Te Pourewa Mātaki
Inspector-General of Intelligence and Security

ANNUAL REPORT 2024-2025

Brendan Horsley
Inspector-General of Intelligence and Security
October 2025

CONTENTS

FOREWORD

I am pleased to present my office's annual report for 2024-2025.

This period has been defined by a complex and challenging global security environment. The challenges include the proliferation of conflicts, the rise of state-sponsored interference and the rapid evolution of technology. New Zealand is not unaffected by this global dynamic and the intelligence and security agencies are rightly focused on these threats. Unsurprisingly the activities of the agencies in those areas have also been the focus of my independent oversight.

The public's trust in our intelligence services is critical to their mandate and this trust is earned through transparency and accountability. This report details the work undertaken by my office to ensure the NZSIS and the GCSB continue to act in way that is proper, lawful and consistent with New Zealand's values. I am pleased to report no major concerns with the conduct of the agencies. There are always areas that can be improved but New Zealanders can be satisfied that, over the period of this report, the agencies have continued to conduct their activities lawfully and with propriety.

On another note, this past year was notable for a significant change in New Zealand's wider oversight architecture: the establishment of the first Inspector-General of Defence. I was honoured to be appointed to this role, on an interim basis, to set up the new office with systems, processes and people. There are important and valuable synergies between the offices of the IGIS and the IGD. I expect the offices will work closely together as the only oversight bodies working predominantly with classified material. The offices also have complementary areas of interest in overlapping activities of the agencies and the NZDF, such as, intelligence support to military operations and the security of the South Pacific. Having both an IGIS and IGD will reinforce the integrity of our national security framework, ensuring independent oversight across a wider scope of government activity.

Brendan Horsley
Inspector-General of Intelligence and Security

THE OFFICE OF THE INSPECTOR-GENERAL

The Inspector-General of Intelligence and Security (IGIS) provides independent oversight of New Zealand's two intelligence and security agencies:

- the Government Communications Security Bureau (GCSB or 'the Bureau'); and
- the New Zealand Security Intelligence Service (NZSIS or 'the Service').

The office of the IGIS is independent of the NZSIS, the GCSB, and the Minister(s) responsible for the intelligence and security agencies.

The functions, duties and powers of the IGIS are set out in the Intelligence and Security Act 2017 (ISA).

The purpose of oversight by the IGIS is to ensure the agencies operate lawfully and in a manner New Zealanders would think proper.

To this end, the IGIS:

- investigates complaints about the agencies;
- conducts inquiries and reviews into activities of the agencies;
- reviews intelligence warrants and other authorisations issued to the agencies;
- assesses the soundness of the agencies' compliance systems;
- receives protected disclosures ('whistleblower' disclosures) relating to classified information or the activities of the agencies; and
- advises the Government and the Intelligence and Security Committee of Parliament on matters relating to oversight of the agencies.

The IGIS does not assess the operational effectiveness of the agencies.

SIGNIFICANT ISSUES IN 2024-2025

Protected disclosures

In 2024 several current or former NZSIS employees raised with me closely-related criticisms of past operations and conduct in a particular branch of the Service. It was the first instance of my office handling any matter under the Protected Disclosures (Protection of Whistleblowers) Act 2022.

Under that Act, I am the appropriate authority for receiving protected disclosures that include intelligence and security information. In the whistle-blowing context, my remit is not restricted to the agencies I oversee; a protected disclosure can come from anyone who needs to disclose a matter that involves classified material. I can protect both the information disclosed and the anonymity of a discloser while I investigate matters (or refer them, if I am not the right person to investigate). Importantly, the law protects disclosures made in good faith even if the receiving authority does not find that any serious wrongdoing has occurred.

In this case, I considered that on their face some of the matters disclosed could have amounted to serious wrongdoing within the meaning of that term in the Protected Disclosures Act. I accepted the disclosers were genuinely concerned and were acting in good faith. Over time, I gathered details from them and it became clearer that the disclosures were predominantly about leadership, financial management, operational capability, and health and safety risks. If borne out they were matters that would require management action rather than investigation by me. Accordingly, and with the agreement of the disclosers, I put the issues to the NZSIS's Director-General.

Through ongoing engagement with the Service I found that some of the matters raised were recognised, some disputed and some difficult to verify. Overall, most involved strong differences of opinion about what constituted appropriate operational practice and risk tolerance. I sought assurances from the Director-General that certain matters (eg some financial management issues) had, or would be, addressed. I consulted with the Office of the Auditor-General to ensure it was aware of relevant matters. Finally, I wrote to the Minister to set out the allegations, the agency's responses, and my conclusions.

I found ultimately that none of the conduct involved would meet the statutory definition of serious wrongdoing. The agency engaged positively throughout.

New Zealand's intelligence community is small, and making a disclosure comes with personal and professional risk. The disclosers in this instance were motivated, in my view, by a genuine wish to see improvements they believed necessary. The protected disclosures regime enabled them to raise issues that deserved to be taken seriously. To that extent I think the process showed its value.

