Te Pourewa Mātaki
Inspector-General of Intelligence and Security

Annual Report

For the year 1 July 2021 to 30 June 2022

Brendan Horsley
Inspector-General of Intelligence and Security
November 2022

CONTENTS

Te Pourewa Mātaki
Inspector-General of Intelligence and Security

2 November 2022

Rt Hon Jacinda Ardern
Prime Minister of New Zealand
Minister for National Security and Intelligence

Tēnā koe Prime Minister

Annual Report 2021-2022

Please find **enclosed** my annual report for 1 July 2021 – 30 June 2022.

The Intelligence and Security Act 2017 (the Act) requires you to present a copy of my annual report to the House of Representatives as soon as practicable after receiving it, with a statement as to whether any matter has been excluded from that copy (s 222). In my view there is no need for any material to be excluded. [The Directors-General of the New Zealand Security Intelligence Service and the Government Communications Security Bureau have confirmed that publication of those parts of the report that relate to their agencies would not be prejudicial to the matters specified in s 222(4) of the Act and that the report can be released unclassified without any redactions.] The Act also requires you to provide the Leader of the Opposition with a copy of the report (s 222(5)).

I am required to make a copy publicly available on my website as soon as practicable after the report is presented to the House (s 222(7) of the Act).

With your concurrence, and in accordance with s 222(8) of the Act, I am available to discuss my annual report with the Intelligence and Security Committee.

Nāku iti noa, nā

Brendan Horsley
Inspector-General of Intelligence and Security

Copy to: Hon Andrew Little
Minister Responsible for the New Zealand Security Intelligence Service
Minister Responsible for the Government Communications Security Bureau

PO Box 5609 Wellington 6140 New Zealand
+64 (0)4 460 0030 enquiries@igis.govt.nz

FOREWORD

I am pleased to present my office's 2021-22 annual report. It has been another interesting, varied and, at times, challenging year.

The coming year will see the conclusion of the first independent review of the Intelligence and Security Act 2017 (ISA) since its enactment. The review, required by the Act itself but brought forward by the Government in response to recommendations from the Royal Commission of Inquiry into the Terrorist Attack on Christchurch Masjidain, is considering whether the Act requires any improvements to ensure it is effective, clear and fit for purpose. At least some amendments seem likely: as with any new legislation, the ISA has technical imperfections that have been brought to light by working with it. Whether more substantive change is needed will be for the reviewers to recommend, the Government to propose and Parliament to determine. I will maintain a close interest, particularly in the arrangements for oversight, and provide whatever assistance I can.

Our work programme in the past year was unexpectedly altered by the tragic attack in the LynnMall supermarket on 3 September 2021, where seven people were stabbed and injured. In a first for our office, we participated in a joint inquiry, with the Independent Police Conduct Authority and the Corrections Inspectorate, into the actions of the New Zealand Security Intelligence Service (NZSIS or the Service), the New Zealand Police and the Department of Corrections in relation to the attacker. The engagement between the oversight bodies has worked very well and will serve as a model for future joint inquiries.

Progress with other items on my office's work programme for 2021-22 was also significantly affected by staffing constraints arising from COVID-19 precautions, illness and personnel changes. As a result our 2022-23 work programme comprises a number of items from the 2021-22 work programme that are still in progress or could not be advanced in the past year. As of early 2022-23 my office is almost back to full strength and I am confident our schedule of inquiries and reviews is back on track.

Working with other intelligence oversight bodies has been a feature of the past year. We hosted a virtual conference of the Five Eyes Intelligence Oversight and Review Council, which is made up of my office and equivalent oversight bodies from Australia, Canada, the UK and the USA. The conference provides an ideal opportunity to discuss differing approaches to oversight and to gain awareness of new areas of interest. Common issues faced by all intelligence oversight bodies included the difficulty of publishing enough about our work to enable public understanding and confidence that oversight is effective, while protecting sensitive information. We all face challenges, too, in keeping up with rapid advances in the technology of intelligence gathering from digital communications. I have raised the latter issue, and some potential solutions, with the independent reviewers of the ISA.

My office and I continue to have a productive relationship with the Directors-General and staff of both New Zealand intelligence agencies, the NZSIS and the Government Communications Security Bureau (GCSB or the Bureau). Recommendations I make for improvement in the course of my reviews and inquiries are generally accepted and implemented. There are times when we disagree but the debate is professional and reasoned. I consider this healthy tension to be a mark of a mature and functional relationship. Overall, I am satisfied the agencies are committed to undertaking their important functions in relation to national security lawfully and with propriety.

