase in baselines over a four-year period to 2020. This injection and what has occurred in the agencies and across the NZIC as a result, is an instructive example of where adverse PIF findings were taken on board by the senior leadership to drive significant change in performance while at the same time investing in new skills, analytics and tools.

In September 2017, following the Cullen/Reddy Review<sup>2</sup> a new Intelligence and Security Act (the Act/ the new Act) came into force. The Act in summary addressed inconsistencies between the two agencies' legislative frameworks allowing them to work together more collaboratively. While the policy work leading up to the Act was led out of DPMC, the implementation of it rests primarily with GCSB and NZSIS.

In that regard, the specific areas of focus for this follow-up review have been to address how well the community is placed to take full advantage of the potential opportunities the new Act provides. In addition, we were asked to explore two other specific areas: demonstration of value and managing growth.

This report tells a story of a lengthy and challenging journey to get basic systems and processes in place and the introduction of additional capability. This has been critical to the positioning of the agencies now and for the future. The agencies can be confident they are on the right track. Feedback from staff and stakeholders is generally very positive although for some there are still unrealised expectations around how well the sector architecture for coordination and alignment of all security and intelligence functions is performing, while others had concerns about what was described to us as "change fatigue". It is nevertheless understood that there is still much to be done and stakeholders in particular have expectations of seeing tangible lifts in capability over time comparable to the investment that has been made.

NZIC now has a consistent authorising environment and the resources to build its capability and is well placed to continue the transformation that is underway. There are a number of key performance challenges ahead that we have outlined including stepping up the focus and pace of deepening operational cooperation; giving ongoing concerted attention to people and leadership development; improving the experience of stakeholders and customers, and continuing to build and sustain public trust and confidence.

**Sandi Beatie**  
Lead Reviewer

**Geoff Dangerfield**  
Lead Reviewer

---

<sup>1</sup> 2009 Murdoch, 2013 Couchman and 2013 Kitteridge reviews.

<sup>2</sup> Intelligence and Security in a Free Society, the First Independent Review of Intelligence and Security in New Zealand by Dame Patsy Reddy and Hon Michael Cullen – 29th February 2016.

---

# Accepting the future performance challenge

## NZIC's commitment

As the leaders of the NZIC, we welcome the PIF Follow-up Review's positive assessment of the agencies and agree with the focus areas identified. The 2014 PIF provided us with a roadmap for change. We have used that roadmap, along with the government investment in the NZIC, to build solid foundations while delivering value to our customers.

It is reassuring that the assessment confirms that we are on the right track and that our efforts over the last few years have been in the right areas and in the right direction. We are half way through the investment programme so expect our performance and impact to continue to improve.

The areas for future focus identified in the PIF Follow-up Review are known to us and we have work in train to address these performance challenges. We have made considerable progress in integrating and aligning functions; particularly core enablement areas such as HR, finance, security, IT, policy and planning. We are committed to a more deliberate approach to integrating our strategies and operations where this will improve our effectiveness, generate value for customers, and is legally permitted. After all, in an increasingly connected operating environment, neither our customers, nor those who wish to harm New Zealand's interests, see distinctions between HUMINT<sup>3</sup> and SIGINT<sup>4</sup>, or domestic and international security.

We continue to build better working relationships across the public sector. This is particularly apparent in working with public sector agencies on policy advice that may have national security implications. Our input has been welcomed by other public sector agencies and we expect the demand for our input and expertise to continue to increase.

GCSB and NZSIS have recently launched a joint leadership competency framework as we know our leaders need to be fully equipped as the organisations grow. The framework has associated training and development depending on the level of leadership role. In addition, we work with the DPMC led National Security Workforce Strategy programme to assist staff to have career paths across the wider security and intelligence sector. We will explore opportunities to better align our values and ensure we engage with the SSC as it looks at common values across the public sector. We will continue to build on the good progress made to date to foster greater diversity and inclusion within the agencies and to address the gender pay gap.

The intelligence customer engagement initiative is now being trialled with other agencies. Customer engagement will remain an area of focus as we improve our understanding of customers and stakeholders' business requirements, and assist them to understand how they can use our products and services to achieve their outcomes.

*It is reassuring that the assessment confirms that we are on the right track and that our efforts over the last few years have been in the right areas and in the right direction.*

---

<sup>3</sup> HUMINT is Human Intelligence: activities that involve the use of any persons to gather intelligence.

<sup>4</sup> SIGINT is Signals Intelligence: intelligence gathered or derived from communications and information infrastructures.

Both Directors-General regularly speak on New Zealand's threatscape, including cyber threats, the role of our agencies, our recruitment needs, and the improvement track the agencies have been on. DPMC has more actively publicised the arrangements in place and the workings of the national security system (ODESC). We are all focused on ensuring more unclassified information is available publicly. Examples of this are that our annual reports have richer content and our joint Briefing to the Incoming Minister was proactively released for the first time in 2017. We are taking a more strategic approach to communications in order to further inform the public understanding of national security challenges.

The NZIC continues to face the challenge of how to measure performance and demonstrate our impact while balancing security and

transparency requirements. We will further explore how we demonstrate that we have the right level of capability to collect and assess intelligence and ensure New Zealand is a credible contributor to international intelligence and security.

The Security and Intelligence Group (SIG) of DPMC takes a leadership role on system level national security policy, risks and issues. The NZIC welcome the reviewer's finding that the GCSB and NZSIS have matured as agencies, which now allows DPMC to focus on leadership and system steering. DPMC has picked up the challenge of steering the national security system, including strengthening shared common goals.

Finally, we would like to thank the Lead Reviewers for the time they took to understand the NZIC, our functions, opportunities and challenges.

*We are taking a more strategic approach to communications in order to further inform the public understanding of national security challenges.*



**Andrew Hampton**  
Director-General of the GCSB



**Rebecca Kitteridge**  
Director-General of Security



**Howard Broad**  
Deputy Chief Executive DPMC

---

# The future performance challenge

The state and performance of the New Zealand Intelligence Community (NZIC) is substantially different from that described in the 2014 PIF Review. The agencies have improved their performance in the critical areas identified in that review. Together with a consistent authorising environment established in the Intelligence and Security Act 2017 and the additional financial resourcing that has been committed through the Strategy, Capability and Resourcing Review (SCRR) process, the agencies are well placed to continue the transformation that is underway.

The agencies are clearly on the right path. The transformation so far addresses weaknesses identified in the PIF review published in 2014 and builds a foundation for the future. The future performance challenge for the agencies is to fully embed the changes that have been made and use that as a platform to drive transformation further into operational areas, which is where lasting improvements in effectiveness will be achieved.