Intelligence sharing relating to armed conflict

In September 2024 I received a request from three public lawyers to open an inquiry into whether, through sharing intelligence, New Zealand's intelligence agencies might have "contributed to the commission of international crimes by Israel in the Gaza strip". That request reasonably sought assurance that the intelligence agencies were not making New Zealand directly or indirectly complicit in activities that could violate international human rights law or the law of armed conflict.

I had already signalled in both my 2023-24 annual report and my 2024-25 work programme that any armed conflict-related intelligence activity would be an area of particular focus for my office, given the war in Ukraine and conflict in Gaza, Yemen, Lebanon and the wider Middle East. At the time of receiving the request for an inquiry, my office had been monitoring relevant intelligence sharing for some months. I was not sure therefore, that an inquiry would significantly add to what I knew.

An inquiry is useful when a structured investigation into past activity is necessary. But an inquiry necessarily 'stops the clock' to examine what has already happened. The grave humanitarian catastrophe in Gaza is ongoing, as are other conflicts in the Middle East and the war in Ukraine.

I decided in favour of continued monitoring rather than an inquiry. Before I made that decision, I asked both intelligence agencies to provide summaries of any forms of intelligence sharing that could potentially be relevant to the request. Their responses were consistent with what I expected to receive, given the findings of my office's independent scrutiny of their records.

The agencies can legitimately share intelligence with foreign counterparts, including where that contributes to the safety of New Zealanders and New Zealand forces overseas or helps meet New Zealand's international obligations and commitments – such as countering terrorism. In doing so, they must operate in accordance with New Zealand law and all human rights obligations recognised by New Zealand law. Their work must also be amenable to oversight. They therefore have policies and procedures requiring them to assess and record, case by case, any human rights risks arising. They must also obtain authorisations from their Minister to share intelligence, and satisfy the Minister that they will meet their legal obligations. This promotes Government accountability for significant decisions about who New Zealand does and does not share intelligence with, and in what circumstances.

Over the past two years I have directed much attention at the processes and procedures the agencies rely on to identify and manage the risk of complicity in human rights abuses, and how they obtain authorisations for international cooperation from the Minister. My office continues to monitor intelligence sharing related to current international conflicts and I routinely obtain updates from the heads of both agencies about how they are responding to current events. So far, I am satisfied with the information I have from this approach, which has not raised concerns that would prompt an inquiry. This does not preclude conducting an inquiry in future, if necessary, and I will continue monitoring relevant intelligence sharing over the coming year.

Use of class warrants

In my past two annual reports I raised concerns about the NZSIS's use of class warrants, particularly for intelligence investigations strongly focused on individuals. My concern, in short, was that a class warrant cannot, by its nature, set out the particular case for action against a specific person. In March 2024 I reported publicly on a series of warrants issued to the Service in 2022 and 2023 authorising it to target classes of individuals in the context of counter-terrorism and violent extremism. These warrants exemplified the concerns I had.

In the past year I have been pleased to see the Service increasingly seeking individual warrants for investigations of individual targets. The last iteration of the series of warrants that had particularly concerned me has expired. At time of writing there has not been another (though the agency has not

ruled out a further application). The individual warrants sought and issued instead have, as expected, set out more clearly and effectively the justifications for the intrusive powers sought.

My office continues to review all warrants issued to both agencies and I have a review of the execution of class warrants in train. That review examines how both agencies assess whether people come within the definition of a class in a warrant and how they decide which authorised activities to carry out. I expect to conclude it in the coming year.

Review of the Intelligence and Security Act 2017

As in the past two years, I have continued to engage with the Department of the Prime Minister and Cabinet (DPMC) on the policy response to the first independent review of the Intelligence and Security Act (ISA), which was published in May 2023.

I have a particular interest in what the response will be to the reviewers' recommendation 26, to amend the Act to clarify the scope for the NZSIS to issue warnings, as this has been the subject of reports by both my predecessor and myself. I have a related close interest in the answer to the reviewers' recommendation (recommendation 27) that policy work should be doneto determine whether the Act should be amended to include an ability for one or both intelligence agencies to undertake "threat disruption" activities, beyond giving warnings, and if so with what safeguards and oversight. Currently the scope for "disruption" is limited by section 16 of the ISA, which provides that the agencies have no function "to enforce measures for national security", with narrow exceptions for information and cybersecurity activities by the GCSB and actions where the agencies work with the Police or Defence Force and may help execute powers held by them.

I expect my engagement with DPMC to continue in the coming year.

Agency compliance systems

Each year, as the law requires, I certify in this report "the extent to which each intelligence and security agency's compliance systems are sound". Since 2019-20 my office has used a framework that identifies five broad components of an agency compliance system and the elements of each. In each component an agency's system can be rated from *inadequate* to *strong*.

In the past two years I assessed both agencies as having under-developed operational policy and procedure, largely for having substantial proportions of their policies overdue for review.

This year again I assess both agencies as having under-developed operational policy and procedure. Systemic, regular and proactive management of policies is necessary to avoid reliance on expired documents and a continuous backlog of policies overdue for review. I cannot yet assess the agencies as 'well-developed' because neither has yet embedded a well-maintained approach to managing their policy suites over the longer term. As I acknowledged last year, both are making efforts to remedy this. They have made progress, though it has not been rapid and the task remains substantial. I discuss each agency in more detail in the assessment at the end of this report, but restructuring has likely been a limiting factor in the past year for both.

