Te Pourewa Mātaki
Inspector-General of Intelligence and Security

ANNUAL REPORT 2022-2023

Brendan Horsley
Inspector-General of Intelligence and Security
November 2023

CONTENTS

FOREWORD

I am pleased to present my office's annual report for 2022-2023.

This past year saw the conclusion and publication of the joint inquiry into the tragic attack at the LynnMall supermarket in Auckland. In my view, this complex inquiry showed the value of truly independent oversight.

At the commencement of my inquiry I was made aware of concerns held by members of Muslim communities that the attacker had been improperly targeted. It was suggested he had been assessed as a threat due to biased and unfounded intelligence reporting by the NZSIS. Obviously any such failing would be a serious matter. My inquiry therefore examined all the classified source material for NZSIS reporting. I found the intelligence reports were unbiased, founded upon solid evidence and fairly stated the violent extremist threat the attacker posed. This enabled me to provide independent assurance, directly to representatives of Muslim communities and in the public report, that the agency had acted professionally, lawfully and properly. I see the provision of such assurance, when it is needed and justified, as a vital part of my role.

In May 2023, the first review of the Intelligence and Security Act 2017 was published. While the past 6 years of experience with the Act has shown it to be workable, there are some things that could usefully be clarified. An example is the scope for "disruption" activities by the Service, given the agencies' lack of any enforcement function. The main practical issues with the Act, however, relate to intelligence warrants. The Act made both agencies subject to a single warrant regime, a change elegant in theory but more problematic in practice. Two of the issues raised are discussed in this annual report: the choice between individual and class warrants and the authorisation of bulk personal dataset collection. As an oversight body we look for clarity in what the law requires but, in both cases, this has raised as many questions as answers. The questions therefore become matters of policy, which make this legislative review and public engagement with the law reform so important.

I welcomed the commencement of the Protected Disclosures (Protection of Whistleblowers) Act in July 2022, which updated the law to better protect whistleblowers in the workplace. My office has a special role under the Act for receiving protected disclosures from employees of the intelligence and security agencies, or concerns involving classified information. These are fraught areas for protected disclosures. I have published updated guidance on the IGIS website.

In terms of business as usual, this period has been focused on catching up on inquiries and reviews that were significantly affected by staffing constraints arising from COVID-19 precautions, illness and personnel changes. At the end of 2022-23 many of these reviews and inquiries were well advanced and will be completed and reported on in the first half of 2023-24.

Intelligence and security oversight continues to be complex and challenging. In society there is increasing expression and adoption of a wide variety of extreme ideologies and views. This is prevalent on the internet and monitoring it for real threats raises difficult and important issues for the agencies. Alongside this, the agencies operate in an environment with increased geostrategic competition, which has profound national security implications. For oversight, it is important to understand the changing threats the agencies deal with, so we can ensure their response is necessary and proportionate – to ensure, in other words, that the agencies continue to act lawfully and with propriety.

As an office we are also taking a step back to look at how we operate and how we choose what work we focus on. We are looking at our work and engagement planning to ensure that we are setting priorities effectively and allocating limited resources where they will have the greatest impact. I will look to publish the outcome of this work in 2023-24.

As a final comment, readers might note that the "significant issues" discussed in this year's report relate somewhat more to the NZSIS than the GCSB. This is not a reflection on either agency. We examine both agencies equally, but issues do not arise equally. In the early years of the Intelligence and Security Act, for example, more issues arose in relation to warrants issued to the GCSB. More recently it is NZSIS warrants raising issues. I also note that the NZSIS is seeking to transform its approach to intelligence gathering, becoming more 'data driven' and stepping up its target discovery activities. Change always brings risk, and risk requires the attention of oversight. I can, of course, confirm that both agencies remain under equal scrutiny. I will continue simply to report matters as they arise.

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

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.

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 2022-2023

Review of the Intelligence and Security Act 2017

In May 2023 the independent reviewers of the ISA published their report *Taumaru: Protecting Aotearoa New Zealand as a free, open and democratic society.* As noted in my last annual report the reviewers engaged widely, including with my office. This included seeking our views and feedback as a draft report was prepared in the later part of 2023. I appreciated the thoughtful hearing my office received.

The reviewers concluded that the legislative framework for the office of the IGIS was sound and needed no major change.[1] They did however recommend amendments they considered modest or routine, providing for the IGIS to:

- have regular engagement with other New Zealand oversight agencies (eg the Ombudsman, the Privacy Commissioner) on matters of common concern;
- be able to discuss classified material with overseas oversight bodies in a manner consistent with its classification;
- be supported by an advisory panel of three people (rather than the current two);
- if established, have oversight of a new national intelligence assessment agency;
- transfer a complaint to another oversight body, where appropriate; and
- have access to a new three-person panel of independent technical experts, shared with the Intelligence and Security Committee and the Commissioners of Intelligence Warrants.

The reviewers also recommended adding express provision for the IGIS to self-initiate reviews of agency activities that do not require authorisation (eg much open source intelligence gathering). This is an apparently illogical gap in the current law, which provides for an inquiry into such matters but not a review, even though a review is less demanding and intrusive. To date, as the reviewers noted, the gap has not prevented me reviewing such activities. They considered it preferable however that my ability to do so is clearly stated.

I engage regularly with other New Zealand integrity agencies, particularly the Ombudsman and Privacy Commissioner, and do not see any pressing need for a statutory duty or prompt for that. I would very much welcome, however, the establishment of an independent panel of technical experts. Expansion of the advisory panel would enable access to a broader range of advisors and provide helpful cover when one member is unavailable.

The Department of the Prime Minister and Cabinet is leading policy development in support of the Government response to the review. Officials are seeking information and views from my office,

[1] Sir Terence Arnold and Matanuku Mahuika *Taumaru: Protecting Aotearoa New Zealand as a free, open and democratic society* (Ministry of Justice, 31 January 2023) at [12.79]-[12.80].

where relevant. I expect this and ensuing legislative reform to be an important line of work in the coming year.