## **Deepen the operational cooperation between the intelligence agencies**

With improvements to the underlying business systems that have been made or are underway, the next challenge is to lift improvements in the operational systems and capability and to lift the level of operational cooperation between the GCSB and NZSIS.

The success of the shared services approach needs to be replicated by a stronger focus on joint operational teams on the national security and risk issues facing New Zealand.

While the operating environments for each of the two agencies are different and distinct, the performance

challenge is to be more purposeful on the expectation of working together and to lay out the cooperation development plan.

## **Build stronger relationships across the public sector**

The GCSB and NZSIS are now more formally part of the Public Service, and that brings with it the opportunity to act more deliberately and collegially as part of the wider policy and operational community that deals with security and intelligence matters. As DPMC focuses more broadly on the rest of the sector, NZSIS and GCSB will need to do as well, as partners in that broader sector. In doing so, the agencies will need to learn to be more open and engaging. To date the latter has primarily rested on the shoulders of the agency heads and while they have a continuing role to play in this, the expectation needs to now be shared more amongst tiers two and three. The new Joint Directors-General Office (JDGO) will play an important role in this.

## **Build and retain the required workforce – including effective leadership and management of people and a common set of values**

Meeting this performance challenge requires persistent concerted attention to the ongoing development of people managers and commitment to the implementation of the workforce strategy developed for the two intelligence agencies and the links to the National Security Workforce Strategy. There is a need to speed up the development of specific skills and training to ensure that the tradecraft and technology skills are brought on board.

A priority for the NZIC must be the implementation of effective leadership and development pathways that enable more mobility of staff and experience between the intelligence community, the national security sector and the wider public sector.

A more seamless way of working between the agencies is a people leadership challenge. While there will always be aspects of different cultures within the NZSIS and GCSB that are evident because of the nature of different work and differing skill sets, a more joined-up workforce needs to be underpinned by a common set of values to guide desired behaviour. The different expressions of organisational values that have been developed by each agency to date work against this.

*The agencies are clearly on the right path.*

---

## **Be truly customer oriented, and bring the necessary products and advice together in a more integrated way**

Developing a customer engagement approach across the NZIC remains a work in progress. It is vital to effective performance, given that this is how stakeholders and customers experience the work of the agencies and make judgements about their effectiveness. Our interviews revealed that a key challenge, especially for Ministerial decision makers, is to clarify the purpose and priority of the information that is presented to them, especially when it is not accompanied by advice on the actions they might take as a result. In part, this stems from the limitations on the roles of the agencies, and on the National Assessments Bureau (NAB) that preclude them from being the policy advisors. There are also challenges to ensure that the protective security activities and the cyber protection initiatives continue to be well focused on customer needs.

We think the big performance challenge here is to ensure that the customer engagement approach is couched more in system terms than in agency terms. When looked at from the customer's experience, they need both intelligence/security information and the "choices on what to do" advice presented together where practical. Part of the performance challenge is to gain a better understanding and regular insights into what is useful for the customer, and in the case of decision-makers what they need in order to make quality decisions and ensure that this is done in a timely way.

## **Strengthen public trust and confidence, and be open and engaging about New Zealand's risk environment**

The performance challenge is to step up the public engagement about the work of the intelligence community and to be open about the issues and security challenges that New Zealand faces. Done in the right manner this will not compromise the activities of the agencies or trust of partners. There is a richness of story that can be told that does not compromise the need for secrecy but talks to what matters to New Zealanders. While often the

public discourse in some sections of society can take a negative slant, the fact remains that intelligence agencies have a legitimate role in protecting New Zealand's safety and security. To do that they have powers given by Parliament that they must carry out in a lawful manner. Less well known is that 'intelligence' plays a role for instance, in protecting our borders from transnational crime. The protective security activities of the agencies protect against cyber threats, cyber crime and also help to protect our personnel, property and information.

## **Develop the Security and Intelligence Group's purpose and refine the structures**

The security and intelligence activities are spread across many aspects of government, and it is the role of the Security and Intelligence Group (SIG) of DPMC to ensure that there is a whole of system view of risks, priorities and actions, and where system performance can be improved.

The performance challenge in this area is to shift from oversight and reacting to developments, to leadership and system steering. As GCSB and the NZSIS have lifted their performance, the SIG purpose and relationship needs to be redefined. While there will still be a need for a collegial collaborative relationship with GCSB and NZSIS, the SIG focus needs to pivot more towards the broader sector and its system role in relation to risk and security (including cyber) policy. The stewardship of the system requires strengthening the shared common goal and clarifying the inter-dependent roles within the Security and Intelligence Board (SIB). It also needs to coordinate the sector's interface with the Prime Minister and other Ministers.

## **Demonstrating the capabilities for success**

A common question is how can we measure what we are delivering in terms of the security of New Zealanders? There is a tendency to want to seek out measures that build on the numbers of intelligence reports prepared at one end of the spectrum or the evidence of outcomes of the lack of harm at the other.

The performance challenge is to demonstrate that the investment in the intelligence community is building the requisite capabilities to achieve a higher degree of protection in each of the high priority national intelligence priorities. That means building a strength in capability assessment methodology that can robustly demonstrate the shifts in capability in the required areas.

*The performance challenge is to step up the public engagement about the work of the intelligence community and to be open about the issues and security challenges that New Zealand faces.*

---

# Progress on performance improvement

## Context

The 2014 PIF Review focused on the 'core intelligence community' (NZIC) which comprised of:

- the National Assessments Bureau (NAB)
- the Government Communications Security Bureau (GCSB)
- the New Zealand Security Intelligence Service (NZSIS).

For the purposes of this follow-up PIF Review, our focus will include the wider Security and Intelligence Group (SIG) within the Department of Prime Minister and Cabinet (DPMC) of which the NAB is a part. Areas where the respective roles between the agencies and the broader sector intersect are also included in the review.

As a collective, the NZIC articulate their purpose as serving their key customers<sup>5</sup> to

- Increase New Zealand's decision advantage
- Reduce threats to New Zealanders
- Strengthen protective security.

This requires working collaboratively with each other and with the wider intelligence sector<sup>6</sup> to collect and analyse intelligence and provide information and advice especially to decision makers across Government that can help protect New Zealand security interests. Further to the core intelligence and security functions played by the NZIC, DPMC plays a coordination role across the whole sector through the functions of the SIG.

