Te Pourewa Mātaki
Inspector-General of Intelligence and Security

ANNUAL REPORT 2023-2024

Brendan Horsley
Inspector-General of Intelligence and Security
October 2024

CONTENTS

FOREWORD

I am pleased to present my office's annual report for 2023-24.

This year saw the completion of a number of inquiries and reviews that were on-going from the 2022-23 year. In particular, we completed reviews into the agencies' support to military operations and their use of human rights risk assessments. Both reviews were timely given the conflicts in the Ukraine and Middle East.

As I said in my Work Programme for the forthcoming year: "The New Zealand agencies can produce intelligence of value to participants in international armed conflicts; collect intelligence relevant to the security of New Zealand forces deployed overseas; and have a legitimate interest in how international conflicts might influence or draw support from violent extremists in New Zealand. Intelligence activity relating to armed conflict generally merits oversight because of the risks involved."

I concluded from my reviews that the agencies conducted human rights risk assessments responsibly and managed the risks involved. I am well aware of the importance of oversight in this context and have been monitoring conflict-related intelligence more broadly over the course of this year. I recognise the need for public assurance that the conduct of New Zealand's intelligence agencies is under independent scrutiny in times of grave humanitarian concern.

My annual report details a significant amount of work completed by the office this year. For most of the year we operated with three full-time investigators (down from our usual contingent of five). I want to acknowledge the hard work and professionalism of my investigators and Deputy Inspector-General in carrying out our 2023-24 work programme.

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 2023-2024

Review of the Intelligence and Security Act 2017

The report of the first independent review of the ISA was published in May 2023: over the past year the Department of the Prime Minister and Cabinet (DPMC) has been leading policy development in support of the Government's response. DPMC officials have sought information and views from my office, in addition to consulting the agencies. I expect this will continue to be an important line of work for my office in the coming year.

At more than 250 pages, with 52 recommendations, the reviewers' report is a substantial and scholarly piece of work. A number of recommendations proposed structural change to the Act. Several called for further policy work to determine what direction change should take. Although a third of the recommendations were identified by the reviewers as "routine improvements", it has been evident over the past year that even those take significant work to become fully formed proposals for legislative amendment.

I am hopeful that some small changes to the Act, which will help the operation of my office, will proceed. These include enabling the appointment of a third person to my advisory panel, so it can meet even if one person is unavailable, and a clarification of the scope of my ability to initiate reviews of agency activities.

The prospects of many of the more ambitious changes proposed by the reviewers are yet to be determined. These include some matters that the reviewers recognised would require substantial policy work to develop. My observation is that some of these, such as removing the structural distinctions between intelligence warrants directed at New Zealanders and non-New Zealanders, could be independent review topics in themselves.

An independent review "of the intelligence and security agencies and [the] Act" is required by the Act itself, every five to seven years (ISA, s 235). Beyond that the scope is determined by the Prime Minister, in consultation with the Intelligence and Security Committee of Parliament. The experience of the first independent review indicates, I think, that a wholesale review of the law and everything the agencies do under it is a very demanding task. There might be a case for more selectively focused review in the future.

Use of class warrants under the ISA

In my last Annual Report I detailed concerns with the NZSIS's use of class warrants, in particular for intelligence investigations strongly focused on individuals. My concern in short is that while a class warrant is suited to the authorisation of activities genuinely directed at a class of persons, an application for a class warrant cannot, by its nature, set out the particular case for action against a specific person. In the past the Service frequently sought individual warrants, submitting to external authorities (the Minister, and if a New Zealander was involved, a Commissioner of Intelligence Warrants) its reasons for proposing intrusive intelligence gathering on the individual concerned. Such warrant applications are now vanishingly rare. Instead, a relatively small set of class warrants now covers NZSIS investigations.

The issue is not with who is investigated under these warrants, but with the quality of the warrant process itself as a safeguard of the rights of people who come to the attention of the security service. In my view New Zealanders have a right to expect – and generally do expect – that before a state agency is allowed to intrude profoundly on their privacy it must have persuaded an appropriate external authority, not just itself, that it has good reason to do so. The reality with the NZSIS class warrants that cause me concern is that the case for action against a specific person, covering their personal history and circumstances, is made within the agency, eg to a manager. For individually-focused investigations the Service has in the past presented robust individualised cases to external authorities, and in my view it should continue to do so.

The Service has made some improvements to its warrants since I first raised my concerns, but has not reversed its overall shift to operating primarily under class warrants. It is satisfied that the law enables it to do so and it is true that the ISA makes both class and individual warrants available, with no express direction or guidance as to when one might be more appropriate than the other. My argument is essentially that preferring individual warrants, where they can feasibly be sought, better serves the fundamental purpose of warranting as a control and safeguard of the fundamental right against unreasonable search and seizure. To date I have not prevailed, but nor has my concern with the Service's approach abated.

This year I began and made substantial progress on a review of the agencies' execution of class warrants. My review examines how they assess whether people come within the definition of a class in a warrant and how they decide which authorised activities to carry out. A key question in relation to the NZSIS is how cases made in-house, for activity against specific persons, compare with the justifications presented in past individual warrants. The review is also examining the approach taken by the GCSB, which has a much longer history of operating under class warrants, in common with other signals intelligence agencies. I expect to complete this review in the coming year and will report on it publicly, to the extent possible.

Open source intelligence collection

In the past year I completed a review of the agencies' use of open source intelligence collection techniques and tools. In October 2023 I gave the keynote address to the Open Source Insights New Zealand conference, discussing principles derived from my review. Shortly after the reporting year end, in August 2024, I published an unclassified version of my review report.

The key insight from my review is the extent to which open source intelligence collection has grown in power and value in recent years. As I noted in my speech and report, historically the collection of publicly available information was regarded as a poor and distant cousin to the collection of intelligence by covert means. But social media, internet browser tracking, commercial and public sector data gathering and the internet of things have dramatically increased the data available on our lives, including our tastes, values, movements and relationships. Modern open source intelligence collection tools can aggregate, analyse and display this information at speed and scale, with rich results.