Finally, I want to acknowledge two important statutory appointments. First, Graeme Speden was appointed as Deputy Inspector-General in December 2021. Graeme brings a real depth of knowledge to the conduct of effective oversight. Second, I am very pleased to have the services of Ben Bateman

as my second advisory panel member. Ben is a former New Zealand Defence Force lawyer and advisor and is currently the deputy chief executive for Ngāi Tahu.

The breadth and diversity of experience on my advisory panel and in my deputy is of invaluable assistance to me and to the running of my office as we navigate the important issues for oversight in this dynamic environment.

Brendan Horsley
Inspector-General of Intelligence and Security

SIGNIFICANT ISSUES IN 2021-22

Every year issues arise that are not anticipated in our work programme. These issues emerge from meetings and discussions with the agencies, from their reports to us of compliance incidents, from our review of agency policies or warrants and from investigations of complaints. Discussing such issues with the agencies as they arise often leads to worthwhile adjustments to their operational practices and documentation. Reporting them contributes to public understanding of how the law applies to the agencies or is interpreted. The following are noteworthy matters that arose in 2021-22.

Review of the Intelligence and Security Act 2017

In March 2022 the Prime Minister notified the appointment of Sir Terence Arnold and Mr Matanuku Mahuika as independent reviewers of the Intelligence and Security Act 2017 (ISA).

The reviewers have engaged widely, including with my office. My staff and I have extensive experience of the Act in operation and have responded as frankly and comprehensively as we can to the reviewers' questions, particularly regarding provisions of the Act relating to oversight. In that area I have suggested some clarification of my ability to initiate reviews of agency activities; a provision enabling other agencies (eg the Police) to provide me with information relevant to an inquiry or review, but not held by the intelligence and security agency concerned; expansion of my Advisory Panel to three members; provision for a small pool of security–cleared experts who can provide me with advice on technical matters; and clarification of a provision on access to agency information for my staff. I am also interested in seeing what provision might be made for oversight of the National Intelligence and Security Agency proposed by the Royal Commission.

Target discovery

Among the recommendations of the Royal Commission for review of the ISA was to assess whether the Act provided sufficiently for the agencies to conduct "target discovery". This is the search for people or entities of legitimate interest to the intelligence agencies as potential security threats or sources of intelligence. If a national security agency such as NZSIS does not do target discovery it is reliant on others – such as overseas partner agencies, the Police and the public – to supply it with leads for investigation. The Royal Commission noted that this "classical model" of investigation is not well suited to identifying new threats from unfamiliar directions. It reported that both agencies appeared to have significantly increased their target discovery activity after the March 2019 attacks in Christchurch.

The Royal Commission expressed concern at the potential impact on target discovery of section 19 of the ISA, which declares that free expression, including advocacy, protest or dissent, does not "of itself justify an intelligence and security agency taking any action". This, the Royal Commission suggested, potentially posed "major problems" for target discovery activities involving monitoring or collecting from online platforms where extremist views are frequently expressed, such as far-right websites or forums.

My view, confirmed in the past year of oversight, is that s 19 poses no significant problem for the conduct of target discovery. While it is an important reminder of the need to respect and protect free expression, in effect it means simply that an intelligence agency must be able to cite some other information, besides the fact of certain ideas being expressed on a platform, to justify monitoring or collection. Typically this would be an association with threats or acts of violence, or some other activity

or characteristic relevant to the collection of intelligence in accordance with Government priorities. The agency must turn its mind to this, which is the value of s 19 and no great inconvenience. The agency is already seeking to optimise discovery by focusing its efforts where multiple indicators suggest they should go. Regard for s 19 is therefore consistent with an effective approach to target discovery, not an obstacle to it.

The potential hazard of target discovery activity, from a civil liberties and privacy point of view, is intrusion into the lives of people who have done nothing to merit the attention of a national security agency. This arises because target discovery is not prompted by information indicating that a certain person or entity requires investigation: it is the examination of information about people or entities in search of indications that they require investigation. This might be, for example, information about a group of people fitting certain broad criteria, or a large dataset of personal information within which an agency expects to find some items of intelligence value. Similarly to bulk data collection – the acquisition, by some signals intelligence agencies, of large volumes of communications traffic for storage and searching – target discovery will often involve collecting information relating to significant numbers of people of no intelligence interest, in pursuit of information on a few people who might be of interest. For that reason target discovery activities require attentive oversight, particularly for proportionality.