As I have noted before, internal policies have particular importance in intelligence and security as, to preserve secrecy, the legislation does not specify how the agencies are to conduct the agencies'

activities with the degree of detail found in law governing other government departments. Nor is there an extensive body of decisions from the Courts, or other appeal or review bodies, binding the agencies' conduct. I will continue therefore to keep a critical eye on progress in this area.

In last year's report I assessed the NZSIS's internal compliance programme as under-developed, noting in particular a persistent inability to complete its internal audit programme. In the past year the Service has improved in areas I previously highlighted as deficient. It created a simple compliance strategy (endorsed by senior leadership) and a work plan to deliver against that strategy. An updated compliance framework was finalised after a lengthy review. The compliance team benefited from having a specialist compliance and policy advisor in place. The agency's audit plan, though modest, was substantially completed, with audit outcomes and recommendations tracked and reported to leadership. Investigation and reporting of compliance incidents continued at reasonable pace despite structural changes and staffing pressures. I have revised my assessment this year therefore to well-developed – noting that this means further improvements are still required, but I have more confidence they will be made.

INQUIRIES AND REVIEWS

Under the ISA, I can inquire into the lawfulness and propriety of particular GCSB and NZSIS activities. For an inquiry, the Act provides investigative powers akin to those of a Royal Commission of Inquiry.

Reviews of operational activity are a substantial component of my office's regular work programme. They are generally less formal than inquiries and aim to ensure my office has a good understanding of agency operations, recommending improvements to compliance systems where necessary.

As far as possible, I report publicly on inquiries and reviews. Where there is limited scope for public reporting due to security classifications, a review might be summarised only in my annual report.

Completed or closed in 2024-25

Inquiry into complaint from a journalist into the actions of NZSIS

I received and inquired into a complaint from New Zealand journalist Mick Hall that the NZSIS had apparently investigated and reported on him after he was publicly accused of 'pushing a false Russian narrative' when sub-editing news stories. I found the Service had made initial enquiries in response to public reporting on the matter, concluded there were no concerns of foreign interference and reported accordingly. I was satisfied the NZSIS's enquiries were legal and proper, given its responsibility for investigating foreign interference, and that the agency had properly recognised the sensitive nature of enquiring into a journalist. It was appropriate, given the public allegations of foreign interference, that the Service reported its conclusion that Mr Hall was not engaging in any form of state sponsored foreign interference.

Although I do not normally name complainants in public reporting, in this case the matter was very much in the public domain, including as a result of Mr Hall publishing on it himself. I published an unclassified account of my findings on my website.

Review of NZSIS human source recruitment and management

I completed a classified report on a review of the NZSIS's recruitment and management of covert human intelligence sources and published a summary on my website. These sources are recruited and managed by specially trained NZSIS officers. Human source operations are tightly controlled, as they can involve high risks to the sources, Service officers and the reputations and relationships of the NZSIS and the Government.

I found that the Service generally complied with its policies and procedures on recruitment and management of human sources. These are the main controls on human source activity, as most of it is lawful and conducted without any need for an intelligence warrant.

On rare occasions, the NZSIS may seek a warrant to provide some immunity for a source who might need to participate in unlawful conduct for the purposes of maintaining cover. My review examined a case where, in my view, the intelligence warrant application could have been clearer as to the scope of the possible offending it anticipated. I advised the NZSIS to ensure it is clear about the nature of any criminal acts it seeks to cover, so it can be equally clear to its source about the immunity available.

In the case studies reviewed, I found variable practices in recording assessments of source welfare and I encouraged the NZSIS to do this more consistently. Other NZSIS records of human source management were generally reasonable, but I noted some instances where record keeping did not follow policy and procedure.

Review of GCSB's collection of intelligence on transnational organised crime

I reviewed how the GCSB collects and analyses intelligence on transnational organised crime. This work supports other agencies with responsibilities for investigating serious transnational criminal offending, including the New Zealand Police and the New Zealand Customs Service.

I found the GCSB's conduct in countering serious and organised crime was consistent with its intelligence collection and analysis function. It had clear authorisation protocols and effective processes for managing collection and reporting. I found no issues in how the GCSB collaborated with other agencies, noting only one instance where the GCSB could have better documented a decision regarding support to a domestic agency.

Overall, I found GCSB kept good records of its intelligence collection and sharing on transnational organised crime. My review did not result in any recommendations.

Review of GCSB target discovery activities

My review of how the GCSB conducts target discovery activities, proposed in the 2022-23 work programme, began in 2023. I examined the legal basis for conducting target discovery; the policies and procedures guiding it; how the activity was conducted; the GCSB's application of safeguards including assessment of necessity and proportionality; and the appropriateness and effectiveness of the GCSB's compliance controls.