It is not straightforward for intelligence agencies or oversight to identify the proper limits to use of these capabilities. At one level, publicly available information is just that: information that anyone can find, if they know where to look. On this view, open source collection tools are simply multipliers of

ordinary human capabilities, producing in seconds what could be collected by individuals or teams applying themselves to the same tasks for days, weeks or months. It does not take much learning to raise questions about this, however. Collection tools may be scraping websites whose terms and conditions of use prohibit scraping. They may also be aggregating and exploiting data that has been made public through hacks and leaks, and therefore stolen or at least released without authorisation. Use of such tools can be made lawful by a warrant. Yet whatever the legal status of the data there remains the question of whose information intelligence agencies should be collecting and retaining, even if it is there for the taking. In law there is no 'right to be left alone' as such, but I am sure there are strong opinions among the public on when it is proper for an intelligence agency to be taking an interest in them and when it is not.

The specific findings and recommendations of my review of NZSIS and GCSB open source intelligence collection are summarised later in this report. One of the key themes is the need for care in the adoption of commercially available open source tools. The most powerful of these increasingly make use of artificial intelligence to analyse and present collected data. How, exactly, this is done is not necessarily transparent, given proprietary interests in the technology. Nor is it necessarily obvious what the providers of the tools, or the tools themselves, will learn and retain from their users. The use of artificial intelligence more generally, for intelligence purposes, is an increasingly significant challenge for oversight. By the time this report is published I expect to have published some preliminary research on the topic and to have under way a review of the agencies' approaches to use of artificial intelligence.

Cooperation with overseas partners

In March 2024 I reported publicly on my inquiry into the GCSB's hosting of a signals intelligence system deployed by a foreign partner. As noted later in this report, I found significant failings in how the GCSB had agreed to host the system and how it had operated.

The GCSB agreed in principle in 2010 to host the system in question, signed a formal agreement to do so in 2012 and supported its operation from 2013 until 2020, when it was stopped by an equipment failure. The issues with it were therefore historic – but that is not unusual in oversight, which is always retrospective. Full inquiries into past actions are laborious, resource-intensive and lengthy. They can be seen as unduly concerned with issues no longer current. But it is necessary to understand past mistakes, to avoid repeating them.

In this instance the essential issue was the proper submission of an intelligence agency to Executive control. Astute staff within the GCSB recognised and pointed out the potential sensitivities, from a national interest perspective, of hosting the partner system. The Bureau appeared poised to consult its Minister on the decision but never did so, for reasons now unclear. Instead it took the decision itself. Had it sought Government approval it might well have received it. We will never know. Unfortunately, having entered the arrangement on its own authority, the Bureau then administered it badly, failing to pay proper attention to the system through its years of operation.

A key question for my inquiry was whether changes at the GCSB in the years since the decision to host the system have made it less likely such failings would occur again. I acknowledged in my report a number of developments that cumulatively, in my view, reduce the risk. I made recommendations for further action, including that the Bureau does a full audit of its systems, including any foreign partner

capabilities, and compiles a register of collection or analysis capabilities in New Zealand that are operated by foreign partners. The Bureau accepted my recommendations and at the time of writing was working on implementation.

Additionally in the past year I completed reviews of how the NZSIS and GCSB carry out human rights risk assessments, when proposing to share intelligence with foreign agencies, and how they approach support to military operations. The agencies are expected to undertake critical assessment of human rights risks, and to ensure that overseas cooperation will not result in a real risk of contributing to, or being complicit in, a breach of human rights. In situations of armed conflict or support to military operations this risk can change rapidly. Both reviews looked at how the agencies assess and manage this risk. I found there is a generally robust framework in place for sharing intelligence and cooperating with overseas parties, and the agencies' actions are consistent with it. I have engaged with the agencies on a number of instances of cooperation with foreign agencies that have raised particular risks and will continue to do so.

Agency compliance systems

An important part of this report, required by law, is my certification of "the extent to which each intelligence and security agency's compliance systems are sound". As an across-the-board assessment this is challenging, and 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*.

My report last year identified issues with the fitness of operational policy and procedure in both agencies. Both had substantial proportions of their policies overdue for review: 50 per cent, for the NZSIS, and 42 per cent for the GCSB.

Internal policies have particular importance in intelligence and security agencies. Intelligence and security legislation does not specify how the agencies are to conduct their activities with the degree of detail found in legislation governing many government departments. Statutory references to intelligence agency activities are broad, to avoid describing or prescribing the nature and extent of sensitive capabilities in too much detail. Nor is there an extensive body of decisions from the Courts, or other formal appeal or review bodies, binding the agencies' conduct. In these circumstances, internal policies establish crucial parameters for the agencies, establishing controls such as thresholds for action, rules of procedure, and levels of decision-making responsibility.

This year again I assess both agencies as having under-developed operational policy and procedure. I acknowledge that both have made progress, as a result of deliberate effort, to reduce the backlogs of policy overdue for review. Details are provided later, in the relevant section of this report. The assessment reflects the scale of the work needed to update policies, which require careful reconsideration and internal consultation. I did not expect this to be accomplished in a year. I will be discussing with both agencies what might be a reasonable standard for policy currency.

I have downgraded my assessment of NZSIS compliance systems in one other respect compared to last year, rating the Service's internal compliance programme as under-developed. Again I detail reasons later, but a key issue is the Service's persistent inability to complete its audit programme, which I have noted in past annual reports.

It is evident to me that both agencies have difficulties in maintaining strong internal compliance teams. This is not a reflection on the capable and committed staff holding compliance and policy positions. It

is more about how many of them there are. In the Bureau, compliance is fostered by the requirements of the Five Eyes partnership. Membership brings obligations. Still, GCSB compliance and policy capability is strongly dependent on the work and skills of a relatively small number of people, which brings fragility. A key absence can significantly affect capacity. In the NZSIS, recruitment and retention challenges for compliance are longstanding. I acknowledge that the agencies have tried, in various ways and with varying degrees of success, to address these issues. I believe they recognise that internal compliance staff are an important check on agency conduct. They help prevent mistakes being made, where I can only point out when they have been made. Internal audits, when they are done, are often impressively thorough and frank. I would like to see more of them. I am sure the agencies prefer to hear of systemic issues from their own audit staff than from me. I hope to see the agencies persisting with efforts to strengthen their compliance teams.

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 are aimed at ensuring 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 reported only in the annual report.

Completed or closed in 2023-24

Inquiry into GCSB support to a foreign partner agency signals intelligence system

I concluded my inquiry into the GCSB's hosting of a signals intelligence system deployed by a foreign agency.