My office has a review of NZSIS target discovery activities under way and a review of GCSB target discovery activities scheduled. A scheduled review of both agencies' acquisition and use of bulk personal datasets is relevant, as is my office's review of warrants enabling acquisition of data that has target discovery applications.

"Disruption" activity by NZSIS

To what extent can the NZSIS act to disrupt or mitigate a threat to national security? The question arises because in a democracy that protects civil rights and liberties, the intrusive powers of intelligence agencies are typically balanced by a limited mandate to observe and report. Enforcement is left to other agencies, chiefly the Police, whose actions and methods are more open to scrutiny and challenge by the public and the Courts. The ISA accordingly specifies that the NZSIS' functions include collection, analysis and provision of intelligence, but it is "not the function of an intelligence and security agency to enforce measures for national security".

This does not mean the Service can do nothing to interfere with the activities of people it assesses as posing a threat to national security. It can, for example, issue a warning, so long as it does not imply it is exercising coercive powers associated with enforcement, such as arrest or the threat of legal sanction. It might warn the person whose activities are at issue (as in an example I have reviewed, where the warning was aimed at disrupting the target's activities on behalf of another state). Or it might warn others about the target's activities, eg community members, business associates or an employer. Such actions can obviously have serious and lasting effects on a person's relationships, community standing and employability.

It is not clear what else the Service can lawfully do as "disruption". There might be circumstances in which sharing intelligence is done for the purpose of avoiding or mitigating a threat. Even if the information is not phrased expressly as a warning, however, it may amount to an indirect one. In some circumstances, for example, information simply indicating to a person that their activities are known to others can be received as a warning.

The Service has not yet explored thoroughly the limits on what it might be able to do to disrupt or mitigate threats, but I expect it to do more in this area. In my view such actions require high certainty about the target's behaviour and a robust assessment that intervention is necessary and not better left to a law enforcement agency. From my review, although the Service has policy covering the delivery of warnings in some situations, I do not think it yet has a fully satisfactory policy framework for decisions in this area, or sufficiently clear understandings with other agencies (including the Police) that have relevant roles and functions.

Potentially the ISA, or a Ministerial Policy Statement under the Act, could be more prescriptive on what scope the Service has for disruption activities and how they are to be controlled, eg by authorisation. Legislative prescription applies in other jurisdictions. In Canada, for example, the Anti-Terrorism Act 2015 empowers the Canadian Security Intelligence Service to take measures to reduce a security threat, subject to obtaining a warrant from a Federal Court Judge if the measures would limit a protected right or freedom, or otherwise be contrary to Canadian law. If the NZSIS is increasingly to undertake disruption, it would assist oversight – and I think the Service itself – for the limits on such action to be clarified.

GCSB acknowledgement of computer and network exploitation

On 19 May 2022 the Director-General of the GCSB, Andrew Hampton, said in a speech to the Wairarapa Branch of the New Zealand Institute of International Affairs:

> Our legislation … allows us to access information infrastructures, which is more than just interception; "accessing information infrastructures" also allows us to retrieve digital information directly from where it is stored or processed. This type of activity is sometimes referred to as computer network exploitation, or CNE, but we prefer to use the term "accessing information infrastructures" in line with the wording in our legislation.

Until this speech the fact that the Bureau does computer network exploitation (CNE) was highly classified. Although it was subject to oversight, it was not possible to provide any clear public assurance of this. For that reason the Director-General's acknowledgement of CNE is welcome. It enables me, if only in the limited terms enabled by the continued classification of operational details, to report on the Bureau's use of this important capability.

My last annual report noted the completion of a review of "GCSB's conduct of certain operations to access information infrastructures", which were "classified to an extent that effectively precludes public reporting". This was in fact a review of the Bureau's compliance systems for the conduct of CNE operations. It found those systems to be generally effective and appropriate. It is useful to be able to say that publicly.

CNE is a broad descriptor. It is, however, more informative in my view than "accessing information infrastructures". Generally, I do not share the Bureau's preference for the latter term, despite its appearance in the ISA.

GCSB requests for partner-collected data

In my last annual report I noted that the GCSB had reached the view that the law does not require it to seek an intelligence warrant to request signals intelligence data from its Five Eyes partner agencies, when that data has already been collected by the partner. Essentially this rests on the presumption that the partner agency has collected the data lawfully and the fact that any data supplied to GCSB is shared by agreement. Further, so long as the Bureau's requests are made to fulfil New Zealand

Government intelligence priorities, in accordance with procedures designed to ensure necessity and proportionality, they will generally be reasonable and so not in breach of the right against unreasonable search and seizure under the New Zealand Bill of Rights Act 1990.