GCSB target discovery is focused on generating leads and resolving identities for further investigation. The activity I observed was narrower than NZSIS discovery activity (which I reported publicly on in August 2024). This was expected and appropriate given the Service's particular focus on domestic threats. I examined examples of GCSB discovery activity and found appropriate policies and processes in place to manage the types of discovery work undertaken. The authorisation framework effectively ensured discovery activity was lawful, compliant with policy controls, and amendable to oversight. Staff were diligent in their record keeping.

While I made no recommendations at the outcome of my review, I alerted the GCSB to the need for ongoing monitoring of the aggregate development of discovery projects to ensure activity remains necessary and proportionate and is routinely subject to review.

Review of GCSB raw data sharing with partner agencies

I completed a report on a review of GCSB systems and procedures for sharing raw (unevaluated) data with partner agencies, which at year end was with the Bureau for any final comment. This long-running review has examined technical arrangements for sharing raw data and a complex history of agreements, arrangements and authorisations. The scope for public reporting is very limited but I will assess that, in consultation with the GCSB, in the coming year.

Ongoing

Review of the agencies' use of artificial intelligence

At year end I was near completion of the second part of this review, which examines the current or planned use of artificial intelligence by the NZSIS and GCSB. This includes their policies, practices, and governance systems, alongside any technology in use. I expect to finalise a report in the coming year.

My first report, published on my website in August 2024, covered the state of regulation and governance of AI from an intelligence perspective, including international and domestic frameworks.

Review of NZSIS and GCSB election-related activities

Foreign interference and malicious cyber activity are possible threats to the integrity of general elections. The intelligence agencies have a role in identifying, assessing and reporting on relevant activity. At the same time they are obliged by law to be politically neutral (section 18 ISA) and to respect the right to freedom of expression, including the right to advocate, protest or dissent (section 19). I am reviewing how the agencies understand political neutrality and what policies and practices they have to ensure compliance with s 18 ISA, focusing on activity in relation to the 2023 general election. I expect to finalise a classified report on this review in the first part of the coming year.

Review of the agencies' execution of class warrants

A class warrant enables otherwise unlawful intelligence activities against a class of persons, rather than a specific individual. In 2023-24, I began a review of how both agencies operate under class warrants, including how they determine whether a person falls within a class, how they review those determinations, and what controls they have to ensure compliance with warrants, policies and procedures. I expect to finalise a classified report on this review in the first part of the coming year.

Review of NZSIS online intelligence operations

Late in 2023-24, I began a review of a specific form of online intelligence gathering undertaken by the NZSIS. I expect to conclude this review in the coming year.

Review of NZSIS use of Business Records Directions

Business Records Directions (BRDs) can be issued by the intelligence agencies under the ISA to obtain business records from telecommunication and financial service providers (eg telephone call metadata and bank statements) in specified circumstances. Early in 2025, I began a review of the NZSIS's use of BRDs. I expect to finalise a classified report on my findings in the coming year.

New Zealanders and international terrorist screening (NZSIS)

In 2023-24, my office began examining the NZSIS's engagement with international terrorist screening databases, including 'No Fly' lists, in relation to the inclusion, review and removal of New Zealanders. I am now reviewing this activity and expect to engage with the NZSIS on a draft report in 2025-26.

COMPLAINTS

Investigating complaints against the agencies is a core function of my office. Any New Zealand citizen or person ordinarily resident in New Zealand, and any employee or former employee of the agencies, may complain if they have or may have been adversely affected by an act, omission, practice, policy or procedure of the GCSB or the NZSIS.

An inquiry into a complaint must be conducted in private and the complainant must be told of the outcome in terms that will not prejudice national security, defence or international relations. This means not everything discovered by a complaint investigation can be reported, either to the complainant or publicly.

Throughout the year, my office is contacted by people expressing concern that they are under some form of covert surveillance or attack. Many of these are effectively queries about what information, if any, the agencies hold on the person concerned. The most appropriate first step is generally to direct the query to the relevant agency or agencies, as requests for personal or official information under the Privacy Act 2020 or Official Information Act 1982. There is then a right of complaint to the Privacy Commissioner, Ombudsman or my office if the response is unsatisfactory.

In general, the Service is the subject of complaints more often than the Bureau because it operates more domestically and does large numbers of security clearance (vetting) assessments. The following table shows complaints received by my office in 2024-25:

Complaints 2024-25				
Received from	**About GCSB**	**About NZSIS**	**About Both**	**Total**
Members of the public	2	15	3	20
Intelligence agency employees/former employees	1	1	0	2
Total	3	16	3	22

The total number of complaints received in 2024-25 was the same as in 2023-24. In most cases preliminary inquiries showed no further investigation was necessary, but four complaints required investigation. Three were about the NZSIS: the journalist's complaint discussed earlier in this report; one I did not uphold; and one that was resolved to the satisfaction of the complainant without any need for formal recommendations. The fourth complaint was about both agencies and on investigation I was satisfied the matters raised had already been addressed by internal review.

My office also received and dealt with a further 25 enquiries seeking information or raising issues that did not amount to complaints within my jurisdiction.

WARRANTS

In this reporting year my office reviewed 42 warrants issued to the agencies, close to the 44 reviewed last year.