I found that there were many reasons why the capability might be tasked, but a key question for the inquiry was whether the capability could be used to support military operations. Based on the information reviewed, it clearly had the potential to be used, in conjunction with other intelligence sources, to support military action against targets. The circumstances of the tasking would determine whether material support had been provided or not. The sensitivity of this issue was clearly identified by the GCSB when it was considering hosting the capability in 2010. I noted however that the risk of GCSB support for the capability contributing to military action was moderated significantly by the geographical limits of GCSB collection.

I found the GCSB had appropriately identified legal and policy concerns with hosting the system, which were circulated at the most senior level within the agency. Despite these concerns and the significance of hosting the system, the inquiry found no evidence of the then Minister being briefed. I was unable to determine why this did not happen. Although operation of the system came within scope of the GCSB's broad authorisation for intelligence sharing, in my view it was improper for the agency to decide to host the system without bringing it to the Minister's attention.

In relation to how the GCSB managed the system after it became operational, I found signfiicant failings. I found that the system operated:

- without any due diligence by GCSB on tasking requests;
- without full visibility for GCSB of the tasking of the system;
- with inadequate record-keeping;
- without adequate training, support or guidance for GCSB operational staff;
- with negligible awareness of the system at a senior level within the GCSB, after the signing of the MOU in 2012 and until the system was re-discovered in 2020; and

- without due attention to the possibility recognised within the GCSB that support for the system could contribute to military targeting.

I found that the GCSB, its operations, its governing statute, its policies and compliances have changed significantly over the period in which the system operated, and since. These developments reduced the risk that the shortcomings identified by my inquiry would recur. I made several recommendations and continue to engage with the GCSB about their implementation.

An unclassified report can be found on my website.

Review of GCSB and NZSIS human rights risk assessments

I reviewed both the NZSIS's and GCSB's carrying out of human rights risk assessments (HRRAs) for cooperation with overseas public authorities.

My office assessed a sample of HRRAs carried out by both agencies under a Joint Policy Statement (JPS) on the Management of Human Rights Risk in Overseas Cooperation. I found the JPS provides a relatively robust framework for intelligence sharing and cooperation with overseas parties and both agencies have implemented it reasonably well.

NZSIS

I reviewed two "standing HRRAs" in depth, which related to cooperation over long periods of time. I identified some areas requiring further consideration from the Service. I also identified some concerns with the policy framework for standing HRRAs. While the Service has taken a relatively cautious approach for some standing HRRAs, I recommended the JPS be amended to include a clearer framework for standing HRRAs, taking into account the points raised in my report.

I also recommended the Service maintain a register or centralised repository for HRRAs, to enable more effective oversight of these activities (particularly where a speculative or real risk of a rights breach is identified); and that the Service audit HRRAs on a semi-regular basis.

The Service accepted all of my recommendations. Following the review, it implemented a new policy for managing human rights risk, no longer shared with the GCSB. This policy took into account the issues raised in my review.

GCSB

The Bureau does a large number of HRRAs and mainly approaches them in a consistent way, with a clear process and recordkeeping. Generally, the Bureau's HRRAs appeared to comply with the JPS requirements. I found some instances, however, where the analysis could have been more robust and practice could have aligned more closely with the requirements of the JPS. I did not, however, have any concerns about the ultimate decision reached by the GCSB in each of these cases.

Based on these findings I recommended the Bureau:

- update the guidance and working aids to align with the current JPS on the Management of Human Rights Risk in Overseas Cooperation; and
- record the HRRA assessed level of risk.

The GCSB accepted these recommendations.

Review of GCSB and NZSIS open source intelligence (OSINT) collection

I completed my review of the agencies' use of specialist open source intelligence tools and methods to collect intelligence.

My review looked at how both the NZSIS and GCSB approached the legal issues that arise with OSINT collection, conducted OSINT collection and checked that it met legal and policy requirements.

NZSIS

My review identified several concerns with Service warrants covering open source collection. For instance, the warrant applications needed to explain the tools used, the individuals who could be targeted under the warrants, and the full range of OSINT activities NZSIS intended to carry out. I raised these matters with the NZSIS and most of my concerns were addressed in recent warrant applications.

I recommended the NZSIS develop and formalise a framework for the acquisition and use of specialised open source intelligence collection tools. NZSIS advised me that it would do so.

The Service's use of its OSINT tools for ongoing collection on individuals and groups, rather than single instances of collection, raised several concerns. I found limited operational planning and documentation had been done before ongoing collection. No request forms had been submitted for the ongoing collection activities I reviewed. Requesting and reporting of ongoing collection had usually occurred verbally, which is not amenable to oversight.

Many of my concerns were addressed by recent changes in NZSIS procedure for the use of OSINT tools, although the new procedure does not explicitly cover the requesting and registering of ongoing collection. I recommended NZSIS amend its procedure to incorporate requirements for initiating, recording, and reviewing ongoing collection. The Service advised me that it would include requirements for ongoing collection when it next updated its procedure.

GCSB

I found that the Bureau approached the use of open source collection tools reasonably carefully. It had a robust warrant framework governing use of the tools and handling of collected data. I considered it could provide more information in warrant applications on the tools it used for open source searches. It undertook to review the relevant material at the next opportunity.

I found that GCSB's guidance material, while useful, needed updating in some areas to reflect current practice. It also required further guidance for one of the tools to cover data retention and assessment. The tool was retaining copies of all search results, which was at odds with the legal and policy requirements that collected information must be assessed for relevance and destroyed as soon as practicable if irrelevant.[1] While I understand this was partly due to the technological constraints of the tool, I could find no recorded justifications for retaining all the information.

I recommended that the GCSB:

---

[1] ISA, s 103.

- update its guidance material;
- review the search results retained by the tool at issue, to assess the information for relevance and comply with s 103 ISA and GCSB's data retention policy; and
- provide my office with routine access to certain records on its collection process.

The GCSB accepted my recommendations.

Review of GCSB and NZSIS support to military operations

I concluded my review into the GCSB and NZSIS support to military operations (SMO).

GCSB

My review identified the threshold for needing to obtain Cabinet authorisation for supporting military operations as a key issue. I found that the GCSB had appropriately obtained Cabinet authorisation for intelligence support to military operations on all occasions I investigated. I considered that there was one consequential amendment that could be made to the Joint Policy Statement on the Management of Human Rights Risk in Overseas Cooperation, to require that a Cabinet mandate is sought if providing information/intelligence support to military operations in an exisiting, or likely, armed conflict. This remains a matter to be explored further with the GCSB.