NZSIS use of class warrants

Under the ISA an intelligence warrant may authorise an agency to carry out otherwise unlawful activities (eg intrusive surveillance) against a person or a class of persons. A warrant relating to a specific (usually named) person can be labelled, for convenience, an 'individual warrant'. A 'class warrant' is one that authorises activities against a defined group of people – a 'target class'. A class is not necessarily made up of people who see themselves as having something in common, however, or who would commonly be recognised as a group. The shared characteristics that make them a class for the purposes of a warrant might only be apparent from an intelligence perspective.

A critical, unavoidable feature of a class warrant is that the decision on whether any particular individual falls within a target class is made by the intelligence agency holding the warrant. The warrant will authorise a range of activities against the target class, potentially up to the maximum level of intrusion the agency is capable of. These activities may begin (and possibly end) at any time within the term of the warrant, which may be up to 12 months. It is up to the agency to determine whether any particular person comes within the class definition. If the agency is satisfied they do, it can carry out the authorised activities against them.

Until the enactment of the ISA the NZSIS could not get a class warrant. Every warrant issued to the Service had to be in relation to a specified person or persons, place or facility. All NZSIS warrants targeting people were therefore 'individual warrants'. The GCSB, however, has long been able to get class warrants. They are effectively indispensable for signals intelligence – the GCSB's specialty – which typically involves collecting and aggregating data for subsequent filtering and searching.

In the past year I became increasingly concerned by the extent to which the NZSIS has moved to acting, almost exclusively, under class warrants. Superficially, at least, the ISA simply makes both class and individual warrants available. It provides no express guidance on when one should be preferred over the other. In my view, however, class warrants provide less protection for the rights of persons targeted under them than individual warrants. An application for an individual intelligence warrant submits the case for action against the person concerned to external scrutiny (by a Commissioner of Intelligence Warrants and Minister, if the agency targets a New Zealander). A class warrant application submits the case for action against the target class to external scrutiny, but not the particular case regarding each person who may be targeted. That case is made within the agency, eg to a designated manager. There is no scope for the warranting authorities to consider whether specific conditions or restrictions on the proposed activities might be required in light of the particular characteristics and circumstances of any individual target.

NZSIS investigations are often focused on particular individuals. Over many years of producing individual warrant applications the agency became proficient at putting together 'intelligence cases' in warrant applications for intrusive surveillance of specific targets. Such applications are now disappearing. They are being replaced by applications for warrants against classes of persons defined in terms of the NZSIS having assessed them as threatening national security. It has become apparent that a class warrant can be drafted to cover any NZSIS investigation, no matter how closely it might be focused on a particular person. With a relatively small set of class warrants in place, an individual coming to the attention of the Service may be assessed as coming within an authorised target class (a class possibly approved months beforehand). That person may then be put under surveillance, potentially up to the maximum possible level of intrusion (if that is what the warrant allows), without

their existence or any intelligence on them having been presented to anyone outside the NZSIS. That is obviously convenient for the agency. I seriously question whether it is consistent with the concept of a warrant as a safeguard for the rights of anyone prospectively in the sights of a state security agency.

I reviewed in depth a particular NZSIS class warrant emblematic of my concern. I questioned whether it was lawful or proper. Shortly before the end of 2022-23 I provided a classified review report on the warrant to the agency, its Minister and the Chief Commissioner of Intelligence Warrants. At the time of preparing this annual report the matter remained under discussion and I have a public report in preparation.

The lack of guidance in the ISA on when a class or individual warrant should be sought was noted in the recent independent review of the Act. The reviewers observed that "in principle" highly intrusive covert surveillance activities against any individual for national security purposes should be authorised by an individual warrant. My concern about NZSIS use of class warrants was developing as the review was nearing conclusion, so the reviewers were unable to consider the issue in depth. They recommended policy work be done to assess whether any statutory amendment is required. The Government response to the review remains under development.

Acquisition of bulk personal datasets

As I have noted in previous annual reports, the NZSIS is expanding its data holdings and looking to build its capability in data analytics. An element of this is the acquisition of bulk personal datasets. These are datasets that include personal information relating to a number of individuals (sometimes a very large number), most of whom are unlikely to be of intelligence or security interest, but some of whom might be. A commonly cited, though somewhat dated, illustrative example of a bulk personal dataset is a telephone directory. A more contemporary example might be a set of subscriber or customer information for an internet platform. Many such datasets are publicly available, including as a result of privacy breaches. For intelligence purposes, bulk personal datasets can be a source of possible leads when matched with other information, including other datasets. They can also contribute useful information on targets about whom little is known, particularly at the early stages of investigation.

An intelligence agency can lawfully acquire copies of bulk personal datasets that are publicly available. This could include datasets that have been disclosed or taken illegitimately if an intelligence warrant authorises the agency to collect such material. Internationally, intelligence agencies may share with one another datasets they have acquired or created lawfully under their respective legal regimes. The NZSIS, additionally, may get access to bulk personal datasets held by other New Zealand Government agencies through Ministerial-level Direct Access Agreements, provided for by the ISA. Currently the Act has a closed list of databases the NZSIS (or GCSB) may gain access to in this way, including information on registered births, deaths and marriages; citizenship; Customs information on people and goods crossing the border; and Police financial intelligence. The NZSIS seeks to have this list expanded. The recent independent review of the Act recommended amending the law to enable this, so it would state which government departments or agencies could enter agreements with the agencies, but not limit which databases within those departments or agencies could be available.[2]

[2] Sir Terence Arnold and Matanuku Mahuika *Taumaru: Protecting Aotearoa New Zealand as a free, open and democratic society* (Ministry of Justice, 31 January 2023), recommendation 16a.

Again as I have previously noted, the more an intelligence agency makes use of 'bulky' data (containing information on large numbers of people who are not of security concern), the more important are post-collection controls on access to and use of that data. This includes systematic recording of access and use, and justifications for searches, so both internal audit and oversight can check they are necessary and proportionate to a legitimate intelligence purpose. The Service is developing systems and procedures to support its growing reliance on data holdings and analysis, but mature and fully satisfactory arrangements are still some way off. The Service acknowledges this and for the moment I am satisfied it is proceeding with a proper degree of caution.

In the past year my office began a review of the Service's approach to the acquisition and use of bulk personal datasets. It became apparent from my preliminary research that the Service expects to make significant changes in the near future. I have decided to discontinue that review to avoid examining practices likely to be soon superseded. My office will continue to monitor developments and I will reassess the need for review when the Service has resolved its current questions about its direction and method.