An agency may seek a Type 1 warrant to carry out an otherwise unlawful activity to collect information about, or do any other thing directly in relation to a New Zealander (a citizen or permanent resident) or a class of persons that includes a New Zealander. It requires the approval of the Minister responsible for the agency seeking the warrant, and a Commissioner of Intelligence Warrants. A Type 2 warrant is sought when a Type 1 is not required (ie the agency is not targeting a New Zealander). The Minister alone issues Type 2 warrants. There are special procedures for authorising warrantable activities in urgent and very urgent circumstances.

This year neither agency sought an urgent warrant or a very urgent authorisation.

	Type 1 warrants	Type 2 warrants	Practice warrants	Removal warrants	Total
NZSIS	16	1	2	0	19
GCSB	12	10	1	0	23
Total	28	11	3	0	42

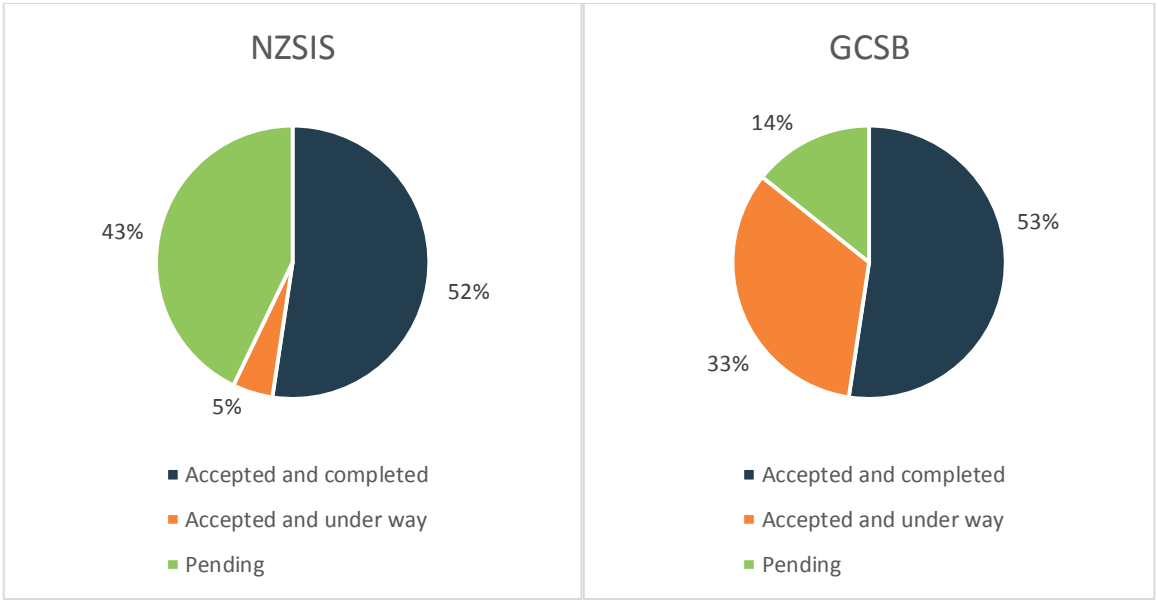
The ISA allows an agency to apply to the Minister and a Commissioner of Intelligence Warrants for a Business Record Approval (an Approval), which authorises the agency to issue orders (Business Records Directions) to obtain business records from telecommunications providers and financial services providers in specified circumstances. Each agency was issued (and my office reviewed) two Approvals this year.

An agency may also apply to the Minister and (for an application involving a New Zealander) the Chief Commissioner of Intelligence Warrants for access to restricted information, eg information held by Inland Revenue, or driver licence photos stored under section 28(5) of the Land Transport Act 1998. Neither agency applied for access to restricted information this year.

IMPLEMENTATION OF IGIS RECOMMENDATIONS

I often make recommendations to the agencies following an inquiry or review. These are non-binding, but I seek to ensure they are practicable to implement, valuable and promote compliance with the ISA. I seek and generally receive agreement from the relevant agency on my recommendations. The time taken by an agency to implement recommendations varies. Minor changes to policy are easier and faster to implement than recommendations for systemic change. If an agency rejects one of my recommendations, that does not necessarily mean the agency is non-compliant with the ISA or the underlying activity was unlawful.

The review and inquiry recommendations tallied below are from the last three financial years (2022-23 to 2024-25). Implementation of an accepted recommendation is "under way" if work is in progress to give effect to it, or "pending" if such work has yet to begin. One recommendation to the GCSB, for an audit to be done, was accepted but not implemented as the GCSB subsequently determined it could not obtain the necessary data.



Status	NZSIS	GCSB	Total
Accepted and completed	11	11	22
Accepted and under way	1	7	8
Pending	9	3	12
Not implemented	0	1	1
Total	21	22	43

OUTREACH AND ENGAGEMENT

Advisory Panel

The ISA establishes an Advisory Panel of two people to provide objective and informed advice to the Inspector-General. The Panel does not have an oversight or governance role but can provide advice on request, or on its own motion.