The intelligence community works together to strengthen protective security including cyber security by providing the policy, protocols and guidelines to help agencies identify what they must do to protect their people, information and assets.

Internationally, the NZIC works in partnership with other intelligence communities, most notably as part of the Five Eyes<sup>7</sup> network. New Zealand provides intelligence products and services to partner countries in areas of specialist capability or focus and receives relevant intelligence products and services in return. New Zealand relies heavily on the resources and products that these partnerships provide.

Since the PIF Review in 2014, there has been substantial change, the intelligence community has been asked to respond both to a rapidly changing international landscape and to organisational challenges and opportunities set out over the past few years and an increasing pressure to maintain and improve public trust and confidence.

During this time, the NZIC agencies received a significant baseline increase in funding in order to build a future-focused strategic operating and investment model over the next four years (2016-2020). This increase was a result of a Strategy, Capability and Resourcing Review (SCRR) with the intent to better position the organisations to meet the current and future challenges.

This PIF Follow-up Review looks at how far the community has come since 2014, into what the future challenges might look like and how well placed the organisations of the NZIC are to respond to them.

*The intelligence community works together to strengthen protective security including cyber security by providing the policy, protocols and guidelines to help agencies identify what they must do to protect their people, information and assets.*

---

5 Customers include Ministers, Government Agencies, Business and New Zealanders – as articulated in the New Zealand Intelligence Community Four Year Plan 2016-2020.

6 The intelligence sector is a group of wider agencies or parts of agencies including the NZIC and others such as Police, NZDF, MoD, MFAT, Customs, MPI and MBIE.

7 Five Eyes refers to the UK, Australia, Canada, USA and New Zealand.

---

## The scale and pace of performance improvement

### 2014 Excellence Horizon

The 2014 PIF identified a number of significant shortcomings within the three core NZIC agencies. Those shortcomings were found to be inhibiting the performance of each of the agencies and impacting the effectiveness of their combined contribution to New Zealand's national intelligence and security sector.

The Review described the challenge within a four year horizon for these intelligence agencies as being able to demonstrate it has enhanced the nation's safety, increased New Zealand's resilience to threat and continued to deliver value in the interests of New Zealand. In order to do this, the agencies needed to deliver strong sustained performance across a number of areas including policy development, assessments, collection, protective security and threat management. The PIF pointed to substantive weaknesses in the organisational health and capability of both GCSB and NZSIS while at the same time being under significant fiscal strain.

### The Journey so far

#### *Responding to the 2014 performance challenge*

Following the 2014 PIF and to understand further cost drivers and capability needs, the agencies undertook a comprehensive Strategy, Capability and Resourcing Review (SCRR) in the same year. This enabled the agencies to substantially address the organisational weaknesses and set the foundations for improving capability. The depth of work undertaken through the SCRR project led to Government support in the 2016/17 financial year for the sequencing of investment in the agencies over an initial four-year period. This has been fundamental to improving both capacity and operational capability across the core functions of domestic and foreign intelligence and security within GCSB

and NZSIS along with some additional capacity to DPMC's Security and Intelligence Group.

#### *Addressing internal infrastructure*

The 2014 PIF identified that the internal support infrastructure of the NZSIS and GCSB was well below accepted standards and not well linked to changes made to management practice in the wider State Sector. Urgent attention therefore needed to be given to addressing a legacy of very weak internal capability and systems to position the agencies well to manage both current and projected growth in future years.

Significant progress has been made in each of these areas with new capability deployed into human resources, finance and IT to establish a 'shared service' approach for GCSB and NZSIS. These functions are integral to achieving the purpose of the agencies. Consequently, a more purposeful approach is being taken to people management, financial management and to improving the IT environment. There have been identifiable improvements to the processes of recruitment, performance management, remuneration and support for people managers along with a step change in financial management and the commencement of upgrading IT support and capability.

These are relatively new improvements and it is recognised that there is still some way to go in all of these areas but there is a clear pathway for building upon what has already been put in place. Nevertheless, critical challenges remain including recruiting a more diverse workforce particularly in core intelligence collection capability. The recently developed Diversity and Inclusion Strategy will help to address the issue in a systematic way. As the community grows and potentially becomes more diverse, there will inevitably be quite a significant cultural challenge to ensure the protection of the integrity and social licence to operate while continuing to build and retain Ministerial, customer and public trust and confidence. Sound systems around induction and training will be critical, as is the continued attention to 21<sup>st</sup> century leadership development.

*Significant progress has been made...*

---

### *Positioning for the future*

While SCRR has been critical to enable the intelligence community to improve resourcing and capability, the heads of each organisation have also set about transforming how their respective organisations operate. This is most apparent for the NZSIS where recent significant structural change combined with a new Intelligence and Security Act has meant a large and challenging programme of change. Other initiatives contributing to supporting transformation particularly within both GCSB and NZSIS include clarity of purpose and mission; a joint workforce strategy; establishment of policy capability; changes to leadership team composition; improved focus on compliance; the successful delivery of a large technology programme to counter cyber threats; and the development of a Joint Directors-General Office. Critical to positioning for the future has been the attention given to the broader development of the top secret workforce. For example, initiatives to close the gender pay gap, the active and successful graduate recruitment programme in the Bureau and support for programmes to encourage women into science, technology, engineering and mathematics with the aim of achieving greater diversity across the workforce.

While new ways of working in a number of areas are still bedding in, the job is not yet done with attention now needing to turn to further improving the core intelligence collection and security protection functions so that they are optimally placed to operate in a faster paced and volatile world. That said, the focus brought to improving performance to date has shown an impressive degree of leadership and persistence to get things right.

### *NZIC and the wider Security and Intelligence Sector*

The purpose of the NZIC is to deliver decision advantage to the Government on managing specific risks to national security. It does this through intelligence led advice and insights as well as specialist advisory services on protective security, cybersecurity

and other security risks. The 2014 PIF noted the need for the NZIC to clarify the scope of its role and to create more seamless collaboration and efficient resource allocation amongst the individual agencies. This approach would help to achieve products and services prized by key customers as vital and which deliver more value than the outputs of the individual agencies.

The PIF coincided with DPMC being mandated by Cabinet to lead the NZIC. This manifested itself in the development and implementation of a broad set of National Intelligence Priorities and establishing cross-sector Priority Co-ordination Groups to implement the priorities. It resulted in DPMC working closely with the NZSIS and GCSB to restore Ministers' trust and confidence and participating in the Strategy, Capability and Resourcing Review (SCRR), the Cullen/Reddy Review and subsequently leading the policy work that provided the legislative framework for the Intelligence and Security Act 2017.