At year end a review of the GCSB's approach to acquisition and use of bulk personal datasets was near completion. I will report on that in the coming year, but note here that the controlled exploitation of bulky data is a much more familiar and developed discipline for a signals intelligence agency (like the Bureau) than a human intelligence agency (like the Service). The more the Service moves into this kind of activity, the more it will need to develop control systems that resemble those applied in signals intelligence processing.

'Mosaic effect' argument for withholding intelligence and security information

The "mosaic effect" is the possibility that public release of individually harmless items of information might reveal sensitive information when pieced together. The concern for the intelligence and security agencies is that adversaries may seek to assemble information for insight into their operations and vulnerabilities. The agencies therefore consider "mosaic risk" when deciding whether to withhold or release information, eg in response to Official Information Act and Privacy Act requests. It may also be a factor in the agencies' views on what can and cannot be included in my public reports.

The concern with the mosaic effect as a ground for withholding official information is that it can involve speculation about risk that is difficult to validate or challenge. There is a risk of undue deference to arguments that releasing apparently unremarkable information might result in 'mosaic-making' that is hard to predict, but still an unacceptable risk to security. This may thwart a legitimate public interest in governmental transparency, as embodied in the "principle of availability" at the heart of the Official Information Act.

I support the view expressed by the Chief Ombudsman that an agency seeking to withhold official information on the basis of mosaic risk needs to set out clearly how its release can be expected to cause harm and what that harm will be.

In the past year this issue arose in discussions with the agencies about the public release of some agency internal guidance that, it seemed to me, would contribute to public assurance about agency compliance systems without compromising security. The agencies expressed concerns about mosaic risk, but eventually published a summary of the guidance at issue. My view remains that more detail could have been safely provided.

My office has engaged with the Office of the Ombudsman on reference to the mosaic effect as a ground for withholding information. I anticipate that will continue. My 2023-24 work programme

includes, as a possible review topic, the agencies' approach to assessment of security risk from official publication or disclosure of information on their activities.

NZSIS archives declassification

In July 2022 the NZSIS adopted a new archives declassification policy. This is a welcome development and follows an IGIS review of the classification system published in 2018, which recommended (among other things) introducing a topic-based approach to systematic declassification of historic classified records.

The Service has been piloting a systematic declassification process on a limited, 'proof of concept' basis, to test its policy. As yet the declassification policy is itself classified, though the Service has indicated an intention to publish an unclassified version once it has incorporated findings from its testing and confirmed a declassification work programme.

On one fundamental point of principle I have taken issue with the Service's approach. Its policy presumes that in some circumstances some information can remain classified indefinitely. However all NZSIS information is official information under the Official Information Act 1982 (OIA) and as such subject to the principle of availability. An assertion that some official information can be withheld in perpetuity appears clearly contrary to that principle. Although the OIA recognises conclusive reasons for withholding official information, they are contingent on specified harms being identifiable. Conclusive does not, in my view, necessarily equate to perpetual.

A principle against indefinite classification would not be novel or unique in the intelligence world: it has been applied in the United States for many years.[3]

Access to agency records

My office has extensive independent access to agency records systems. I do not think it is possible to overstate how important this is to the conduct of effective oversight within the limited resources of a small office. It enables independent research rather than reliance on agency disclosure. It enables a level of day-to-day familiarity with the work of agencies that intelligence oversight bodies in other jurisdictions struggle to maintain. It also relieves the agencies of a significant amount of work that would otherwise arise from requests for research and disclosure.

Though our access is extensive it is not total. I noted last year that the NZSIS had responded positively to requests for review and improvement of my office's direct access to its systems. This year I initiated the same discussion with the GCSB. It too has responded constructively, though not rapidly. As the year ended there were still some unanswered questions about the exact scope of our access and the reasons for a lack of default access to certain records. I hope to progress this work further in the coming year.

[3] Executive Order 13526 Classified National Security Information (December 2009) at section 1.5(d).

INQUIRIES, REVIEWS AND AUDITS

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 2022-23

Coordinated Review of the actions of the Police, Corrections and NZSIS in relation to the attack at LynnMall Countdown

In December 2022 I, the Independent Police Conduct Authority (IPCA) and the Corrections Office of the Inspectorate together reported publicly on the actions of the New Zealand Police, the Department of Corrections and the NZSIS in relation to Ahamed Aathill Mohamed Samsudeen, who attacked and injured seven people with a knife at an Auckland supermarket in September 2021. Mr Samsudeen, who was shot and killed by Police shortly after the attack began, had previously been imprisoned and was under close state surveillance due to his known violent extremist beliefs.

My contribution to the review covered the six-year period Mr Samsudeen was under investigation by the NZSIS and focused on whether the Service's decisions and actions to assess and mitigate the threat posed by Mr Samsudeen were lawful and proper. I examined files, emails, meeting minutes and intelligence reports and interviewed relevant NZSIS personnel. In summary I found the Service had lawfully shared intelligence on Mr Samsudeen with the Police and Corrections in a timely and proportionate manner.

Review of an NZSIS class warrant

As discussed earlier in the 'significant issues' section, this review examined an intelligence warrant issued to the NZSIS, authorising activities in relation to specified classes of persons. The warrant was sought to cover investigations that under past NZSIS practice would typically have been the subjects of warrants against individuals or smaller groups.

I was concerned that the warrant classes were too broad and it was difficult to make out the required legal tests of necessity and proportionality for all the activities against all the possible members of the target classes. It seemed to me to amount to a general warrant at common law, due to its lack of specificity.

I provided my report on the warrant to the Service, the Minister responsible for the Service and the Commissioners of Intelligence Warrants. The Service subsequently sought advice from Crown Law on the legality of the warrant. At year end I was preparing an unclassified public report of my review.

Review of a warning delivered by the NZSIS

In October 2022 I published a public report of this review, which examined an instance of the Service warning a target it was aware of their activity, which it considered a threat to national security, and

telling the target to stop. It provided an opportunity to examine in depth an operation in which the NZSIS took action intended to disrupt a threat.

I found that the planning of the warning at issue was reasonably thorough and recognised the uniqueness of the operation. The NZSIS took into account relevant factors to ensure the warning was carried out lawfully and properly. The warning itself did not convey the impression of enforcement.