In the past year Lyn Provost, a former Controller and Auditor-General, left the panel having served on it since 2018. The office has benefited greatly from Lyn's experience and counsel over the years.

The panel is now chaired by Ben Bateman (Ngāi Tahu, Cook Island Māori), who has been a member since 2021. Ben has an extensive background in law and governance in the public sector and is currently Kaihautū (chief executive) of Te Rūnanga o Ngāi Tahu.

Melanie Matthews joined the panel in the past year. Melanie brings extensive governance and advisory experience from both the public and commercial sectors in New Zealand and the United Kingdom. She specialises in governance with a particular focus on the impact of geopolitical risk on organisational strategy.

The Advisory Panel met four times in the reporting period. I have valued their insight and advice.

Other integrity agencies

I participate in the Intelligence and Security Oversight Coordination Group with the Privacy Commissioner, the Chief Ombudsman, and the Auditor-General. Each of us has a role in oversight or scrutiny of the intelligence and security agencies. It has proved useful to manage possible areas of overlap in our responsibilities and broader issues of common interest.

Foreign oversight counterparts

The Five Eyes Intelligence Oversight and Review Council (FIORC) comprises the non-Parliamentary intelligence oversight and review bodies of the UK, USA, Canada, Australia, and New Zealand. FIORC enables us to exchange views on subjects of mutual interest and concern, compare oversight methodology and explore possible cooperation. In November 2024 I attended the FIORC annual conference in Canberra.

Commissioners of Intelligence Warrants

My office engages with the Commissioners of Intelligence Warrants occasionally on matters of mutual interest. Commissioners also join my office in attending the FIORC annual conference.

External engagement

I welcome opportunities to engage with the public, community groups and the public sector about the role of the Inspector-General. This year I accepted ten speaking opportunities, to academic, public service, and intelligence sector audiences. Staff in my office regularly attend conferences and events related to our work, eg on security, geopolitics and technology in the national security sector.

FINANCES AND ADMINISTRATION

Funding and resourcing

The IGIS Office is funded through a Permanent Legislative Authority, covering the remuneration of the Inspector-General and Deputy Inspector-General, and Vote Justice, covering operating costs (as a non-departmental output expense). Total expenditure for 2024-25 was 21.3 percent under budget, mainly due to temporary vacancies while new investigators were recruited to replace departing staff. At year end the office had a total staff of seven: the Inspector-General and Deputy Inspector-General, an office manager and four investigators (3.27 FTE), with one further investigator appointed but not yet at work.

Office of the Inspector-General of Intelligence and Security 2024-25 Budget		
	Actual ($000)	Budget
Staff salaries, advisory panel fees, travel	510	832
Premises rental and associated services	361	373
Other expenses	26	124
Permanent Legislative Authority	699	700
Total	1596	2029

Premises and systems

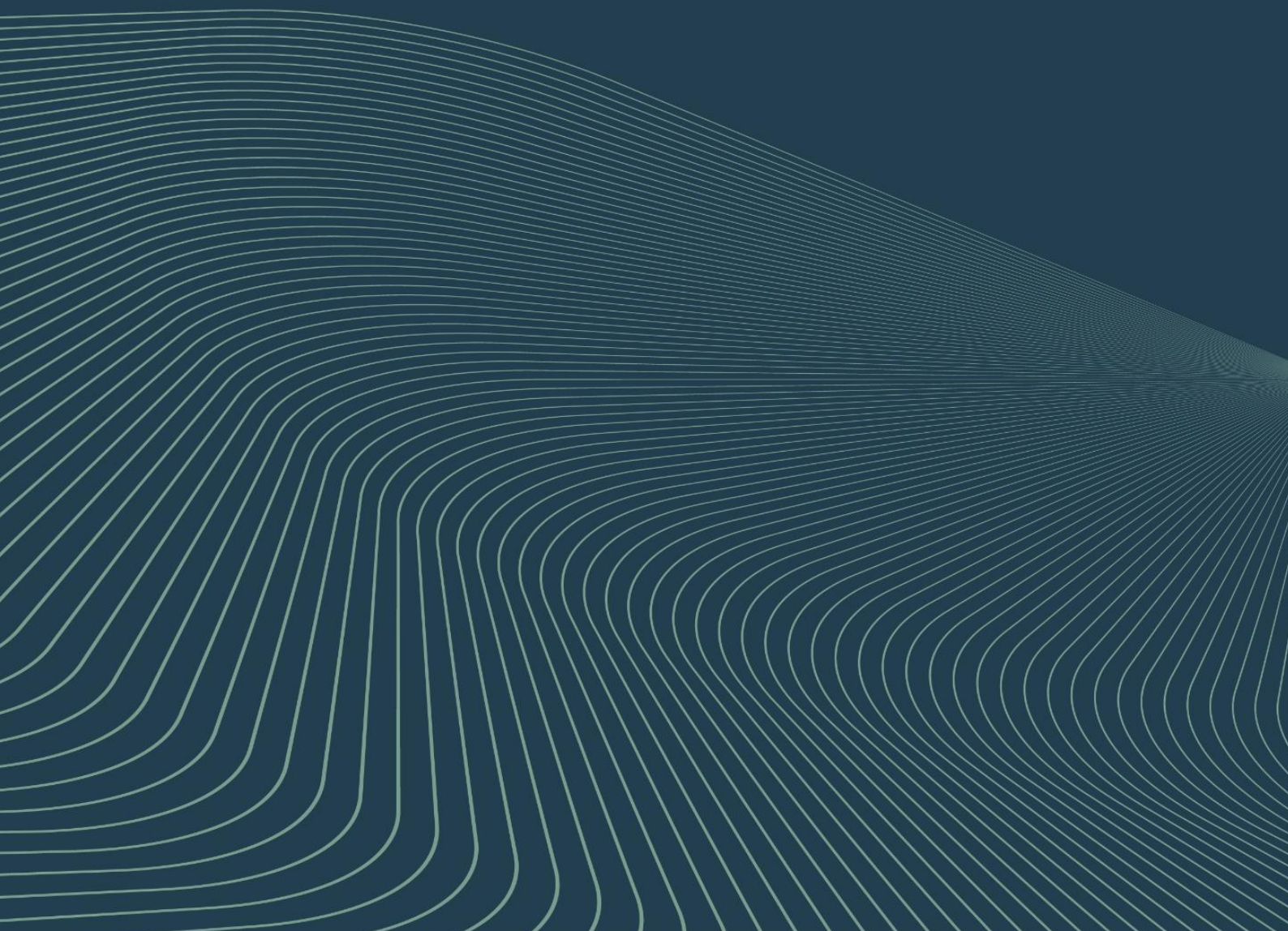
Since 2019 my office has operated from secure premises in Defence House, Wellington.