I noted there might be value in a high-level agreement between the GCSB and the New Zealand Defence Force and I will continue to engage with the GCSB on this.

I also considered there was value in the GCSB implementing a policy to provide staff providing support to military operations with supervision, information and training about:

- the legal and policy basis for their roles;
- agency policies and procedures relating to New Zealand's human rights obligations; and
- the process for raising any questions or concerns about the nature of their work.

NZSIS

The NZSIS was not actively providing support to military operations in the period under review. I found however that its definition of support to military operations was too narrow. This meant it did not identify its contribution to a particular operation as being support to military operations, when the GCSB had reached the opposite view about its own contribution to the same operation. I considered that the Service should develop a clearer definition of what consitutes support.

Following recommendations from an inquiry by the previous Inspector-General, I recommended the Service revise its guidelines for interviewing individuals detained overseas. In response the NZSIS advised it was discontinuing its current guidelines for support to military operations. Instead it would ensure that tailored guidance was available to staff for future SMO activity, alongside guidance in its revised human rights policy.

Review of GCSB acquisition and use of bulk personal datasets

I reviewed the approach taken by the GCSB to the acquisition and use of bulk personal datasets. These are datasets which include the personal data of individuals, most of whom are unlikely to be of intelligence or security interest.

I found the GCSB had a sound approach to the planning and approval of dataset acquisition under warrant, and to the use and retention of collected datasets. The relevant warrant was clear in how the activities could be undertaken. Collected datasets were stored in systems with controlled access that required searches of the material to be justified. All searches were logged, auditable and regularly audited. The GCSB had no policies and procedures specifically addressing bulk personal datasets, but this was understandable given the level of activity.

I identified a potential issue that could arise for bulk personal datasets and compliance with section 103 of the ISA and the GCSB's data retention policy. By their definition, bulk personal datasets typically contain information on individuals of no intelligence interest. I consider that determining whether a dataset can be retained as "relevant" is a matter of degree, which depends on the contents and purposes for retention of the particular dataset. A dataset cannot always be retained as a whole simply because it contains some relevant information. Continued retention of data within a dataset should be justified by demonstrable current or future value for a GCSB function.

I recommended the GCSB develops guidance on how section 103 ISA and GCSB's data retention and destruction policy apply to its retention of bulk personal datasets. The GCSB has agreed to do so.

Review of NZSIS counter-terrorism and violent extremism class warrants

I reviewed three intelligence warrants issued to the NZSIS in 2022 and 2023. The warrants authorised it to target classes of individuals in the context of counter-terrorism and violent extremism.

I found that the first two iterations of the warrants did not meet the legal tests for necessity and proportionality in the ISA for warrants to be issued. I considered that the target classes in the warrants were too broad and required too subjective an assessment to justify the prior authorisation of the most intrusive powers against individuals who might fall within the target classes. I thought the warrants gave the NZSIS too wide a discretion to operate without any external scrutiny of the case against any particular target.

I also considered that, even if the warrant met the tests under the ISA, as a matter of policy the NZSIS should not have applied for such a class warrant. I saw no substantive reason for applying for a class warrant rather than individual warrants, other than the minimal administrative convenience of reducing the number of warrant applications the Service is obliged to make. In my view that undermined the purpose of the warranting regime.

The Service disagreed. Following the provision of my classified report to the Service and its Minister, the NZSIS obtained advice from Crown Law on the first two iterations of the warrants. Crown Law considered that some aspects of the class definitions were overly broad but some were sufficiently certain under the ISA. It advised that changes could be made to meet the tests under the ISA and to ensure the lawfulness of the warrants.

The Service obtained a third iteration of the warrant in September 2023, signed by the then Minister and the Chief Commissioner of Warrants. I considered the third iteration of the warrant an improvement and it followed the advice of Crown Law.

I remain concerned that it is not proper for the NZSIS to apply for such a warrant, as I have been unable to see any reason why individual warrants cannot be obtained in the circumstances. In my view, there should be a preference for individual warrants, all other things being equal, as this provides for better oversight of the Service's activities, greater protection of individual rights and a greater safeguard against agency overreach. This is predominantly a policy issue with the ISA.

Although I considered the first two iterations of the warrant did not meet the legal tests for necessity and proportionality under the ISA, I had no information to suggest the NZSIS inappropriately targeted individuals. The Service appeared to have been reasonably cautious in its work under the warrants. I have been carrying out an in-depth review of how both the NZSIS and GCSB have operated under class warrants to further assess this and expect to report on it in the coming year.

My findings do not invalidate the warrants or the activities carried out under them and I have not recommended to the Minister that information obtained under the two versions of the warrant be destroyed.[2] My concerns rather go towards the integrity of the authorisation system in the ISA and ensuring proper use of intrusive powers.

I published an unclassified report on this review on the IGIS website.

Review of NZSIS cooperation with the New Zealand Police on counter-terrorism

I completed my review of how the NZSIS cooperates with the New Zealand Police on counter-terrorism investigations. I found that the NZSIS and Police cooperate closely on counter-terrorism, sharing information frequently at multiple levels, from informal exchanges between officers to formal, minuted discussions between middle and senior managers. Both agencies had a reasonably clear understanding of their respective roles and functions, with responsibility for particular activities discussed and agreed on, as required.

I found the Service's record-keeping on interactions with the Police varied. While formal interactions were reasonably documented, recording of informal interactions (eg in-person conversations) was ad hoc. The quality varied between individual staff members. I reminded the NZSIS of the importance of appropriate record-keeping.

I noted that the Security Information in Proceedings Act 2022, which entered into force in late 2023, establishes new procedures for dealing with intelligence as evidence in proceedings, intended to be more workable than previous arrangements. I expect this development will increase the likelihood of NZSIS intelligence being sought as evidence for Police terrorism-related prosecutions, while also increasing the practicability of bringing it to court. At the very least it will become more relevant to the pre-trial criminal disclosure process.

The Service's long-standing position is that its intelligence is usually not available for use in proceedings, even if it has evidential value. This position already looks out of date and inconsistent

---

[2] Section 163(2)(a) of the ISA.

with recent developments. I consider it would be useful for the Service to consider the fitness of its investigative procedures ahead of any request for intelligence to be used in proceedings.

I published an unclassified report of the review on my website.