I found some deficiencies in planning in relation to the consultation with another New Zealand government agency which had interest in the operation and I recommended that the NZSIS work to develop a more formal consultation process with relevant agencies.

I also recommended the Service develop a new policy in relation to warnings, which the Service had already committed to during the course of the review. I identified some issues I thought that should be addressed in such a policy.

Review of GCSB operations enabling Computer Network Exploitation (CNE)

Our work programme for 2022-23 included a review of GCSB's operations that enable it to conduct computer network exploitation (CNE). The baseline review was included in the 2021-22 work programme but was unable to be resourced at that time. The review examined the methods the Bureau uses to obfuscate its CNE operations and the procedures it follows to ensure those methods are properly authorised or otherwise lawful. It followed an earlier baseline review of the Bureau's CNE operations.

I produced a classified report of this review but the operations concerned are sensitive to an extent that precludes a separate public report. I found that the GCSB has reasonably robust systems in place to manage the operations, with compliance controls proportionate to the risks involved. A thorough planning process for the operations means that decisions and actions can be followed retrospectively, given a base technical understanding. A requirement to document operational proposals, on which the GCSB compliance team is consulted, followed by approvals for specific actions, provides a clear record of the legal and policy basis for an operation. Overall, the review did not identify any significant gaps in relevant policies and procedures, noting that the Bureau had recently implemented a new standard operating procedure.

I made one recommendation, for the GCSB to provide my office with access to relevant parts of its records system, as a matter of course, to enable more effective oversight of these activities. The GCSB agreed to do so and has taken steps to address this recommendation.

Review of GCSB acquisition and use of bulk personal datasets

In June 2023 I provided the GCSB with a draft classified report on this baseline review, which examined its approach to acquisition and use of bulk personal datasets. As discussed earlier in the 'significant issues' section, these are datasets that contain information about a large number of individuals, the majority of whom will not be of any intelligence interest. This review was originally proposed in the 2020-21 work programme (as a review of 'data matching'), but was deferred to enable progress on other work. My classified report was finalised in August 2023 and a public report was in preparation for 2023-24.

Unscheduled audit of NZSIS data stewardship

In May 2023 I completed an unscheduled audit of NZSIS procedures for reviewing its categorisations of individuals assessed as being of security concern or intelligence interest (but not requiring investigation). NZSIS may collect some basic information on such individuals, including some automatically collected information, but less than it can collect under an intelligence warrant.

An examination of this activity was not in my work programme, but my office noted a large and sudden increase in the number of overseas-based individuals categorised by NZSIS as being of interest. It emerged also that the NZSIS had decided to cease reviewing some categories to verify that the inclusion of people in them remained relevant. The previous review process had been introduced in response to a recommendation in an IGIS review in 2018 of over-collection of Advance Passenger Processing (air travel) data.

My audit found a number of issues regarding the changes in how NZSIS manages and reviews records on these individuals. My concerns included an absence of systematic necessity and proportionality assessments, data issues, and a lack of recording long-term trends and data. I recommended that NZSIS reconsider its review process and regularly record data on growth in the number of people it deems to be of some (albeit low) intelligence interest, to keep accurate records of trends.

The Service defended its process and clarified some aspects, particularly regarding possible information collection on New Zealanders. Though it has not accepted my recommendations, it has reduced my concerns to some extent. My office will continue to monitor the relevant processes and I anticipate revisiting the matter in future, by review or further audit.

GCSB collection against New Zealanders

My work programme for 2022-23 included a review of GCSB's collection against New Zealanders to examine the GCSB's systems and procedures for ensuring it complies with legal and warrant controls when collecting on New Zealanders. This review was carried over from 2021-22 but was paused while the GCSB undertook some relevant policy work. In early 2023 I made the decision to not proceed with this review as the questions originally prompting it had been sufficiently addressed by preliminary research for the review and by changes in GCSB policy.

The original cause for review was a series of self-reported compliance incidents in 2019-2020 involving inadvertent collection on New Zealanders under a Type 2 intelligence warrant (which authorises only collection on foreign nationals). In the last three years however my office has observed far fewer compliance incidents of a similar nature. Updated GCSB policy and procedure appears to have improved compliance with legislation and warrant controls, particularly nationality checks on proposed targets. The checks themselves have also become more robust.

Ongoing

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

During the 2020-21 reporting year I initiated an inquiry into the history of the GCSB's support to a signals intelligence system deployed by a foreign partner agency, with particular attention to the approach GCSB took to approval and authorisation of its contribution. This inquiry, which has required extensive searching of historic GCSB records, advanced significantly in the past year. A classified report has nearly been finalised and a public report has been provided to the GCSB for comment.

Review of GCSB and NZSIS open source intelligence collection

This is a baseline review of each agency's collection and use of open source (ie publicly available) information, including the use of specialised tools and methods. At year end draft reports were near completion and I anticipate producing a public report in the coming year.

Review of GCSB and NZSIS support to military operations

This review has examined how the intelligence support to military operations overseas is authorised, particularly when it requires Cabinet authorisation. At year end this work was near conclusion.

Review of NZSIS and GCSB human rights risk assessments

The Service and the Bureau undertake human rights risk assessments when sharing intelligence with, cooperating with, and receiving certain intelligence from overseas public authorities. In 2021, the agencies adopted a revised joint policy statement on managing human rights risk assessments. This review is examining a sample of assessments carried out under the policy. I expect to complete a report in early 2023-24.

Review of NZSIS target discovery projects

This review, begun in 2021-22, is examining the Service's approach to target discovery, which is directed at finding leads for security investigations. It initially focused on early target discovery projects but was re-scoped in late 2022-23 to encompass more recent developments. The review covers the Service's collection methods for target discovery purposes, its use and retention of data, and how target discovery is and is not affected by section 19 of the ISA, which protects freedom of expression. It will also examine in depth a particular, recent Service target discovery project.

Review of an NZSIS counter-espionage investigation.

In 2018-19, following review of a warrant issued to NZSIS, I began reviewing closely the associated counter-espionage investigation of a New Zealand citizen. The NZSIS investigation, which came to include some supporting activity by the GCSB, has been long-running and at the time of preparing this report was not concluded. My review has involved monitoring its progress and questioning the agencies (particularly the Service) about key actions, including mitigation/disruption activities and the basis for assessments. In the coming year I intend to conclude this review and consider what form of report, if any, is required.