While differing from the Bureau on some points of statutory interpretation I accept the ultimate conclusion that a warrant is not legally required. The Bureau continues, as a matter of policy, to seek warrants for requests to search partner-collected data relating to New Zealanders. That ensures the justification for such requests is examined by the Bureau's Minister and a Commissioner of Intelligence Warrants. All such warrants are reviewed by my office.

At the time of my last annual report the GCSB was still working on policy and procedure to control requests for searches of partner-collected data without a warrant, so was still seeking warrants for all such activity. In the second quarter of the past year, however, the GCSB finalised the relevant policy and procedure. Now, as planned, it seeks warrants for requests to search partner-collected data only when it anticipates doing so in relation to New Zealanders. My office reviewed the relevant policy and procedure in the course of a broader review (reported later) of GCSB compliance systems for access to partner data. The requirements include thorough record-keeping of requests and the reasons for them, regular internal audits and annual reporting to the Minister. I anticipate these measures being of value for oversight purposes and my office will see how they are implemented.

NZSIS Direct Access Agreements

Under the ISA the NZSIS can acquire access to specified public sector databases through Direct Access Agreements (DAAs) between relevant ministers. Existing DAAs include one for access to Advance Passenger Processing (APP) data (on air passenger movements) held by the Ministry of Business, Innovation and Employment, access to New Zealand Customs' primary operational database (CusMod) and access to the Department of Internal Affairs Births, Deaths and Marriages and Citizenship database.[1] By law a DAA must be reviewed every three years, including consultation with my office and the Privacy Commissioner.

In September 2021, the Service notified me that it had drafted a DAA for access to the New Zealand Police Financial Intelligence Unit database. A draft was provided to my office and the Privacy Commissioner for consultation. At year end, the DAA remained in progress.

In October 2021 the Service informed me it was reviewing its DAA with the Department of Internal Affairs. It supplied a revised draft agreement in December 2021. I was pleased to see the Service take comments and advice provided by my office and the Privacy Commissioner into consideration in the final version. At the end of the financial year the revised DAA was awaiting Ministerial approval. This was a relatively quick and efficient review and consultation process, with only minor delays in the process, primarily due to Covid-19 and the Service facing accommodation disruptions.

In my last annual report I noted slow progress on reviews of NZSIS DAAs for access to New Zealand Customs' main operational database (CusMod) and to Advance Passenger Processing (APP) information, on air passenger movements, held by the Ministry of Business, Innovation and Employment. My office and the Privacy Commissioner continued to engage with NZSIS on these in the first half of the past year. At the time of writing, however, although the reviews have been completed, revised agreements are yet to be approved. By law a DAA must be reviewed every three years. It is now two and a half years since the reviews of these two agreements began. This is not a timely process

[1] DAAs are publicly available via the NZSIS website.

for updating the terms and conditions for NZSIS access to considerable data repositories, including personal information about New Zealanders and others. I recognise that the timetable is not wholly under the Service's control. There is no statutory timeframe for completion of a review and conclusion of a revised agreement. Perhaps there should be.

Information sharing with foreign partners and human rights abuses

In my last two annual reports I have commented on my office's engagement with the agencies on the test for when they may share information with a foreign partner agency if there is a risk it will contribute to human rights abuses.

The agencies' management of human rights risks in overseas cooperation is the subject of a joint NZSIS/GCSB policy statement (JPS). I was concerned that this policy, dated 2017, was insufficiently protective of rights. It was due for review in 2019, but this waited on a review of the Ministerial Policy Statement (MPS) on Cooperation with Overseas Public Authorities. A revised MPS was approved in April 2021 and the agencies finalised a revised JPS in December 2021. It is in my view a marked improvement on the 2017 policy, although I continue to maintain some reservations on important details, namely the terms employed in risk thresholds; specific criteria and definitions for overseas bodies; and the handling of reports likely obtained by torture. I have also proposed that for transparency the majority of the JPS could be made public.

The agencies published on their websites in June 2022 a significantly abbreviated summary of the policy. I continue to engage with them on whether a more comprehensive publication is feasible without harm to national security.