Review of the issue and execution of a NZSIS seizure warrant

My office reviews every intelligence warrant issued to the intelligence and security agencies. When necessary, I conduct a more in-depth review (or 'deep dive') of the issue and execution of an intelligence warrant.

This year I completed a review of an intelligence warrant issued to the NZSIS to search for, and seize, a dataset. I examined the Service's planning and decison-making for the seizure, how it obtained the data, and its subsequent handling, storage, and access to the data.

I found the Service's process for obtaining the intelligence warrant and carrying out the authorised activities was reasonable. It took a cautious approach to internal approvals, and went beyond what was required by policy and procedure. This included a thorough privacy assessment.

I was concerned, however, that regarding the necessity of accessing the dataset the Service had required only that staff tick a box confirming a connection to a National Security Intelligence Priority and the Service's statutory functions. This is not an assessment of necessity.

As the Service began substantially revising its bulk dataset acquistion policies and procedures during the course of my review I made no recommendations, but will reassess the postion when that work is complete.

Review of NZSIS use and sharing of security clearance assessment information

The functions of the NZSIS include conducting security clearance assessments (vetting) for individuals who are required to hold a national security clearance for their work. Section 220 of the ISA prohibits the Service using information collected or disclosed to the NZSIS for a clearance for purposes other than vetting or counter-intelligence. I reviewed the Service's compliance with section 220.

I found that on a limited number of occassions the NZSIS used or shared vetting information for other purposes, including counter-terrorism investigations, and an internal disciplinary process, and in one case disclosed information to law enforcement. These were contrary to the ISA.

In some instances the Service sought and was granted intelligence warrants to access and use vetting information for counter-terrorism investigations. In my view the NZSIS cannot obtain a warrant to authorise activities that are unlawful under the ISA. I recommended the NZSIS cease applying for such warrants and revoke any related policies.

I recommended NZSIS develop further guidance for staff to ensure compliance with section 220.

The Service accepted my recommendations.

Review of NZSIS counter-terrorism discovery projects

I reviewed the NZSIS's approach to discovery work for counter-terrorism and violent extremism purposes (CT discovery). This review involved an assessment of discovery projects, which seek to

understand threats and generate leads for investigation, undertaken by the Service from 2018 to 2023.

I found the Service's approach to CT discovery has developed considerably since 2018 and is still evolving. It uses a variety of methodologies and is continuing to assess and develop its approach as new ideologies and threats emerge. This has included creating a variety of internal resources to guide CT discovery work, which I considered in detail in my classified report.

I found the Service has used a wide variety of intelligence collection methods for discovery work. Most have tended to be at the lower end of intrusiveness, though at times limited warranted activities have been conducted.

A key question for this review was whether and how the protection for freedom of expression in section 19 of ISA affected the Service's CT discovery work. In general, I found that NZSIS has taken a carefully constructed approach to assessing terrorism and violent extremism and identifying individuals or groups displaying behaviours of concern. Section 19 ISA does not appear to be a barrier to the Service undertaking extensive discovery work.

I identified two instances of the NZSIS collecting information, for discovery purposes, about the online activities of individuals and groups who were part of fringe political movements. The collection was relatively limited and was at the low end of intrusiveness. I was concerned however that there did not appear to be any record of consideration of what expression or activities by the group's members justified the Service's activity. I recommended the Service amend its process for discovery projects so that staff are required to expressly consider section 19 ISA at the beginning of a CT discovery project, and, in relation to specific collection decisions, to document this.

I also assessed whether the Service's internal resources to guide CT discovery work were fit for purpose and up to date. My review found the results to be mixed. The Service has identified that it needs to review these resources and has committed to doing so. I recommended it review these resources comprehensively to ensure they are fit for purpose, including confirmation that behavioural indicators of security risk are appropriately weighted.

The Service has taken action to implement these recommendations.

Review of two NZSIS compliance incidents

Both agencies report compliance incidents to my office when there is, or may be, a material breach of the law or a warrant. Two incidents reported to my office this year raised sufficient concern for me to initiate a review. Both incidents involved administrative errors in conducting activities under a class warrant. The Service's internal compliance reviews found that although the incidents amounted to a breach of policy, the collection activity was still authorised. I disagreed.

My review concluded the collection was unauthorised because the NZSIS failed to follow the process described in the warrant for taking action under it. As a result I determined the NZSIS would need to either destroy the information collected or apply for an intelligence warrant to retrospectively authorise the collection, as provided for by section 102 ISA. The Service accepted my findings and agreed to implement a recommendation to reduce the possibility of future errors.

Ongoing

Review of NZSIS and GCSB use of artificial intelligence

In the past year I completed an open source research report on artificial intelligence governance from an intelligence perspective. This was published on my website not long after year end. I am now examining current or planned use of artificial intelligence by the NZSIS and GCSB. The review aims to identify any good practice principles or models emerging internationally, understand the New Zealand intelligence agencies' approach and assess it. I expect to complete a classified report in the coming year.

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). In the coming year I propose to examine and if necessary review how the agencies understand political neutrality and what policies and practices they have to ensure it. This may include reviewing activity in relation to the 2023 general election.

Review of the execution of class warrants

A class warrant enables otherwise unlawful intelligence activities against a class of persons, rather than a specific individual. Both agencies now operate predominantly under class warrants. In 2023-24 I began a review of how each agency operates under class warrants, including how they determine whether a person falls within a class, how that determination is reviewed, and compliance controls. 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 be concluding this review by the end of the coming year.

Review of NZSIS human source recruitment and management

In 2022 I began a baseline review of the Service's approach to the recruitment and management of human sources. This has been a challenging review for both my office and the Service due to the high level of security protection given to the source material. At year end I was engaging with the NZSIS on a final draft classified report and considering the scope for a public report.

New Zealanders and international terrorist screening databases (NZSIS)

In 2023-24 my office began examining the NZSIS' 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 complete this work in 2024-25.

GCSB's collection of intelligence on transnational organised crime

Collection of intelligence on transnational organised crime is a niche area of intelligence collection for GCSB. I began a review of this activity in 2023-24, seeking a baseline understanding of GCSB's approach, and expect to conclude it in the coming year.

Review of GCSB target discovery activities

I have reviewed how the GCSB's target discovery activity is authorised, and examined a number of discovery projects. My purpose was to better understand how the work has evolved since 2019, particularly for domestic counter-terrorism purposes. I am in the process of completing a classified report on my findings.