Review of NZSIS information sharing with the Police

At year end a draft report on this baseline review, examining how the Service works with the New Zealand Police on counter-terrorism investigations, was near completion. The review began in 2020-21 but was paused to enable staff to work on the Coordinated Review (noted above), which also examines NZSIS-Police cooperation. The review is informed by the findings of the Coordinated Review but considers a broader range of counter-terrorism operations.

Review of the issue and execution of a NZSIS seizure warrant

This is a 'deep dive' review of the issue and execution of an intelligence warrant issued to NZSIS for the seizure of a dataset. It examines the Service's planning and decision-making for the seizure, how it obtained the data and its subsequent handling and use of it.

Review of NZSIS human source recruitment and management

This baseline review examines how the Service recruits and manages human sources. Using case studies, it examines the Service's relevant policies, procedures and practices, including payments and discontinuation. This review was started in 2021-22 and at year end a draft report was near completion.

Review of NZSIS use and sharing of vetting information

The Service conducts vetting to assess an individual's suitability to hold a national security clearance. The information the Service collects as part of the vetting process is highly sensitive and protected by both the Intelligence and Security Act 2017 and Privacy Act 2020. This review assessed the Service's compliance with these protections and examined the Service's relevant policies, procedures, and practices. A draft classified report was sent to the NZSIS at the end of June and an unclassified report will be released in early 2023-24.

Review of GCSB target discovery activities

GCSB target discovery activities are directed at finding leads for further investigation. This review will examine how the Bureau conducts these activities and whether the policies and procedures are fit for purpose. The review began in late 2022-23 and will carry over into the coming year.

Review of GCSB raw data sharing with partner agencies

The Bureau collects signals intelligence data and may lawfully share "raw" (unprocessed or minimally processed) collected data with partner agencies in other countries. This review has advanced intermittently since 2019, as resources have allowed. It has examined selected examples of operations involving raw data sharing, to assess how the Bureau ensures lawful and proper handling and use of the data concerned. I expect to complete a classified report on the review in the coming year.

Review of GCSB access to partner agency data

This review, completed in September 2022, examined the Bureau's systems and practices for ensuring that its access to data collected by its Five Eyes partners meets compliance requirements and is properly justified. It found that several relevant GCSB policies and procedures were out of date when the review began, though practice was generally sound. Justifications for use of partner data were generally clear and in some cases impressively comprehensive. Policies and procedures were largely updated by the time the review was complete and the Bureau acknowledged that my draft report had assisted with that. The Bureau's internal procedures for monitoring staff access to partner data were reasonably robust and effective. I recommended some clarification of the limits of those monitoring procedures in Bureau warrant applications; more systematic analysis by GCSB Compliance of self-reported compliance issues in accessing partner data; an improvement to internal communication of compliance issues; some changes to Bureau monitoring procedures; and an audit of a particular form of access to partner data. Due to the sensitivity of the systems and processes examined I am unable to report publicly in any further detail.

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 2022-23 are tallied in the following table. Additionally my office received and dealt with a further 23 contacts seeking information or raising issues that did not amount to complaints within my jurisdiction.

Complaints received 2022-23			
From	**Against GCSB**	**Against NZSIS**	**Total**
Members of the public	7	32	39
Intelligence agency employees or former employees	0	0	0
Total	7	32	39

The total number of complaints received in 2022-23 is roughly double the number in recent years, though the proportion requiring substantial investigation has not significantly increased.

NZSIS vetting

Two complaints regarding security clearance assessments required particular attention.

One complainant was concerned that a decision by a prospective employer to withdraw a job offer had been influenced by informal exchanges with the NZSIS, and the lack of a formal adverse finding made it difficult for the decision to be challenged. The key issue that emerged on investigation was whether the applicant had a “checkable background” due to time spent overseas in countries difficult to obtain information from. I found the NZSIS had handled the clearance application appropriately and made decisions in accordance with established policies and procedures. There was an opportunity, however, for the NZSIS to be more transparent about the options available for

background checks, to prevent misunderstandings in circumstances such as the complainant's. The Service accepted my recommendation to meet the complainant and explain what had happened in their case. It also agreed to provide more information for clearance candidates, detailed information for sponsoring agencies and additional training to relevant government agencies on background check processes. I appreciated the willingness of the Service to work constructively with the complainant and my office to resolve the matter.

Another complaint concerned a Service recommendation to a sponsoring agency to grant the complainant a security clearance, with a note that a specified security risk would need to be managed. The complainant questioned that and raised concerns about the reasons the NZSIS gave for its recommendation. In response to my inquiry the Service reviewed and revised its security clearance assessment and recommendation, acknowledged an error and apologised to the complainant. The Service revisited its view of the security threat it initially identified and acknowledged a need for care in assessing any security risk attributed to membership of a large voluntary community group on the basis of actions by a few members. The complaint also caused me to emphasise to the Service the relevance of positive security-conscious behaviour by the complainant.

NZSIS national security checks

In the past year 17 complaints against NZSIS related to the length of time apparently being taken for national security checks in immigration processes. The NZSIS provides advice to Immigration New Zealand on any potential security risks relating to an applicant for a New Zealand visa. There is no statutory timeframe for completing such checks. The Service is obliged, however, as it is in performing all its functions, to proceed with integrity and professionalism. I have engaged with it to understand the current state of its procedures for national security checks and how it works with Immigration New Zealand (INZ) to manage enquiries about applications. As a result of reviewing NZSIS visa screening processes two years ago I am aware that the two agencies have an ongoing programme of process improvement. To date I have not found any complaints necessitating inquiry. I will continue to assess each on its merits, though I am conscious also that a complaint to my office should not become a *de facto* means of accelerating one visa application at the expense of others, or creating a perception that this will occur. I will continue to take an interest in the systemic improvements being pursued by the NZSIS and INZ.

Public confirmation of a complaint investigation

Unusually, I was obliged in the past year to publicly confirm that I had received and was investigating a complaint about the NZSIS from a named individual. My legal obligation to conduct a complaint investigation in private means I do not normally do this. The law does not however prevent a complainant from speaking publicly about their complaint. This past year Mr Yuan (Jason) Zhao publicly stated that he had complained to me about NZSIS activities, prompting news media requests to me to confirm this. Mr Zhao advised he had no issue with me doing so. At year end my investigation was in progress.