Agency data management

In December 2021, the GCSB adopted a new data retention and destruction policy. Since the enactment of the ISA it had been working with an interim policy that its own auditing had identified as difficult to implement and probably not fit for purpose. The new policy (which is classified) is relatively simple and clear, putting data into categories aligned with the intelligence production cycle, and applying default retention time limits for each. Unlike the interim policy, which could not be applied effectively across all relevant operations, the new policy expressly covers all data obtained or created in performance of the Bureau's intelligence and protective security functions. The Bureau expressly adopts the position that it may not retain information merely because it may be useful for its functions in the future: it must have a demonstrable future use. The new policy appears to be an improvement on the old. The proof will be in its implementation.

I noted last year that the Service was facing new data management challenges as a result of its heightened commitment to target discovery, which includes more data analysis and acquisition. This approach continues to amplify NZSIS data holdings significantly. International jurisprudence and good practice emphasise the importance, when "big data" analysis is used for intelligence purposes, of a suite of checks and controls applying throughout the process – from acquisition, through storage and access controls, search procedures and justifications, record-keeping, audit and amenability to oversight. The Service is in the process of developing the necessary systems and processes, but – as it acknowledges – it is not there yet. I continue to take a keen interest in its progress.

The Service responded positively in the past year to requests for review and improvement of my office's direct access to its records. It was cooperative in reviewing our default access arrangements

and enabled access to a new, extensive search capability. I appreciated the agency's recognition that our ability to search agency records independently is critical to effective oversight.

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 we have a good understanding of agency operations and recommending improvements to compliance systems where necessary.

As far as possible we 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.

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 GCSB records, advanced significantly in the past year and will be completed in 2022-23.

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

On 3 September 2021, Ahamed Aathill Mohamed Samsudeen attacked and injured seven people with a knife at a supermarket in New Lynn, Auckland. He was shot and killed by Police shortly after the attack began. Mr Samsudeen had been under close state surveillance since his release from prison seven weeks earlier, due to his known violent extremist beliefs.

The Independent Police Conduct Authority (IPCA), the Corrections Office of the Inspectorate and I began a coordinated review into the actions of the New Zealand Police, the Department of Corrections and the NZSIS in relation to Mr Samsudeen before the attack. The Police shooting of Mr Samsudeen is being investigated separately by the IPCA and Police.

My contribution to the coordinated review focused on whether NZSIS decisions and actions to assess and mitigate the threat posed by the attacker were lawful and proper. At law it is a self-initiated inquiry. Coordination with the other oversight bodies enables us jointly to examine the extent to which there were collective decisions about strategies to assess and manage the risk presented by Mr Samsudeen.

The coordinated review advanced substantially in the past year and will report publicly in 2022-23.

Review of NZSIS information sharing with the Police

This baseline review, examining how the Service works with the New Zealand Police on counter-terrorism investigations, was begun in 2020-21. It was paused to enable staff to work on the coordinated review (above), which also examines NZSIS-Police cooperation. Completion of the coordinated review in 2022-23 will enable us to resume the baseline review in the coming year. The findings of the coordinated review will be relevant, but the baseline review will consider a broader range of operations.

Review of NZSIS and GCSB engagement with international partners

This review examined agreements and procedures designed to safeguard the interests of New Zealand and New Zealanders when the agencies collaborate with those of other nations, particularly their partner agencies in the Five Eyes countries. As noted in my last annual report, a draft classified report was supplied to the agencies at the end of 2020-21. The report was finalised in December 2021. The sensitivity of the arrangements examined means a public unclassified report is impracticable and so the review is summarised here.

The review found a significant difference between the GCSB and the NZSIS in the extent to which arrangements with partner agencies regarding any intelligence collection against New Zealanders are formally prescribed. The Bureau and its Five Eyes partner agencies have long-standing rules and checks on any proposed signals collection against their own nationals. These are mutually recognised between the partners, each of which has complementary policies, procedures and training programmes to enforce them. The Service has established expectations with partner agencies that it will be informed of any proposed intelligence activity against a New Zealander or within New Zealand, but limited formal documentation of these expectations and no mutually operative compliance procedures.

While the difference in the extent and formality of the safeguards between the signals and human intelligence agencies is initially striking, my review found it was less of an issue than might first appear. The higher specification of controls on signals intelligence collection against Five Eyes nationals by the Bureau and its partners reflects their ability to operate remotely and the higher potential for technical collaboration between them. The Service and its human intelligence agency counterparts do not have the same capacity to operate remotely or seek the use of partner capabilities against their own nationals.