Review of GCSB raw data sharing with partner agencies

My review of GCSB systems and procedures for sharing raw (unevaluated) data with partner agencies was close to completion at year end, pending some final advice from the Bureau. The scope for public reporting is likely to be very limited but I will assess that in due course.

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, to the complainant or publicly.

Throughout the year my office receives contact from 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 conducts large numbers of security clearance (vetting) assessments.

Complaints received in 2023-24 are tallied in the following table. Additionally my office received and dealt with a further 36 contacts seeking information or raising issues that did not amount to complaints within my jurisdiction.

Complaints received 2023-24			
From	**Against GCSB**	**Against NZSIS**	**Total**
Members of the public	5	16	21
Intelligence agency employees or former employees	0	1	1
Total	5	17	22

The total number of complaints received in 2023-24 decreased from previous years, though the proportion requiring substantial investigation has not changed significantly.

In December 2023, I completed my inquiry into a complaint against the NZSIS, in which the complainant alleged the NZSIS without justification advised their employer they were an “insider threat” due to their relationships with foreign embassy staff; that they were detained and subjected to an involuntary interview; and that they were targeted due to their ethnicity. I found the NZSIS had cause to investigate the complainant and to report on him to his employer. I also found that the complainant was not detained and the interview with him was conducted on a voluntary basis. I did not uphold the complaint. I published my findings on my website.

At the end of the 2023-24 period, I had one ongoing inquiry into a complaint received about the NZSIS.

WARRANTS

In this reporting year my office reviewed 44 warrants issued to the agencies and 13 other authorisations. This was a small decrease on the preceding year (61).

A Type 1 warrant is sought when the agency intends to carry out an otherwise unlawful activity for the purpose of collecting information about, or doing 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). It can be issued by the Minister alone.

The ISA allows for the GCSB and NZSIS to apply to the Minister and Commissioner of Warrants for a Business Record Approval (BRA), which authorises the agencies to obtain business records from specific business agencies. A BRA is valid for six months.

The ISA permits the agencies to apply 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. The application is made to the Minister responsible for the agencies, and for an application involving a New Zealander, the Chief Commissioner of Intelligence Warrants.

Intelligence warrants and Business Record Approvals reviewed in 2023-24								
	Type 1 warrants	Type 2 warrants	Access to restricted information	Practice warrants	Removal warrants	Revoked warrants	Business Record Approvals	Total
NZSIS	11	0	1	2	3	7	3	27
GCSB	14	13	0	1	0	0	2	30
Total	25	13	1	3	3	7	5	57

This year, neither agency sought a very urgent authorisation under section 78 of the ISA.

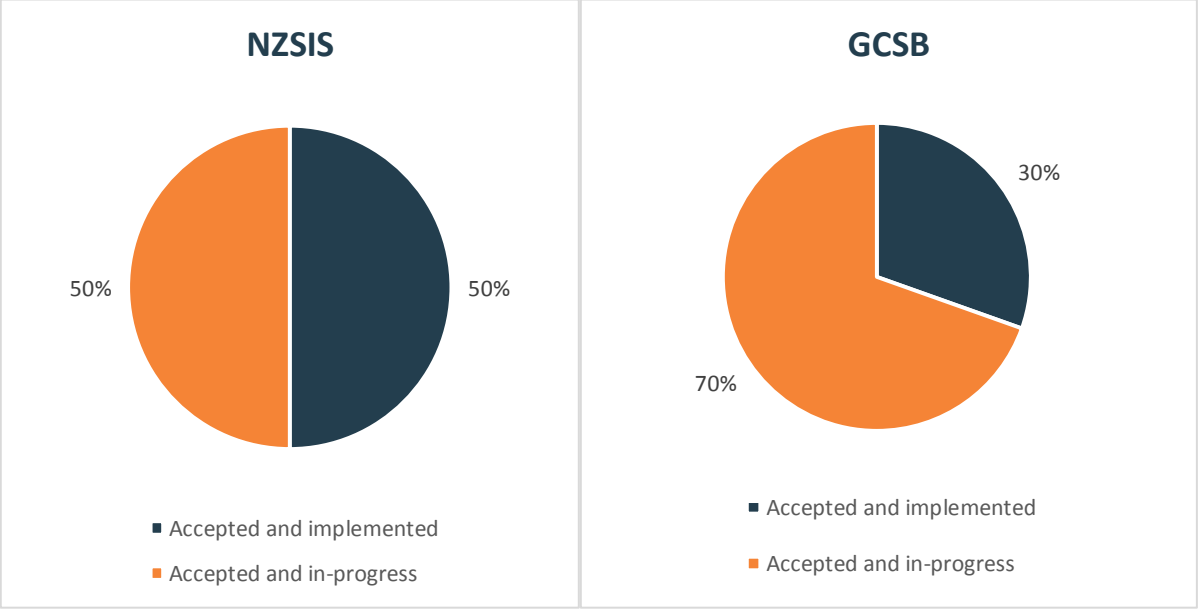
IMPLEMENTATION OF IGIS RECOMMENDATIONS

As the result of an inquiry or review I often make recommendations to the agencies. These are non-binding, but I seek to ensure they are practicable to implement, will add value and ensure compliance with the ISA. I seek and generally receive agreement from the relevant agency that my recommendations will be implemented and I receive updates on the implementation process. The length of time for an agency to implement recommendations varies. Minor changes to a policy might be easily made, while recommendations for systemic change can take longer.

If an agency rejects my recommendation, it does not mean it is non-compliant with the ISA or the underlying activity was unlawful.

The review and inquiry recommendations tallied below are from the last three years. The larger number of recommendations to the Service than to the GCSB is due in part to multiple recommendations arising from complaints about a relatively small number of security clearance (vetting) assessments.

At the close of the year I was awaiting a formal response from the Bureau regarding nine recommendations made near year end. The Bureau accepted the recommendations in the current year, which will be reflected in next year's annual report.



Status	NZSIS	GCSB
Accepted and implemented	13	7
Accepted and in-progress	13	16

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. Lyn Provost, the former Controller and Auditor-General (2009-2017) chairs the panel. Supporting Lyn is Ben Bateman (Ngāi Tahu and Cook Island Māori descent), who has an extensive background in law and governance within the public sector, including in the New Zealand Defence Force and the Department of Prime Minister and Cabinet.