WARRANTS

In this reporting year my office reviewed 61 warrants and business record approvals issued to the agencies. This was a small decrease on the preceding year (63).

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 allows the agencies to obtain business records from specific business agencies. A BRA is valid for six months.

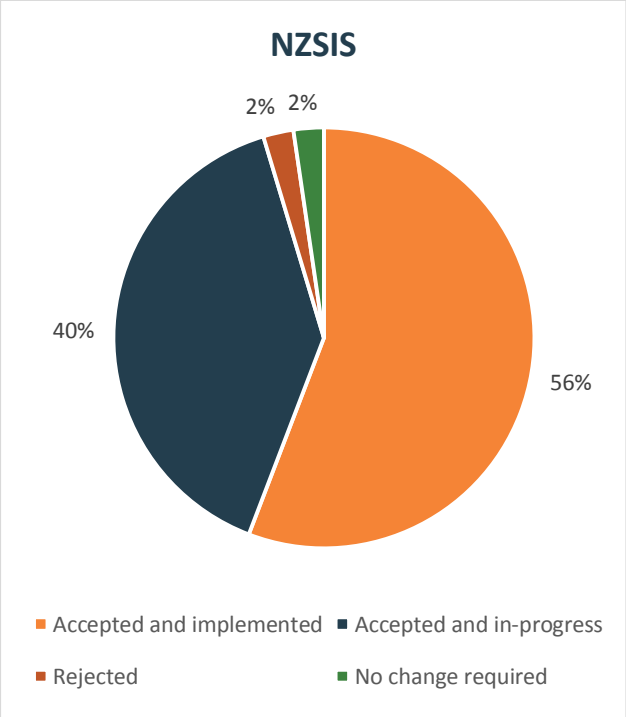
Intelligence warrants and business record approvals reviewed in 2022-23								
	Type 1 warrants	Type 2 warrants	Very Urgent	Practice warrants	Removal warrants	Revoked warrants	Business Record Approvals	Total
NZSIS	10	3	0	2	2	5	4	26
GCSB	15	12	3	1	0	2	2	35
Total	25	15	3	3	2	7	6	61

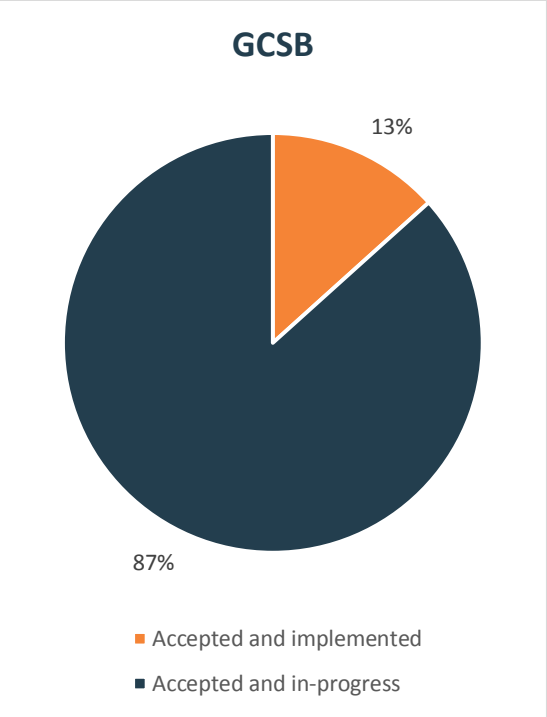
This year, the GCSB sought three very urgent authorisations under section 78 of the ISA. A very urgent authorisation allows the Director-General of an intelligence and security agency to authorise the carrying out of an otherwise unlawful activity for which an intelligence warrant is required. After authorising a very urgent authorisation the Director-General must apply for an intelligence warrant within 24 hours (as per section 55 ISA). A very urgent authorisation can only be sought if, under normal circumstances, an application for an intelligence warrant would be made but a delay in making that application would defeat the purpose of obtaining the warrant. I was advised of all three authorisations in a timely manner and considered all applications were properly made.

IMPLEMENTATION OF IGIS RECOMMENDATIONS

As a 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, will add value and promote compliance with the law. I seek and generally receive agreement from the agency that my recommendations will be implemented. I receive updates on the implementation process. The time needed for implementation varies: minor improvements might be easily made, but more systemic change takes longer.

Charted below are the numbers and status of the recommendations I have made over the last three years. The significantly larger number for the Service than the GCSB is due in part to recommendations arising from complaints about security clearance (vetting) assessments, which are a function of the Service not the Bureau. I note also that raw numbers of recommendations are not indicative of the seriousness of the underlying issues: a significant change might be captured by one recommendation, while multiple recommendations can arise where a system is largely functional but requires several minor improvements.





Status	NZSIS	GCSB
Accepted and implemented	24	2
Accepted and in-progress	17	13
Rejected	1	0
No change required	2	0

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.

Other integrity agencies

Among the other integrity and oversight agencies, my office works most frequently with the Office of the Privacy Commissioner. This year we have engaged on matters related to the Privacy Act and open source intelligence gathering. My office has also had useful discussions with the Office of the Ombudsman on Official Information Act matters.

I continue to 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 discuss 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 United Kingdom, United States, Canada, Australia and New Zealand. FIORC enables us to exchange views on subjects of mutual interest, compare practices in review and oversight and explore opportunities for cooperation.

For the first time since COVID-19, I was able to meet my FIORC counterparts in person, in Washington DC in November 2022. One outcome of particular value was the establishment of working groups to share knowledge and experience, including one on work programming and methodology led by my office.

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 year, I accepted 13 speaking opportunities, to academic, public service and intelligence sector audiences.

In May my office was invited to attend a cultural orientation programme hosted by the Federation of Islamic Associations of New Zealand (FIANZ). We were grateful to FIANZ for their time, knowledge and hospitality. We also heard in depth this year from the Classifications Office about how they classify violent extremist objectionable material and the trends they have observed. Staff from my office attended a number of conferences, including He Whenua Taurikura Hui in Auckland, the Trans-national Organised Crime Conference, the Public and Administrative Law Conference, and the National Security Conference hosted by Otago University.