The office operates a highly secure computer network, in accordance with the requirements of the New Zealand Information Security Manual.

Administrative support

The New Zealand Defence Force provides IT support to the office, for some of our systems, on a cost-recovery basis. The Ministry of Justice also provides some administrative assistance, including finance, communications and human resources advice and support. These arrangements are efficient and appropriate given the size of the office. I am grateful for the ongoing assistance of the Ministry of Justice and the New Zealand Defence Force.

CERTIFICATION OF COMPLIANCE SYSTEMS



CERTIFICATION OF COMPLIANCE SYSTEMS

The ISA (s 222) requires me to certify in my annual report "the extent to which each agency's compliance systems are sound". This is not a certification that everything the agencies' have done has been lawful and proper, but an assessment of their approaches to minimising the risk of illegality and impropriety.

For this assessment, my office uses a multi-factor template, rating the compliance systems of each agency on five main headings. The headings, guiding questions and relevant factors in our assessment are set out below. This report provides a summary of my assessments for each agency, along with a rating for each of the five areas assessed.

Operational policy and procedure

Does the agency have a robust and readily accessible suite of policies and procedures providing guidance for staff on the proper conduct of its operations?

Maintaining this generally requires:

- clear and coherent documentation
- well organised and effective dissemination of policies and procedures
- specialist policy staff
- a programme of policy review
- timely remediation of any deficiencies in policy or procedure.

Internal compliance programmes

Does the agency have an effective internal approach to the promotion of compliance?

This will generally require:

- a compliance strategy informed by best practice and endorsed by senior leadership
- specialist compliance staff
- a rigorous programme of compliance audits, covering significant functions and risks
- timely remediation of any shortcomings found by audits
- regular reporting to senior leadership and IGIS on compliance issues, statistics, trends and corrections
- proactive measures to maintain or improve compliance.

Self-reporting and investigation of compliance incidents

Does the agency encourage self-reporting of compliance issues?

An effective approach to self-reporting will generally involve:

- promotion of compliance self-checking as part of normal operating procedure
- established policies and procedures for responding to compliance issues

- a supportive (rather than punitive) response to self-reporting of compliance issues and errors
- timely, thorough investigation and remediation of self-reported issues and errors
- timely reporting of compliance incidents to the IGIS.

Training

Does the agency train staff effectively in their compliance obligations?

This will generally require:

- a training strategy including comprehensive induction and refresher training programmes
- a systematic approach to assessing the effectiveness of training and identifying new or revised training needs
- a dedicated training capability, typically requiring specialist staff and facilities.

Responsiveness to oversight

Does the agency respond appropriately to the Inspector-General's oversight?

This will generally require:

- open, constructive and timely engagement with the office of the IGIS
- timely articulation of an agency position on any compliance related legal issues arising
- commitment of resources to deal with the requirements of IGIS inquiries and reviews
- timely and effective implementation of accepted IGIS recommendations.

For each heading, I assign a rating from a simple four-level scale:

Rating	Summary of Rating
Strong	Systems are mature, well maintained and effective. Any issues or shortcomings are minor, recognised by the agency and remediation is imminent or under way.
Well-developed	Systems are predominantly well developed, well maintained and effective, but there needs to be some change to make them fully sound. Necessary improvements are in development and/or require further time and resourcing to implement.
Under-developed	Systems require significant change to function effectively. Necessary improvements require substantial planning and resourcing and may require medium to long-term programmes of change.
Inadequate	Systems are critically deficient or about to become so.