In the security and intelligence sector all three agencies are seen as key contributors at senior levels to the various fora that have been established to aid collaboration, cooperation and information sharing in times of national crisis and in addressing external threats to New Zealand. The Chief Executive of DPMC chairs the Officials Committee for Domestic and External Security Coordination (ODESC) which is called together when a particular threat or situation requires collaborative action. DPMC, through its Security and Intelligence Group has established other architecture for the purposes of sector coordination and information sharing and the assessment and collation of all hazards and all risks. DPMC's Deputy Chief Executive chairs the Security and Intelligence Board (SIB), which focuses on external threats and intelligence issues, and oversees the National Intelligence Priorities (NIPs). There is also a Hazard Risk Board (HRB) which focuses on civil contingencies and hazard risks. Both Boards allocate risks to specific agencies.

*Critical to positioning for the future has been the attention given to the broader development of the top secret workforce.*

---

During the course of this Review there were a spectrum of views expressed around the effectiveness of this architecture. There was clarity on the role of ODESC. On the other hand some were critical of SIB and felt that its role needed to be better defined, while others thought it was a maturing forum whose development depended upon the willingness of the respective agencies to make it work. Sector collaboration at the best of times is not always an easy thing to achieve. While the formality of architecture is useful, it cannot take the place of constant attention to relationships. These appear relatively strong at senior levels and between certain individuals across the agencies. The modelling of trust and coordination by NZIC leaders is seen as a strength by sector partners who are keen to see that spirit of collaboration consistently applied by middle managers and at day-to-day working levels.

As a result of structural changes within DPMC, a Deputy Chief Executive, Security and Intelligence was created to lead a newly formed Security and Intelligence Group (SIG) taking the place of the former Intelligence and Co-ordination Group. This group operates at a functional level (intelligence) and a system level (i.e. all-risks approach to national security). Given the strength of leadership evidenced in the GSCB and the NZSIS and the status and accountabilities of the Directors-General and their agencies as government departments, there is no longer a need for DPMC to provide the significant level of oversight and supervision that it has.

The challenge now for the NZIC and in particular, DPMC SIG is to work collaboratively with the NZSIS and GCSB on intelligence and security matters and advice to government, while at the same time focussing its efforts toward cross-sector and system stewardship. This latter role is the core purpose of SIG. It means a focus on sector priorities and assessing whole of sector capability to achieve them. It also means developing efficient mechanisms to enable sector coordination and information sharing. Conversely, it means not being drawn into operational matters.

The three agencies working collaboratively together is still an important aspect of being part of NZIC, especially as the Government has invested through SCRR to increase the community's capacity and capability but also because there are opportunities to collaborate around intelligence collection and reporting. Some important foundations to this collaboration have been put in place including an agreed NZIC strategy and four-year budget plan. A joint leadership team comprising representatives from the respective agencies was established to provide a governance mechanism for key projects including SCRR report backs. It is also intended to refresh the cyber security action plan and national cybercrime plan. These initiatives have been necessary to ready the agencies for their next phase of growth, and to provide a combined view to improving performance.

#### *Establishing a Protective Security Approach*

In addition to the changes noted above, a Protective Security Requirements framework has been developed and implemented across government and to some key private sector economic generators. The framework initially started by DPMC has been transferred to the stewardship of the NZSIS and has been in place for 2 years. It relies upon the external organisations self-reviewing against capability criteria on an annual basis. These self-reviews enable transparency around maturity levels and the areas that require most attention. This has been a well-supported and sound initiative that appears to have led to greater awareness of protective security requirements and increased maturity as well as being viewed positively by Five Eyes partners. GCSB's National Cyber Security Centre proactively helps agencies and organisations of national significance protect and defend their information systems against cyber-borne threats that are typically beyond the capability of commercially available products and services.

*The modelling of trust and coordination by NZIC leaders is seen as a strength by sector partners...*

---

### *Reshaping the approach to Vetting*

The NZSIS also responded with some urgency to customer criticism of the vetting for clearances service. A 'Better Every Day'<sup>8</sup> approach to improvement was initially adopted to better understand customer needs and pain points. Process improvements and technology changes have been made as well as the introduction of new skills within the team. There is now greater transparency around the day-to-day workflow through a set of metrics for tracking performance. The average time taken has reduced by over 50% since mid-2017, however, the service is still hampered by backlog issues with waiting times that can in some cases take up to a year for candidates seeking Top Secret and Top Secret Special clearances. This includes those seeking a renewal at the same level.

The remaining challenge is to find a sustainable means of addressing the pipeline issues that in turn affect perception of the quality and timeliness of the service. Action is being taken to segment how the different levels of clearance requests are handled. There are also opportunities to explore segmenting further high volume customers and finding solutions with them that could be mutually beneficial. For example, exploring a potential fee for service to allow for additional specialist vetting staff. Given the low level of clearances where an adverse recommendation is made there could also be other opportunities for improvement that would further reduce timeframes. Another area to consider is whether judgements on the level of classification required are being consistently applied particularly in situations where customers are seeking high volumes of Top Secret or Top Secret Special clearances.

The processing nature of vetting does lend itself well to the 'Better Every Day' continuous improvement method, and we encourage the continuation of making improvements through staying close to the customer and candidate experience. To achieve more substantive changes to vetting will be reliant on automating tasks and processes where possible within the system. We understand a case is being prepared to seek internal support for a technology upgrade.

#### *Customer focus*

In responding to the challenge called out in the initial PIF Review around value products and services to customers, the National Cyber Security Centre (NCSC) and Protective Security Requirements (PSR) Outreach are examples of an improved understanding of customer demand.

The NZIC has initiated a customer engagement initiative which is also utilising the 'Better Every Day' method. The Ministry of Foreign Affairs & Trade (MFAT) was selected as the first customer to work with, and are enthusiastic about the results. The work to date has included understanding pain points and customer needs. Trials are now underway with MFAT testing new approaches to the delivery and utilisation of information. The intent is to extend this engagement initiative to other customers.

The initiative is a positive step, however progress is fairly slow and labour intensive. This raises the question as to whether the improvements being trialled with MFAT could be sustained over a wider group of customers if not accompanied by alternative and improved means of disseminating and enabling access to information.