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 2022-23 was 16 per cent under budget:

Office of the Inspector-General of Intelligence and Security 2022-23 Budget		
	Actual ($000s)	Budget
Staff salaries/advisory panel fees; travel	750	933
Premises rental and associated services	352	444
Other expenses	4	12
Non-Departmental Output Expenses (PLA)	664	664
Total	1,770	2,053

The under-spend was primarily due to holding an unfilled vacancy (since filled) and deferred rental charges.

For 2022-23 the office had a total staff of nine: the Inspector-General and Deputy Inspector-General; an office manager and an IT and security manager (0.8 and 0.62 FTE respectively), and five investigators. Functionally, investigative staff capacity was significantly reduced in the past year by illness and injury.

Premises and systems

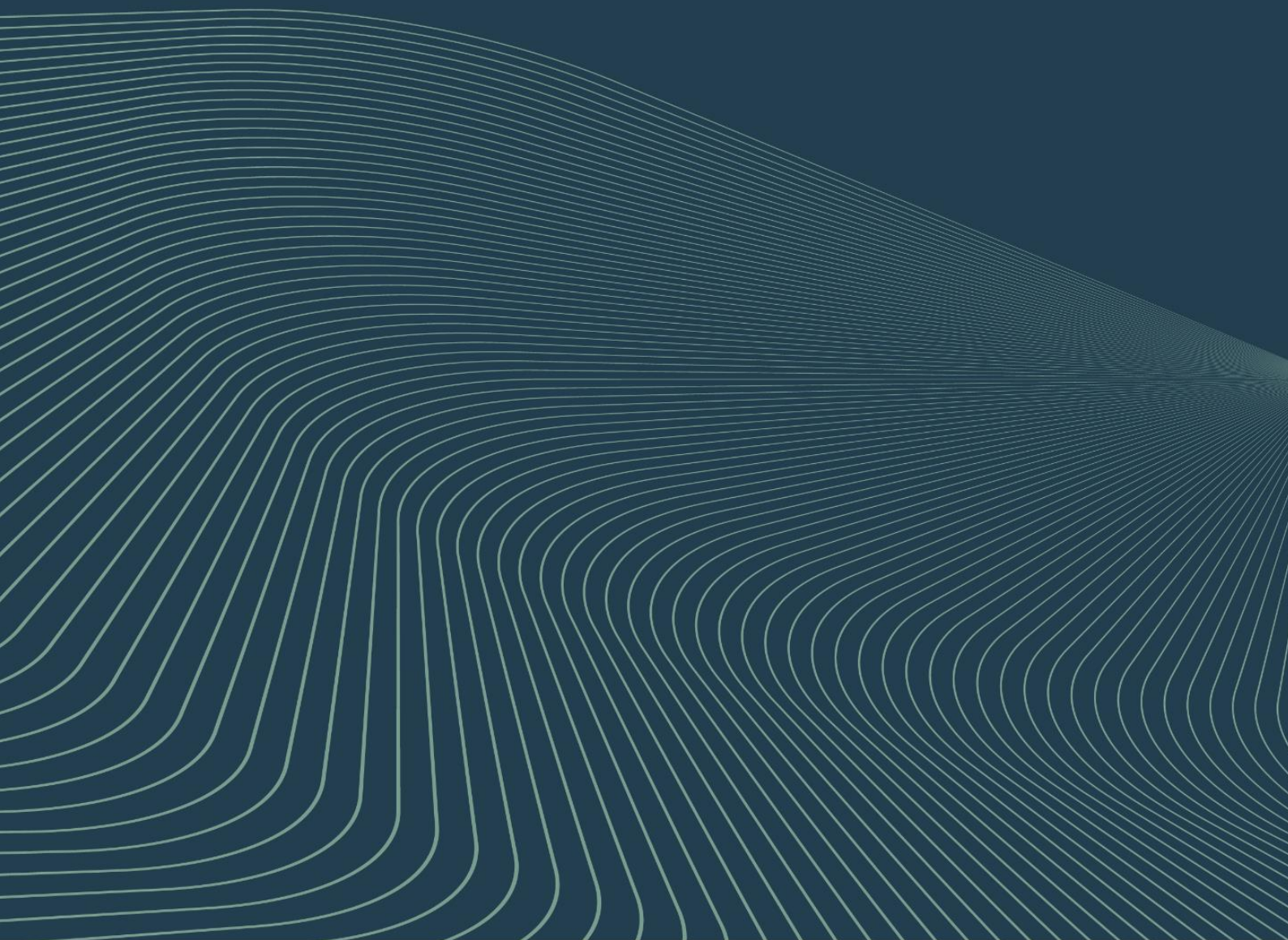
Since October 2019 my office has operated from secure premises in Defence House, Wellington. Current staffing is at the maximum the existing space can accommodate.

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 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 appreciate the assistance of the Ministry and the New Zealand Defence Force.

CERTIFICATION OF AGENCY COMPLIANCE SYSTEMS



CERTIFICATION OF AGENCY 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:

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.

Assessment for 2022-23

My assessment of the compliance systems of both agencies for 2022-23 follows, applying the framework above. For each heading I give the rating for each agency, then summarise the information underlying the assessment.

Operational policy and procedure

GCSB	NZSIS
Under-developed	Under-developed

Clear and coherent documentation?

Both agencies have substantial and wide-ranging suites of policies and procedures covering their operations. Generally, these are clear and concise.

At year end, 50 per cent of NZSIS policies and procedures were overdue for review. Although an improvement on last year (when 93 per cent were overdue), this is a significant backlog. In the meantime there is no assurance these policies are fit for purpose and some activities are guided by draft policies and procedures.

At the end of the year 42 per cent of Bureau policies were past their review date, although for 60 per cent of those a review was under way.

Both agencies have joint policies, such as those for corporate functions, of which 60 per cent are overdue for review.

Overall both agencies face a substantial task in bringing their internal policies up to date, making this the only area under assessment in which both rate as under-developed.

Well organised and effective dissemination of policies and procedures?

Both agencies' policies and procedures are accessible through their intranets and document management systems, by index or search. For both agencies, the intranet portal is the authoritative source of guidance, though at the time of reporting not all current NZSIS policies and SOPs had been uploaded.