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

Commissioners of Intelligence Warrants

This year saw my office engage more regularly with the Commissioners of Intelligence Warrants. My office discussed oversight of the agencies, the intelligence warranting process, and shared a number of classified reports with the Commissioners. This was a welcome engagement, which I hope to continue.

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 review and oversight methodology and explore possible cooperation. In September 2023 the conference was held in Ottawa, Canada.

External engagement

I welcome opportunities to engage with the general public, community groups and the public sector about the role of the Inspector-General. This enhances transparency about our activities and fosters public discussion on the role of the intelligence and security agencies in New Zealand.

This year, I accepted 11 speaking opportunities, to academic, public service, and intelligence sector audiences.

Staff in my office regularly attend conferences, workshops, and public talks related to our work. This year these have included events on disinformation, artificial intelligence and open source intelligence.

FINANCES AND ADMINISTRATION

Funding and resourcing

The IGIS office is funded through two channels. A Permanent Legislative Authority covers the remuneration of the Inspector-General and the Deputy Inspector-General. Operating costs are funded through Vote Justice, as a non-departmental output expense. Total expenditure for 2023-24 was 9.7 percent under budget, mainly due to salary lag while vacancies were carried:

Office of the Inspector-General of Intelligence and Security 2023-24 Budget		
	Actual ($000s)	Budget
Staff salaries/advisory panel fees; travel	699	881
Premises rental and associated services	371	407
Other expenses	9	9
Non-Departmental Output Expenses (PLA)	692	663
Total	1,853	2,052

At year end, the office had a total staff of six: the Inspector-General and Deputy Inspector-General, an office manager, and three investigators, with one further investigator appointed but not yet at work. To meet budgetary restraints a retiring IT and security manager position (0.5 FTE) has not been filled, with the responsibilities of the role picked up by other staff.

Premises and systems

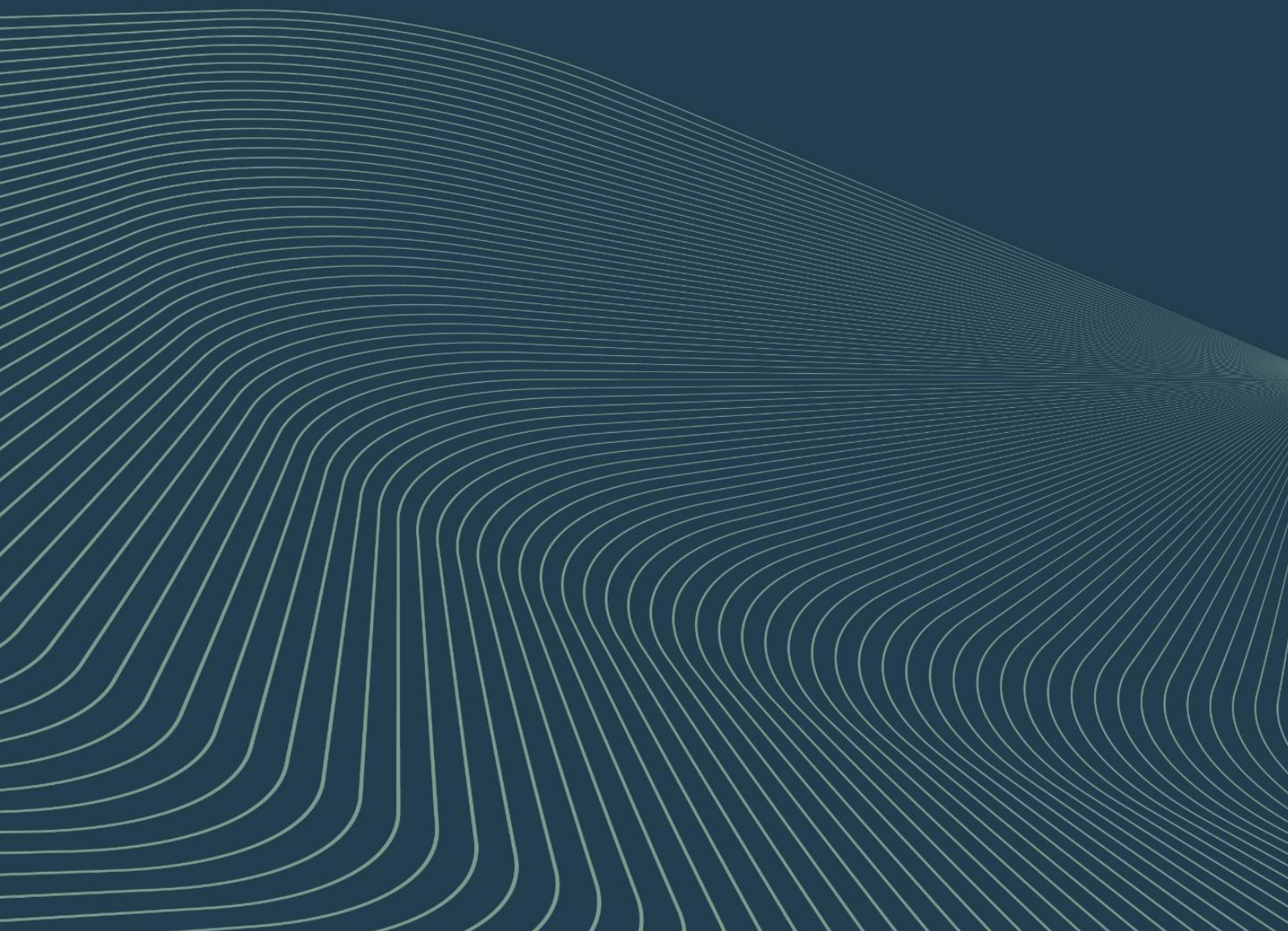
Since October 2019 my office has operated from secure premises in Defence House, Wellington.

The office operates a highly secure computer network, accredited in 2023 as compliant with the requirements of the New Zealand Security Information Manual. The next assessment is due in 2025.

Administrative support

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

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 some change is needed 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 2023-24

Heading	Rating
Operational policy and procedure	Under-developed

The GCSB has a cohesive, accessible suite of policies and procedures. A governance group oversees operational policy maintenance and development. The group met four times in 2023-24. Quarterly compliance updates show the pace of approval, review and revocation of policies increased this year. The agency has specialist policy staff and clarity about the work needed to update policy. A running policy stocktake indicated 48% of policies were overdue for review at May 2024. Work was in progress for 71% of those. The governance group was monitoring the work required to align policies and procedures following CERT NZ's integration into the GCSB's National Cyber Security Centre. I anticipate ongoing progress as the GCSB pursues its Operational Policy Work Programme.