It is also clear that the customer agencies themselves will need to further develop their own systems and processes to handle secure information and to make effective use of it in their assessments. Given the variable maturity level amongst staff to 'customer'<sup>9</sup> across the NZIC agencies, there is also a question as to whether in this instance, taking an improving processes method on its own will lead to sustainable outcomes. Bedding in customer awareness and why it is important to the normal way of working is as much a cultural challenge for the respective agencies as it is to do with processes and requires an overall defined strategy and plan. This has been seen to work successfully in situations utilising a first principles approach. This approach is informed through taking a whole of system perspective coupled with development of an in depth understanding of the customer base, the segments within that, the needs of each segment and the value they are seeking. This in turn drives clarity about the value that can be brought to each customer grouping as well as identifying priority areas for making improvements to levels of engagement and process improvement. Focussing on the quality of engagement and the simplification of processes through learning from the voice of the customer become an essential part of day-to-day continuous improvement backed up by strategy and data sets. There could be value in each of the agencies individually taking a more considered view of their current customer set, segments, needs and the value they seek, then coming together to understand the differences and commonalities and to derive a forward strategy for taking the customer initiative into the future.

---

8 Better Every Day is a methodology developed by the State Services Commission focussed on improvement through the lens of the customer.

9 "Customer" in this context includes the intelligence sector agencies, other agencies of State, private sector partners or those the agencies works with and, decision-makers including Ministers.

---

## Sector Workforce Strategy

Apart from intelligence matters, sector chief executives have also addressed pressure from within the workforce for a more organised system of talent management akin to the broader public sector. This initiative has culminated in the development of a National Security Workforce Strategy. The workforce covered by the strategy comprises approximately 1,600 personnel who hold Top Secret or Top Secret Special clearances. A third of this workforce is under 35, mostly university educated with a 15.8% diversity statistic against a public sector average of 35%.

Club funding for this initiative made it possible to hire an experienced manager to drive the initiative and to enable a more systematic approach to understanding workforce

demographics including remuneration differentials, career needs and succession challenges. A sector based Career Board has a focus on succession for critical roles. Other initiatives include a sector Job Board for notifying vacancies and a formalised mentoring programme for women. To create a better appreciation of the roles of each agency, workforce showcases have recently been held in Auckland and Wellington with a total of 700 attendees. Staff we spoke with were extremely positive about both the showcase and the strategy itself as it is giving them a sense of being part of a bigger system with potentially greater opportunities. The success or otherwise of this initiative rests with the sector chief executives and their commitment to continuing the work that has been started.

*Staff we spoke with were extremely positive about both the showcase and the strategy itself as it is giving them a sense of being part of a bigger system...*

---

# Areas of focus

This PIF Follow-up Review looks at three specific areas, detailed below:

1. The Intelligence and Security Act 2017. How well are the agencies placed to get the full benefits from the Act, and where do they still need to build functions and capability?
2. Demonstration of value. What does public and customer value look like in the complex environment of the intelligence community and to what extent can this be measured and communicated?
3. Managing growth. During the current period of significant change, how well is the community positioned to grow, not only in size, but in capability and performance delivery?

## The Intelligence and Security Act 2017

To a large extent the new Intelligence and Security Act 2017 grew out of the Report of the First Independent Review of Intelligence and Security in New Zealand by Dame Patsy Reddy and Sir Michael Cullen, published in February 2016. The review found that the legislative mandates for the two intelligence agencies were out of date and incomplete. It recommended that the legislation be overhauled to address inconsistencies between the agencies that created barriers to them working effectively together. Amongst other things, the review concluded that the agencies need to be able to combine their skills and knowledge to provide information that the Government requires. While required by their terms of reference to maintain separate agencies, an underlying theme of the Review was how the agencies should be aligned and cooperate without undermining each CEO's accountability or compromising security outcomes.

Essentially the new Act creates a common authorising and compliance environment for the two intelligence agencies. The provisions of the new Act are designed to focus on the intelligence and security objectives, functions and operating frameworks. With a few exceptions for individual responsibilities and requirements, the Act makes joint provisions for the NZSIS and the GCSB. The Act also reinforces the role of the NAB, hence covering the core elements that make up the NZIC which is the focus of this PIF report.

The Act came into force in September 2017, and a great deal of work was done in the prior period after the date of assent in March 2017 to establish a number of the policies and operating procedures that required to give effect to the Act.

## What the new Act enables

The 2014 PIF stated that the performance challenge for the NZIC was to clarify the scope of its role and then to create a more seamless collaboration and efficient resource allocation amongst the individual agencies in support of its purpose. In terms of business strategy and operating model, the performance challenge was to ensure that the NZIC works together effectively so New Zealand gets the maximum combined benefit from its security intelligence agencies – by working together to avoid duplication and to maximise synergies.

While maintaining the separate agencies, the Act creates a common authorising environment and establishes expectations around cooperation between them and other agencies. We look at whether the agencies are together making the most of the new Act and what it enables.

## Common objectives, functions and priorities

Having common objectives and functions for the work of the intelligence agencies has clarified the role of the agencies and their mandates to collect intelligence whether in New Zealand or overseas. It has removed distinctions that previously existed based on the type of intelligence collection, and focussed on the objectives of intelligence and the steps that must be taken to ensure that the range of intelligence activity is appropriately authorised and lawful. While the Act creates common functions around protective security services and advice and assistance, it gives GCSB specific responsibilities in relation to information assurance and cybersecurity activities.

The 2014 PIF review concluded that clarifying the national security priorities was an essential requirement to enable effective resource allocation. It noted that it would be ideal that the priorities chosen were achievable with the resources available. While not a requirement of the new Act, the Government has established a set of National Intelligence Priorities that guide the work of these intelligence agencies - as well as all other agencies with intelligence responsibilities across the public sector (MFAT, Ministry of Primary Industries, Customs and so on). The agencies now have a much better basis than before to guide the development of their respective work programmes.

Each agency has worked to establish a set of strategic plans and operational priorities within this environment, and to get alignment within their agencies on these plans. This could move to the next stage of a common strategy between the agencies that could effectively lay the

---

groundwork for establishing a joint operational focus on specific issues that is now required to maximise the value of the stronger foundations of agency capability.

## Cooperation initiatives and frameworks

The Act is framed around an expectation of cooperation. To date this is most visible in the GCSB and NZSIS Shared Services approach.

A substantial step has been taken recently to establish a Joint Directors-General Office (JDGO) with responsibilities for strategy development, Ministerial relationships and servicing, communications and international engagement. While staffed from both agencies, the JDGO is designed to merge capabilities and hence lift the capacity of the two organisations to jointly understand their operating environment and to plan how each agencies operational capability can be developed and used to greatest effect. It is still in the early days of its establishment and not yet fully staffed. The two agencies are letting the JDGO “evolve” rather than define too closely what is expected in the future.