I recommended the Service consider my report in updating an operational document, which I found could more accurately represent NZSIS expectations of partner agencies.

Review of NZSIS visa screening

This review looked at NZSIS systems and procedures guiding its assistance to Immigration New Zealand with the screening of visa applications from people wanting to travel, work, study or reside in New Zealand. I provided a summary of this review in my last annual report. In November 2021 I published on my website an unclassified report of the review.

Review of NZSIS framework for disclosure of information about crime

While collecting intelligence the Service sometimes obtains information about criminal acts unrelated to national security. At law it has discretion on whether to disclose such information to the Police. This review examined how the Service makes decisions on disclosure, examining relevant policy and some examples from a counter-terrorism investigation. I summarised the outcome of this review in my last annual report. In December 2021 I published an unclassified report.

GCSB access to partner agency data

This review 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. The review began in 2020-21 and I provided GCSB with a draft classified report in the first quarter of 2021-22. Personnel changes and illness in my office then delayed progress, although the report was near final by the end

of the year. Due to the sensitivity of the systems and processes examined there is little if any scope for an unclassified public report and I anticipate reporting the outcome of the review, to the extent possible, in my next annual report.

NZSIS and GCSB role in first Control Order

The first Interim Control Order under the Terrorism Suppression (Control Orders) Act 2019 was issued by the High Court in May 2021, in respect of an individual then expected to return to New Zealand from overseas and considered to present a risk of providing financial support to Islamic State and promoting its ideology to others. The Interim Control Order was issued for 12 months, expiring in August 2022. Any identifying particulars of the subject were subject to suppression orders.

This baseline review examined what if any intelligence or information the agencies contributed, directly or indirectly, to the Control Order application, which was made by the Commissioner of Police (with assistance from Crown Law). The review has been completed. I made no recommendations and do not expect to produce any further public report.

A warning delivered by the NZSIS

This review 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 (see the discussion of disruption activity in the "Significant issues" section of this report). I expect to have published a public report of the review by the time this annual report is released.

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. My review has involved monitoring its progress and questioning the agencies (particularly the Service) about key actions, including mitigation/disruption activities, and assessments. I will consider in the coming year whether to continue or terminate the review.

NZSIS and GCSB support to military operations

This baseline review examines what current support the intelligence agencies provide to New Zealand military operations, along with current policy. It follows past IGIS inquiries into the agencies' involvement with the CIA during the 'war on terror' and, following publication of the book *Hit and Run*, into NZSIS and GCSB activities relating to Afghanistan. The review brings aspects of those inquiries up to the present, including considering whether previous IGIS recommendations relevant to support to military operations have been implemented. Separate classified reports on GCSB and NZSIS are in draft. Key questions emerging from the review are how the agencies identify what comprises 'support to military operations', and determine when support to military operations requires a specific mandate from Cabinet. Some of these matters have proved complex to address. I expect to complete and report on this review in the coming year.

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 examines 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.

GCSB and NZSIS acquisition and use of bulk personal datasets

This baseline review is to examine the agencies' acquisition and use of bulk personal datasets. It was originally proposed in the 2020-21 work programme (as a review of 'data matching'), but deferred to enable progress on other work. Preliminary research began in the past year. As a result the parameters and sequencing of the review have been revised. I expect to progress this review, beginning with the GCSB, in 2022-23.

NZSIS use and sharing of vetting information

The Service conducts security clearance assessments (vetting) to assess individuals' 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 will assess the Service's compliance with these protections and examine the Service's relevant policies, procedures, and practices. Preliminary research and planning was done in late 2021-22 and I expect to complete a classified report in the coming year.

NZSIS human source recruitment and management

This baseline review is examining how the Service recruits and manages human sources. Using case studies, the review will examine how the Service's practices align with the relevant policies, procedures and practices. This review was under way in 2021-22 and continues in the coming year.

NZSIS target discovery projects

The NZSIS' target discovery effort is directed at finding leads for security investigations. This review, begun in 2021-22, is examining selected target discovery projects. The context for this review is discussed in the 'significant issues' section of this annual report.

COMPLAINTS

The investigation of 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 has a right to 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.

Each year my office receives a significant number of contacts from people expressing concern that they are under some form of covert surveillance or attack. Many of these are effectively requests for personal or official information under the Privacy Act 1993 or Official Information Act 1982. The most appropriate first step is generally to direct their request to the agency or agencies that might hold the information, with a right of complaint to the Privacy Commissioner, Ombudsman or my office if the response is unsatisfactory. Such contacts are not counted as complaints.