Specialist policy staff?

The agencies' specialist policy resources reduced over the past year. At year end, the Service and Bureau both had one policy advisor and recruitment was underway. Both agencies rely on subject matter experts in operational roles to contribute substantially to operational policy development.

A programme of policy review?

The Service adopted a policy development framework in late 2022, intended to align policy development with organisational strategies and objectives. Accountability for delivery is assigned to senior staff. The Bureau has a senior governance group overseeing operational policy development and rationalisation. It met regularly in the past year to monitor and prioritise policy work.

Timely remediation of any deficiencies in policy or procedure?

Both agencies have improved leadership, direction and resources for policy development. Given the limited number of specialist policy staff, both agencies continue to make modest progress on policy development and rely on operational staff making time to develop or review policy. As noted above, the Service has fallen behind schedule in revising and updating policy.

Internal compliance programmes

GCSB	NZSIS
Well-developed	Well-developed

A compliance strategy informed by best practice and endorsed by senior leadership?

GCSB has a compliance strategy endorsed by its senior leadership. The Service plans to develop one. It has the elements of a strategic approach, including maintenance of operational policies and procedures; a commitment to training; promotion of self-reporting; and maintenance of capacity for compliance investigations, audits and advice. The Service is currently reviewing its compliance framework and audit charter.

Specialist compliance staff?

Both agencies continue to maintain small specialist compliance teams, which provide advice on operational policy questions, support policy development, carry out compliance reviews and audits, and investigate and report on self-reported compliance incidents. In the year under review both agencies' compliance and audit staffing decreased, although recruitment was under way.

A rigorous programme of compliance audits, covering significant functions and risks?

The GCSB planned for six compliance audits in 2022-23 and the NZSIS for seven. Both scaled down their audit plans, however, citing COVID-19, resourcing constraints and accommodation disruptions. At year end, the Bureau had completed three audits, and had two in progress. The Service had completed five. Postponed audits were rescheduled for 2023-24.

The Bureau also maintained regular audits of access to signals intelligence databases. Bureau audit staff remain responsible for compliance incident investigations, which seems inevitably to affect their capacity to complete audits.

Timely remediation of any shortcomings found by audits?

Both agencies' compliance teams track the progress and implementation of audit recommendations. Their records indicate that recent recommendations have either been implemented or are in progress. Bureau tracking indicates that internal acceptance and action on older audits remains unclear. Both agencies schedule follow-up audits.

Regular reporting to senior leadership and IGIS on compliance issues, statistics, trends and corrections?

Both agencies' compliance staff report regularly to senior leadership. They seek to identify any systemic issues underlying compliance incidents, but have limited capability to provide analytical reporting on statistics and trends. Both agencies share their internal compliance reporting with the IGIS office routinely or on request.

Proactive measures to maintain or improve compliance?

Both the NZSIS and GCSB use internal communication channels for proactive communication of compliance measures. These include 'town halls', internal email, team newsletters and their intranets.

Self-reporting and investigation of compliance incidents

GCSB	NZSIS
Well-developed	Well-developed

Promotion of compliance self-checking as part of normal operating procedure?

Both agencies encourage self-reporting of compliance incidents or suspected errors. Records show a steady level of self-checking before commencing activities and willing self-reporting of suspected or actual breaches.

Established policies and procedures for responding to compliance issues?

The NZSIS is in the process of updating its policies on assessment and investigation of compliance incidents. The GCSB has current compliance policies and procedures, approved in the previous financial year.

A supportive (rather than punitive) response to self-reporting of compliance issues and errors?

Generally, both agencies' internal reports and records continue to indicate that analysis and investigation of compliance incidents focuses on identifying systemic issues, rather than assigning individual blame.

Timely, thorough investigation and remediation of self-reported issues and errors?

In both agencies straightforward compliance incidents are usually analysed promptly. Investigation of more complex incidents falls to a small number of staff and generally proceeds slowly. Most incidents requiring investigation took three months to a year to resolve. Bureau investigations continue to vary widely in duration, with complex incidents commonly taking many months.

Timely reporting of compliance incidents to the IGIS?

Both agencies routinely report compliance incidents to the IGIS office without undue delay.

Training

GCSB	NZSIS
Well-developed	Well-developed

A training strategy including comprehensive induction and refresher training programmes?

Both agencies run induction and refresher training. This is often updated in response to legal guidance, compliance incidents or changes in policies or practices.

A systematic approach to assessing the effectiveness of training and identifying new or revised training needs?

Both agencies periodically review and revise their training programmes. They amend training material, where relevant, in response to compliance issues identified through internal audits, reviews and self-reported compliance incidents, and in response to IGIS recommendations.

In 2022-23, the Service re-designed its training on compliance with the terms of its Direct Access Agreement for Customs information. The Bureau updated its fundamental compliance training materials.

A dedicated training capability, typically requiring specialist staff and facilities?

Both agencies have specialist staff developing and delivering training. Both have an extensive suite of online training courses.

Responsiveness to oversight

GCSB	NZSIS
Well-developed	Well-developed

Open, constructive and timely engagement with the office of the IGIS?

The agencies' engagement with the IGIS office is generally cooperative and constructive. Differences of opinion and occasional tensions (including around access to specific agency information) inevitably arise, but interactions with agency staff are typically routine, professional and reasonably efficient. Both agencies occasionally volunteer briefings for the IGIS on new developments in their work, in addition to providing briefings on request. In the year under review, despite COVID-19, resourcing constraints and accommodation disruptions, responses from both agencies to questions and requests have been reasonably timely.

Timely articulation of an agency position on any compliance-related legal issues arising?

The agencies are generally cooperative and timely in articulating their views on questions of law.

Commitment of resources to deal with the requirements of IGIS inquiries and reviews?

Both agencies commit resources to dealing with oversight. They rely heavily on legal and compliance staff as points of contact for the IGIS office. When delays occur they are typically due to the small size and workloads of those teams, combined with the agencies' internal consultation processes.

Timely and effective implementation of accepted IGIS recommendations?

As reported earlier, most recommendations made in recent IGIS reviews and inquiries have been accepted by the agencies, and have been implemented or are in train.

Te Pourewa Mātaki
Inspector-General of Intelligence and Security