While good progress has been made, there is not a clear overall vision on what working together looks like or a joint plan on where the next steps lie. The “cooperation plan” has been developed as a plan as you go rather than been a more purposeful exercise. They have taken opportunities as they have arisen. This creates an environment of uncertainty for staff about what the journey ahead looks like and what can be expected of them.

To date the prevailing view is that the agencies will cooperate and will seek to make common service provision where it makes sense to do so. Each function has been dealt with and assessed separately and sequentially. The underlying framework tends to reinforce the interests of each separate agency first and then cooperation as a secondary objective.

The alternative is to put the cooperation requirement the other way around; the default position being that

the agencies will cooperate and build collaboration in all that they do unless there is a good reason not to do so. They will put their cooperation interests first, and then assess those within the requirements of each separate agency. In other words, they will maintain their “separateness” as individual agencies where it is necessary to achieve their responsibilities under the Intelligence and Security Act and cooperate and collaborate on everything else. It still requires a very careful assessment of the collaboration proposition, but weights it in favour unless the costs and risks are too high and outweigh the benefits. If this was the stated objective, it would provide a strong internal signal in terms of the culture of cooperation to be created. In time we would expect to see a stronger “one strategy – two agencies” approach.

The challenge now is to deepen the cooperation on the operational side. The new Act provides for closer operational activity and then the next generation of cooperation initiatives can be based around joint teams that can tackle the major national security priorities. The changing context for intelligence collection seems to point to a degree of overlap and convergence over time of HUMINT and SIGINT as sources of intelligence. At the very least it is “SIGINT enabled HUMINT” and vice versa. To make sense of information on a person or organisation of interest requires bringing those streams of intelligence together. Doing that across the borders of separate agencies contains risks.

The other elements of cooperation are with New Zealand agencies such as NZ Police, Customs, Immigration and NZ Defence Force. While the feedback in the interviews for the Review indicated much stronger relationships and joint working than had existed before, it was also acknowledged that there is still some way to go. The new Act’s requirements on sharing of relevant information how that may occur have helped create a stronger cooperation environment. Ministerial expectations have also been established on the management of information obtained by an intelligence agency.

The performance challenge is to create the best conditions possible that enable the cooperation that will enable better intelligence gathering and assessment and ultimately stronger security. If at some point in the future Ministers were to decide to merge the agencies, then the prospect would be less daunting and the performance loss that often occurs in such circumstances would be diminished.

## Operational policies

The new Act has established a common framework for operational policies, a clearer basis to establish the bounds of lawful activity and where specific authorisations are required. As a result, the agencies worked promptly to make use of this environment by developing a suite of core operational policies that give effect to the Act’s provisions.

The Act enables clear guidance to the security and intelligence agencies from the Minister on how they conduct their activities through a formal mechanism of Ministerial Policy Statements (MPS). These cover activities such as collecting information lawfully from persons without an intelligence warrant, or requesting certain information from other agencies. Ministerial Policy Statements also provide guidance relating to cooperating with overseas public authorities. All the mandatory Ministerial Policy Statements were developed before the Act came into force. Internal policies reflecting those MPS requirements are being worked through.

In terms of other operational policies, the agencies have approached this as a joint exercise where applicable. Given the different operating environments it has taken time for each to be developed and consulted on with relevant staff.

---

The Act provides for the application and issue of joint intelligence warrants, which once issued the authority to act under the warrant can be taken by Director-General of either service “jointly or severally”. No joint application has to date been made, even though we understand there have been cases where separate warrants have been sought for the same reasons. Working through the required operational policies to support such joint application would seem to be a priority.

## Oversight and Compliance

The new Act largely carries over the functions of the Inspector-General of Intelligence and Security (IGIS) from the earlier (separate) Act, but with enhanced independence. The IGIS has a broad range of functions as set out in the ISA. These functions include the ability to conduct inquiries into certain matters referred to the IGIS by the Minister, the Intelligence and Security Committee or the Prime Minister, or to undertake such inquiries on the IGIS’s own initiative. There are also a number of review functions, including to conduct reviews at least once a year, on the effectiveness and appropriateness of the procedures of each agency. These reviews ensure that the agencies are compliant with the Act in relation to the issue and execution of an authorisation and the compliance systems for all their operational activities.

Each agency is continuing to develop its own compliance systems and procedures given the different environments they operate in and the different stages of development. Nevertheless in some areas there have been opportunities to develop new procedures together that have not been taken up, e.g. the development of processes for the issue of warrants.

## Reporting – building trust and confidence

The new Act requires the Director-General of each of the intelligence agencies to prepare an annual report for the Minister on the activities of

the agency. The report must cover the financial performance of the agency, as well as assistance it has provided, the warrants it has sought and the authorisations each agency has given. The Minister must give the report to the Intelligence and Security Committee, and after suitable redactions as authorised by the Act, a copy of the report is to be presented to the House of Representatives.

These provisions are designed to provide a more open environment for discussion and scrutiny of the activities of the agencies and brings them into a similar reporting regime as can be found for the public sector more generally. Needless to say, sensitive information can be withheld for good reason.

The annual reports – which are available on-line – now contain information on the NZSIS and GCSB that is significantly richer about their context and priorities, and the broad scope of their activities that has been available before. Both agencies see this as an important step in building the public’s trust and confidence about what they do and why they do it.

The Inspector-General of Intelligence and Security also plays a critical role as part of the independent oversight system that checks on the appropriate and lawful use of the powers that are available to the intelligence agencies under the new Act. While this scrutiny might at times feel uncomfortable, it has considerable value in building an environment of trust with critical stakeholders and the public. Given the intrusive powers of the agencies, the role of the IGIS is an important component in preserving their licence to operate with both Ministers and the public.

Both Directors-General are to be congratulated on being much more visible and engaged on the public stage than ever before. There remains an opportunity for the organisations as a whole to be even more open without compromising their underlying security mission. Ultimately, this requires judgement on the appropriate balance between transparency and security.

*Given the intrusive powers of the agencies, the role of the IGIS is an important component in preserving their licence to operate with both Ministers and the public.*

---

## Demonstration of Value

The issue here is how does the intelligence community assess the value of what it does and how does it demonstrate that to a range of stakeholders?

A key difficulty is that the value of security and intelligence activities is inherently hard to demonstrate – in large part because of much of the work is secret and also because these activities are just one of a number of inputs to building a more secure and protective environment for New Zealanders.