Heading	Rating
Internal compliance programmes	Well-developed

The GCSB has effective internal programmes for promoting compliance. A compliance strategy for 2021-25 defines desired compliance outcomes. The agency assesses progress against actions and measures defined in that strategy. Compliance reporting to leadership has forecast a need to revisit the strategy in 2025. The GCSB has an audit plan for 2024, and reports consistently against the progress of that audit plan. In the 2023-24 year the agency made progress in staffing specialist compliance and policy roles, with a team of seven staff and a manager. Audits are time-consuming and complex, and progress to implement the recommendations from internal audits can be slow. There are some proactive measures to understand and improve compliance and engage more broadly with staff.

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

There have been no substantive changes to the GCSB's effective self-reporting and internal management of compliance incidents. Observations from reviews conducted indicate staff readily and regularly seek advice on compliant and lawful conduct. Compliance checks are embedded into business processes, particularly in use of signals intelligence tools. Policies and procedures for managing compliance investigations are in place and current. Complex incidents typically take between three and five months to investigate, but investigations reported to this office are thorough.

Heading	Rating
Training	Well-developed

Although implementation is in progress, the GCSB has made an effort to strategically identify and track the maturity of operational training; a number of actions in the GCSB's operational compliance strategy relate to a stated objective to ensure compliance resources and training can develop highly capable staff and managers. Quarterly reports to leadership provide examples of specific training sessions delivered in-person by compliance staff. The agency has dedicated learning and development systems and staff (joint with NZSIS). A documented induction plan with compulsory compliance training is in place, and routine compliance certification exams are required for staff.

Heading	Rating
Responsiveness to oversight	Well-developed

The relationship between my office and GCSB staff remains constructive and professional. This year the agency provided training sessions for my staff on two occasions, and pro-actively briefed my office on a cyber-defence initiative. Most engagements relate to facilitating reviews and responding to reports and recommendations. As in previous years, these tasks fall to legal and compliance staff. My work is occasionally delayed by slow responses from the GCSB (for instance, my inquiry into their hosting of a foreign partner capability was delayed in its last phase by some months). Notification of newly issued intelligence warrants has not always been timely. Some issues regarding access for my office to GCSB records have been progressing very slowly. The GCSB uses a range of technical tools; ensuring ongoing visibility and access to these tools and associated records remains a priority. I appreciate the agency's ongoing engagement on this issue, particularly the efforts of the GCSB's internal compliance team.

NZSIS Compliance System Assessment for 2023-24

Heading	Rating
Operational policy and procedure	Under-developed

The NZSIS continues to make a concerted effort to review, update, and consolidate policies and procedures. In 2021-22, I reported that 92% of the Service's policies were overdue for review. By 2022-23 that number had reduced to 50%, and by the end of 2023-24 it was 36%. Excluding corporate policies and policies shared across both agencies, the number of operational policies overdue for review is 22%. Policies are published and easily accessible to staff, and there are guidelines and locatable resources on how to develop and manage SOPs and policies. A specialist operational policy advisor was recently appointed, but for much of the year the internal compliance team operated as a team of one advisor and one manager. A policy plan for the 2024-25 financial year is scheduled for development.

Heading	Rating
Internal compliance programme	Under-developed

For the past three years I have reported the NZSIS has no compliance strategy in place or endorsed by leadership. NZSIS proposed to develop one but has not done so. An audit plan is now in place for the remainder of the 2024 calendar year, but an internal audit plan for the 2023-24 year was not drafted; the agency instead carried over audits planned for the previous year. Three quality audit reports delivered to my office this year demonstrate that when conducted, internal audits provide considerable value in identifying risk and remediation opportunities. Regular quarterly reporting is provided to senior leadership and proactively shared with my office. Trend analysis is evident in focus areas (such as measuring progress in improving policies), but limited in areas such as progress against audits and remediation planning. Compliance staff attend inductions for new staff and publicise their work on the intranet, but much of their work remains necessarily reactive as they respond to compliance incidents and manage routine tasks.

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

The Service's internal compliance team has prioritised improving operational policies and procedures, and investigating self-reported compliance incidents. There is an effective internal process for receiving and investigating internally-reported compliance incidents. Staff clearly engage with legal and compliance teams to seek advice and report incidents. Procedures for reporting and responding to privacy and compliance incidents are current, and remediation efforts are aimed at increasing staff competencies, with no observations of a disciplinary or punitive culture. It takes time to internally investigate and to make an assessment about the full impact of reported incidents. The Service's practice of notifying my office when they become aware of an incident, and before an investigation is complete, is appreciated. This year I initiated a review of two of these incidents (discussed earlier).

Heading	Rating
Training	Well-developed

The NZSIS has a dedicated learning and development system, staff, and a training policy in place (joint with GCSB). There is an induction programme for new staff, and some mandatory minimum compliance training is expected. A range of training courses are available across the unique skills required for the agency's functions. New or refreshed policies are sometimes accompanied by complementary training modules, but proactive efforts are generally in response to operational needs rather than any strategic effort to identify and respond to training gaps across the agency. NZSIS staff have acknowledged that formalised training pathways and certification requirements could be developed, particularly for high-risk operational roles. An additional observation across reviews and incidents is that non-compliance with existing policies is sometimes attributed to a lack of staff awareness (for example, failing to follow policy when conducting warranted activity) or re-occurring user errors (such as incorrectly assigning access rights to documents). These reflect training issues. In my view they are also a logical consequence of under-developed policies, and an under-developed compliance programme – both of which are necessary drivers for setting standards to assess compliance against, and for identifying and addressing training needs to improve compliance.

Heading	Rating
Responsiveness to oversight	Well-developed

The NZSIS is responsive to oversight and its engagement with my office is timely, frank and constructive. We meet frequently. Despite resource constraints the NZSIS responds promptly to questions and receives and implements recommendations without undue delay. The Service proactively and routinely shares compliance reports and provides updates on compliance investigations. Because of its domestic focus and functions, a greater proportion of the complaints I receive and investigate concern the NZSIS (as discussed earlier in this report). This creates a demand on NZSIS staff to arrange access to records and engage with me on the details and outcomes of those complaints. I appreciate their diligence and professionalism.

Te Pourewa Mātaki
Inspector-General of Intelligence and Security