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 2021-22			
From	*Against GCSB*	*Against NZSIS*	*TOTAL*
Members of the public	7	14	21
Intelligence agency employees or former employees	1	2	3
Total	8	16	24

Additionally my office received and dealt with a further 58 contacts seeking information or raising issues that did not amount to complaints within my jurisdiction.

WARRANTS

In this reporting year my office reviewed 63 warrants issued to the agencies. This was a small decrease on the preceding year (77).

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.

	Type 1 warrants	Type 2 warrants	Practice warrants	Removal warrants	Total
NZSIS	20	4	2	1	27
GCSB	19	16	1	0	36
Total	39	20	3	1	63

One of the Type 1 warrants issued to the NZSIS was sought under the urgency provisions of the ISA, which enable the application to be made orally or in person, subject to automatic revocation unless the warrant is confirmed in response to a written application made within 48 hours.

In my last annual report I noted some concerns with warrants issued to the Service for seizure of datasets. Although it had specific datasets in mind when it sought the warrants, it had not identified them in its applications. I was concerned also that the warrants defined the targeted classes of datasets so broadly as to be almost general-purpose. In the past year the Service revised its approach. It provided more information in warrant applications on datasets it intended to collect and, in some relevant warrants, identified thematically the intelligence purposes it expected target datasets to serve.

This year my office has continued to engage with the Service on intelligence warrants related to the seizure and retention of datasets. In the absence of a specific statutory framework for this activity, warrants are a key component of the NZSIS' emerging model for the acquisition and (in some instances) long-term retention of such information. As noted earlier in this report (under the heading "significant issues") this model is not yet fully adequate. I expect this to remain a key issue in my office's reviews of warrants in the coming year.

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:

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 2021-22

My assessment of the compliance systems of both agencies for 2021-22 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
Well-developed	Under-developed

Clear and coherent documentation?

Both agencies have substantial and wide-ranging suites of policies and procedures covering their operations. In general these are competently drafted and coherent.

At year end, however, 93 percent of NZSIS policies were overdue for review. In some areas of NZSIS operations, including data analytics and engineering, planned policies and procedures were non-existent and draft procedures were being relied on to guide decisions. Unusual pressures including coronavirus and accommodation issues contributed to this, but the result is a backlog of policy review that will require significant effort to clear. In the meantime there is no assurance these policies are fit for purpose.

Near the end of the past year 46 percent of Bureau policies were past their review date, although for just over half of those a review was under way. Overall the Bureau assessed 53 percent of policies as fit for purpose, 20 percent as partially fit and 27 percent as not fit. Half of those assessed as unfit for purpose were assessed as high risk: reviews of all these were in progress.

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. The Bureau updated its intranet policy pages in the past year to remove obsolete policies from circulation and collated the policies by directorate. The Service's policy portal remains their authoritative source of guidance, although it is not yet a complete or fully accurate resource.

Specialist policy staff?

Both agencies' specialist policy resource remained static: the Service with two staff, and the Bureau with three. Both agencies continue to rely on subject matter experts in operational roles to contribute substantially to operational policy development.

A programme of policy review?

The Service continued a policy simplification project begun in 2019-20, following a review of its operational policies in 2018-19. This reduced the number of its policies by 20 percent. At year end it was developing a plan to address its backlog of policies overdue for review.

The Bureau has a senior governance group overseeing policy development and rationalisation. The group 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. They continue to make modest progress on policy given their few specialist policy staff and reliance on operational staff making time to develop or review policy. As noted above, the Service has fallen significantly 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?

Last year I noted that neither agency had a compliance strategy documented as such and endorsed by its senior leadership, but both proposed to develop one. This is yet to occur, although both agencies have 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. GCSB revised its compliance policies and procedures in the past year. The Service has identified a need for, but not yet progressed, a review of 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 maintained relatively steady levels of staffing across the compliance and audit function.

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

Both agencies planned 10 audits in 2021-22, with the GCSB intending further spot audits. Towards the end of quarter two, however, citing Covid and accommodation disruptions, both scaled down their audit plans. At year end, the Bureau had completed four of seven planned audits, with two in progress. The Service had completed seven of eight, with one in progress. Postponed audits were rescheduled for 2022-23. 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?

NZSIS compliance team tracking of progress on audit recommendations indicates that recent recommendations have been implemented or are in progress. Bureau tracking indicates reasonable progress on more recent recommendations although internal acceptance and action on some 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 routinely or on request.