Furthermore, there are quite different audiences for the “value story” – from key Government decision-makers that have access to highly sensitive information on national security risks to a broader public engagement that might be sceptical on why we should have intelligence agencies at all. It is also important to be able to tell the performance story to the staff engaged within these agencies, as making a difference is the strong motivation for working in the sector. Unlike other parts of the public sector, these agencies work in an environment where it is not able to publicly disclose the full nature of its activities, and hence the need to find the right balance between security and transparency.

## Outcomes – keeping New Zealanders safe

The fact that the attribution between the activities undertaken and the outcomes achieved is not direct is a common challenge for a number of government agencies, and hence the need to find ways of building a performance framework that uses a series of measures to form an overall picture of value and success to a range of customers and stakeholders.

At the outcome level, these agencies contribute to keeping New Zealanders safe. The intelligence community’s contribution is to ensure that the Government, enforcement agencies (NZ Police, Customs, NZ Defence Force etc.) and key national organisations make effective decisions based on the best possible

information and advice. The unique contribution is the gathering of intelligence from sources that others cannot access, and building relationships with decision makers that enables the information to be best suited to their needs. That points to performance measures that are focussed around the relevancy and timeliness of reporting on changes and developments in the security environment and on the nature of specific threats. Relevancy will be linked to judgements that the information cannot be readily duplicated or sourced elsewhere.

While the desired outcome is clear, the security and intelligence contribution is one of several to achieve it.

## Intelligence capability

This is at the heart of the value proposition for the intelligence community, and how the key Government decision makers are likely to assess whether the agencies are on track to deliver stronger security. Success should be measured in large part by the extent to which the agencies have developed the right level of capability to be:

- effective in collecting and assessing intelligence in their own right – in terms of the Government’s National Intelligence Priorities
- credible contributors to the international intelligence community through the Five Eyes relationship, and hence the access to the much larger intelligence gathering and assessment capability of our partners.

Measures of capability require a clear description of the different components of intelligence collection and assessment across the community, and the levels at which these can be operated. This is a similar framework as used for the New Zealand Defence Force, where each component of the NZDF capability is described in some detail (such as Air Force or Army Capabilities for Joint Operations and Other tasks) along with levels of NZDF readiness for deployment.

*The unique contribution is the gathering of intelligence from sources that others cannot access, and building relationships with decision makers that enables the information to be best suited to their needs.*

The essence of this intelligence capability framework has been set out in the context of the Strategy, Capability and Resourcing Review (SCRR). Here an assessment is made on where the collective capability of the NZIC to mitigate New Zealand's risks against the desired performance level as set and funded by the Government for the period to 2020. A "Slider Scale" for each of the high intelligence priorities makes an assessment of the capability from "high risk/low protection" to "low risk/high protection". The capability in 2020 is briefly described for each of the intelligence priorities. The Slider Scale also lays out an assessment of the generic enablers of building the desired capability in terms of customer satisfaction, protective security, international relations and access, and organisational health (as covered in the discussion below).

The assessment of the progress with the development of each capability requirement is described in the material accompanying the progress on achieving the objectives of the increased investment and resourcing of the agencies. This sets out the steps taken and progress made, as well as planned future initiatives. An overall judgement is then made on the current capacity of each capability and shown graphically on the slider scale. In many instances the shifts in capability between 2013/14 and 2017 are quite small so far, and indicate the distance yet to travel.

The need here is to ensure that the judgements being made on changes in capability are backed as much as possible by well-developed statements of the desired end state. As presented, these look brief and high level and the capability assessment story would be better served by a deeper description of what is required to meet the intelligence priorities.

Then it needs to be matched by a stronger capability assessment methodology. We were informed that the capability assessment "position" on the slider scale was a matter of judgement and there was (at this stage) no specific science behind it. However, we understand that both qualitative and quantitative directorate performance

measures are in development and will feed directly into the capability assessment.

We have drawn out the relationship with the Five Eyes partners as a distinct but integral part of the capability assessment, and consider there would be value in making an assessment of this in its own right. This is because access to the broader capability of our partners requires a credible "threshold" capability level and contribution from New Zealand. We note that in the capability assessments made in the reporting on SCCR, there is sometimes reference to actions taken in conjunction with partners that enables increased reporting as a result of their contribution. That contribution enhances the New Zealand intelligence "product", but would not be available were it not for their confidence and recognition of the New Zealand capability in the first instance.

### Protective security

Protective security is not outlined as a distinct capability, but contributes to a number of the other capabilities discussed above. On these activities of NZSIS and GCSB, it is possible to assess how those services are delivered and to assess how well they meet the needs of the government agencies and the private sector that seek them. The Protective Security Requirements are mandatory requirements across core government agencies and require a self-assessment against standard criteria. The NZIC can therefore assess how well the public sector is placed in creating the desired state of protection and security for its people, information and services.

The vetting activities can be readily measured in terms of efficiency and timeliness for customers. In terms of effectiveness, this would require an assessment of the extent to which the levels of vetting contribute to the required operating environment.

On the cybersecurity and protective measures activities, these are delivered to government agencies and a wide range of other nationally significant organisations. There are other initiatives such as

the development of encryption infrastructure and engagement with telecommunications and other technology providers. The level of satisfaction with these services and advice can be measured in customer surveys. Furthermore, an independent quality assurance of a major cyber security investment has shown that the project was well managed and achieved its objectives.

### Compliance

A further set of measures of success is the degree to which the intelligence agencies are compliant with the law – and act lawfully in everything that they do. This might seem obvious, but the nature of the law is that it needs to be interpreted and applied in the circumstances of each specific case. The work of the intelligence agencies is scrutinised for compliance by the Inspector-General of Intelligence and Security who works within the agencies on a daily basis, and specific actions such as the issue of type 1 intelligence warrants are independently assessed by a Commissioner of Intelligence Warrants (who must have previously held office as a Judge of the High Court).

Therefore, any areas of non-compliance are subject to scrutiny and reporting by the IGIS who provides a certification of compliance in each year's annual report enabling a picture to be formed of the compliance culture within the intelligence agencies.

### Public trust and confidence

Related to the above measures on lawful activity and compliance, are measures relating to public trust and confidence. The agencies are working to build a stronger public engagement on what they do and why, and to be more transparent in their public reporting on activities and outcomes (through such things as the enhanced annual reporting regime). It will be further developed by a more active stance on discussing the risk environment and challenges for New Zealand. Ultimately this needs to flow through to finding measures on how that public trust environment is changing.