GCSB Compliance System Assessment for 2024-25

Heading	Rating
Operational policy and procedure	Under-developed

The GCSB is revising its approach to measuring policy effectiveness. Though not yet embedded, the new approach will prioritise reviewing policies that directly relate to known organisational risks and compliance issues. A significant amount of work has gone into aligning policy and procedures to support the integration of CERT NZ and the National Cyber Security Centre (NCSC) and to review policies shared jointly with the NZSIS. In the past year the GCSB planned a reorganisation of policies, making them easier for staff to browse and access. Despite on-going progress, however, there is still limited evidence of a well-maintained and effective system to manage policy and procedures in the long term.

Heading	Rating
Internal compliance programmes	Well-developed

The GCSB has a mature compliance team that includes specialist policy and audit staff. Audit plans and a compliance strategy are in place and staff track and report progress against plans and objectives. Routine audit functions are integrated into daily operations. There is some proactive work to identify emerging and future compliance challenges. Organisation and staff changes may have impacted capacity, but the internal compliance programme continues to work effectively.

Heading	Rating
Self-reporting and investigation of compliance incidents	Well-developed

At the GCSB information on identifying and reporting compliance incidents is readily available to staff and compliance culture is well promoted. The Bureau has current procedures and policies in place to guide how compliance incidents are handled. Compliance checks are embedded into how teams work. Compliance investigations are sometimes lengthy and process changes or remediation can be incremental and slow. For incidents the GCSB reports to my office, the average time between an incident being identified and my office receiving notice of that incident is three months, with some notifications taking four to six months.

Heading	Rating
Training	Well-developed

The GCSB has mandatory compliance training for operational staff and requires regular re-certification to ensure staff remain aware of changing legal or policy obligations. The agency shares a dedicated learning and development team with the NZSIS. This year organisational change was a priority, with limited capacity to focus on strategic planning or training reviews and improvements.

Heading	Rating
Responsiveness to oversight	Well-developed

The Bureau is receptive to my oversight. Responses to questions or requests are constructive but can be slow. Most of the work in engaging with my office falls to legal and compliance staff, who facilitate reviews and respond to queries about warrants, incidents or issues. Some of the issues arising from the GCSB's work involve complex technologies and systems that can present challenges for visibility and review. The Bureau makes expert staff available to assist my office in understanding technical capabilities and their implications.

NZSIS Compliance System Assessment for 2024-25

Heading	Rating
Operational policy and procedure	Under-developed

The NZSIS has a programme of work to improve policies and standard operating procedures. It continues to track and report on the progress made against the plan. Policies and procedures are readily accessible to staff. This year the number of policies overdue for review remained steady at approximately one third of the total. Organisational change may have delayed some progress, especially as policies were re-allocated to new owners. I anticipate improvement as NZSIS embeds systems to ensure its policy suite remains current and fit-for-purpose.

Heading	Rating
Internal compliance programme	Well-developed

Despite resource constraints and pressure from organisational change the NZSIS has made progress in remedying some issues raised in my previous reports. A concise compliance strategy, compliance work plan and audit plan are in place. In the coming year, stable staffing should enable the Service to review and track progress against that plan. In 2024-25 the Service reviewed and updated its compliance framework. Three of four planned internal audits were completed and one nearly so. The Service tracks progress on audits and the implementation of audit recommendations, reporting regularly to senior leadership. Separating strategic risk management from the compliance team may enable compliance and audit staff to focus more exclusively on their functions.

Heading	Rating
Self-reporting and investigation of compliance incidents	Well-developed

The NZSIS benefits from an experienced senior compliance advisor and the support of the legal team in assessing and investigating compliance incidents. Policies and procedures for reporting incidents are clear, current and easily accessed by staff. The Service notifies my office of serious incidents or breaches of legislation in a timely manner, usually within a month of the incident's identification. Any questions arising from incidents are resolved promptly. Where reporting of incidents indicates an issue or trend, the NZSIS uses this information to inform its audit planning.

Heading	Rating
Training	Well-developed

The Service has dedicated operational training staff, as well as learning and development staff and systems (shared with GCSB). Induction and essential compliance training is mandatory. I have previously reported concerns about the NZSIS's limited capacity to evaluate the effectiveness of training across the breadth of operational activities, potentially raising a risk of staff being unaware of legal or compliance obligations. In the past year the NZSIS completed a comprehensive operational training review, resulting in a number of sound observations and recommendations. These have yet to be implemented as a restructure took priority, limiting capacity for training needs assessment or re-design.

Heading	Rating
Responsiveness to oversight	Well-developed

The NZSIS's relationship with my office is open and constructive. The Service facilitates access to its records and contacts for complaints, reviews, and inquiries. Questions are answered in a timely way. The NZSIS is often proactive in sharing information about its work, including routinely providing copies of compliance updates or briefings on system changes. The NZSIS is especially responsive to requests regarding complaints, which helps my office to investigate thoroughly and respond quickly to complainants.

Te Pourewa Mātaki
Inspector-General of Intelligence and Security