---

## Managing Growth

As referenced earlier in this report, the 2014 PIF was critical of how well the agencies were positioned to deliver then and in the future. The dimensions of leadership, direction and delivery were either rated as weak or needing development and people development and management were similarly rated. Decisions taken as a result of the SCRR led to an investment over a four year period of \$178.7 million. This is to address some of these long standing issues impeding organisational performance, and to make capability and capacity improvements to enable the agencies to better serve the domestic and foreign intelligence interests relevant to New Zealand's safety and security.

Growth in capability is different for each of the three agencies. For instance for DPMC SIG and the NZSIS it's primarily about people and skills whereas for GCSB it is people plus analytics and tools.

Sustaining high levels of new capability and growth is challenging for any organisation and no less so for the NZIC given both the nature of its work alongside the need to realise tangible benefits from the investment of tax payer's money. To manage the growth well with the agencies and across NZIC requires:

- regular reinforcement by the organisation's leaders of common purpose and mission;
- an unrelenting focus on people leaders and their role in ensuring 'how things are done around here' and the behaviours expected are made transparent to staff;
- a steely focus on delivering value to decision-makers coupled with strong engagement with customers and other stakeholders; and
- recognising the skills and talents of the workforce as a whole through a common set of values that underpin trust and respect for what others bring to the table and foster collaborative effort.

The agencies, especially NZSIS and GCSB, have done a lot to clarify mission and purpose and the sense of that amongst staff we spoke with was impressive. There is also appreciation

for the attention that has been given to getting the internal infrastructure better positioned for now and the future. However some believe that a downside of this means more work for managers. Getting some basic systems and processes in place does take time especially when they need to be brought up to a standard enjoyed by other public sector agencies.

The opportunity now is to build upon the foundations laid so that the agencies are well placed to realise the investment in increasing the core operational roles in national security and intelligence collection.

## Right Systems – Right People

Having the right systems in place along with easily accessible policies and processes are important stepping-stones to growing safely. As is good leadership and management practices accompanied by relevant training and coaching. Three areas that we highlight as being critical to get right over the next few years are recruitment, induction and retention.

## Recruitment

Attracting quality skilled candidates starts with the image, brand and information available publicly to potential applicants. Consistently managing recruitment as an end to end, two-way engagement from the moment an applicant files their interest in a role within the NZIC and how they are managed throughout the process is important to get right. While you are forming a view about the applicants, they too are gaining insights into the community and the agency they are interested in joining. Attracting the right talent and keeping them in the process which can be a very lengthy requires a lot of commitment on the part of an applicant and they therefore need to know where they stand at every step along the journey.

Tangible progress has been made in joining up the recruitment approach between NZSIS and GCSB and to improving the recruitment brand. However, given the competitive market for talent we believe there is scope to take this further. To get good quality candidates from a diverse range of backgrounds and experience to stay the course (in some instances up to

12-14 months to clearance point) is a challenge in itself. Candidates who get through the initial filter and are taken to the next stage would benefit from knowing more about what being employed in the community means and from receiving more regular communication as to where they stand in the process at key points.

*The agencies, especially NZSIS and GCSB, have done a lot to clarify mission and purpose and the sense of that amongst staff we spoke with was impressive.*

---

## Induction

An old adage of ‘first impressions count’ is very true for induction and how that is perceived by a new employee. With the number of new staff forecast to come on board and the strategy of attracting a greater diversity in background and skills it is timely to consider whether there are improvements to be made to how initial induction is approached. It would appear that there are opportunities to enhance the consistency with which people managers plan for and manage induction that would improve the overall experience of new staff. Given the complexity of the environment they are entering there is also a balance to be struck between learning about the environment and learning the job and avoiding information overload at the front-end. It would be worthwhile continuing to gain insights from recent recruits and separately from managers about their experiences of induction and applying those as a continuous cycle of improvement.

With the trajectory of approximately 50% growth in personnel over the 2016-2020 four-year period, a key metric for senior leadership teams is retention. Turnover rates for the agencies when compared alongside the need to expand staff numbers and operational capability are not currently as healthy as they could be. While we acknowledge that turnover statistics don’t tell the whole story, we were told anecdotally that factors that play into people leaving can include the role not being what was expected, dissatisfaction with a lack of reasonable levels of autonomy, and the current approach to trade craft training which is no longer seen as fit for purpose. These are in our view symptoms of organisations in

transition in which changes have been made, but are still to bed in and there is still more to do. However, turnover in any situation isn’t without cost both of managers’ time and lost investment in the person when they don’t stay.

## Retention

Recruitment, induction and training are core components to stabilising turnover and to avoiding a circular loop of opportunity lost and we believe this requires the ongoing attention of the senior leadership teams. In relation to tradecraft training, this by its nature will be a combination of ‘on the job’ and formalised learning. Getting the approach to this right is essential to lifting operational capability and being able to realise the benefits from the investment from SCRR. There are good practices that could be drawn upon from the intelligence sector and others for example, the Police have recently shifted to a more modulated method of training better suited to a modern workforce.

In summary, the management of growth is about right systems, right people and leveraging the combined talent, knowledge and skills of the community but also the wider security sector and the public sector ecosystem. The agency self-reviews fairly identify the significant advances made in addressing organisational weaknesses, and the challenge now is to take a deliberate planned and purposeful approach to attracting and retaining quality talent. Intelligence Community Shared Services, the JDGO and the recent establishment of the new Capability Directorate within NZSIS are all still in formative stages but are key to supporting a sustained lift in organisational performance if utilised consistently well.

*The management of growth is about the right systems, right people and leveraging the combined talent, knowledge and skills of the community but also the wider security sector and the public sector ecosystem.*

---

# Appendix

## Lead Reviewers' acknowledgement

We wish to acknowledge the leadership and staff of the Government Security and Communications Bureau, New Zealand Security Intelligence Service and the Department of the Prime Minister and Cabinet for their engagement on this review. Their input was open and thoughtful and they gave generously of their time. We would also like to acknowledge the feedback and insights from a wide range of external parties and stakeholders of the New Zealand Intelligence Community. We much appreciated the assistance given to us by Jacqui T, NZSIS and Josh Tendeter, SSC.

**Sandi Beatie**  
Lead Reviewer

**Geoff Dangerfield**  
Lead Reviewer

Note: Sandi Beatie took a formal leave of absence from her role on the Risk and Assurance Committee for the Department of the Prime Minister and Cabinet to avoid any potential conflict of interest in the lead up to and for the duration of the PIF Follow-up Review.