Proactive measures to maintain or improve compliance?

Both agencies use internal communications to enhance compliance awareness. The Service has continued a regular intranet blog on compliance issues, with an associated message board. The Bureau recently created online interactive guidance documents.

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 indicate 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 policy on handling compliance issues was due for review in mid-2020 but has yet to be updated. The policy is high-level, so assessment and investigation of compliance incidents relies significantly on the skills and experience of compliance staff. The Service has scheduled the policy for review in 2022-23. Revised GCSB compliance policies and procedures were approved early in the reporting year. The updated documents enables the Bureau to be less reliant on the institutional knowledge and skills of key staff members and ensures best practice can be adhered to.

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

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

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

Although 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 between three months and a year to resolve. Bureau investigations continue to vary widely in duration, with complex incidents commonly taking many months to resolve.

Timely reporting of compliance incidents to the IGIS?

Both agencies routinely report compliance incidents to the IGIS 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. The Bureau produced a new Compliance Essentials training course: a mandatory yearly course for all staff to ensure compliance with the ISA. Alongside the mandatory compliance training, the Bureau released new detailed training modules for operational staff and expanded their core compliance modules. The Service updated their mandatory human rights training and included a new, specialised human rights training course.

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 also 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 2021-22, the Service re-designed their human rights training, including an advanced course for staff who cooperate with foreign partners, and introduced new information management training. The Bureau turned newly implemented polices into online interactive documents to complement traditional online training modules and held drop-in sessions to discuss new policies.

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 this 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. Despite COVID-19 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?

Fewer questions of legal interpretation arise with the passage of time since the ISA was enacted: a number of difficult matters have been worked through. The agencies are generally cooperative in articulating their legal positions.

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

Both agencies commit resources to dealing with oversight. They continue to rely heavily on their legal and compliance teams as points of contact for the IGIS. Where delays arise, they are typically due to the small size and consequent heavy workloads of those teams, combined with the agencies' internal consultation processes. Both agencies' ability to respond to oversight was affected in the past year by Covid-19 and accommodation issues.

Timely and effective implementation of accepted IGIS recommendations?

Most recommendations stemming from our more recent reviews and inquiries have been accepted by the agencies, and have been implemented or are in train.

OUTREACH AND ENGAGEMENT

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. My office hosted a virtual annual FIORC conference in late 2021, replacing an in-person conference scheduled for 2020 but cancelled due to the coronavirus pandemic.

Advisory Panel

The ISA establishes a panel of two people to advise the Inspector-General. Lyn Provost chairs the panel and in December 2021 Ben Bateman was appointed for a term of five years. The Advisory Panel met four times in the reporting period.

Other integrity agencies

Among the other integrity agencies, my office works most frequently with the Office of the Privacy Commissioner. This year we collaborated on matters including comment on revised NZSIS Direct Access Agreements.

This year I also worked closely with the Independent Police Conduct Authority and the Corrections Office of the Inspectorate on the coordinated review of the actions of the Police, Corrections and NZSIS in relation to the attack at LynnMall Countdown (discussed earlier in this report).

My deputy and I met and provided information to officials working to establish an independent Inspector-General of Defence, an office I anticipate engaging with in due course.

I continue to participate in the Intelligence and Security Oversight Coordination Group, with the Privacy Commissioner, the Chief Ombudsman and the Auditor-General.

Public and sector group presentations

I accepted six speaking opportunities during the year, to academic, public service and intelligence sector audiences.

Website and branding

This year when an upgrade of my website was due I took the opportunity to refresh its design and adopt a logo for the office. This annual report is the first to use the logo and associated publication elements.

FINANCES AND ADMINISTRATION

Funding and resourcing

The IGIS office is funded through two channels. A Permanent Legislative Authority (PLA) covers the remuneration of the Inspector-General and Deputy Inspector-General. Operating costs are funded through Vote Justice, as a non-departmental output expense. Total expenditure for 2021-2022 was 21 percent under budget:

Office of the Inspector-General of Intelligence and Security 2021-22 Budget			
	Actual (000)	Budget (000)	Variance (over)/under
Staff salaries/advisory panel fees; travel	683	950	267
Premises rental and associated services	513	589	76
Other expenses	1	50	49
Non-Departmental Output Expenses (PLA)	554	644	90
Total	1,751	2,233	482

The under-spend was due to a number of factors and not indicative of the true operating costs of the office. For most of 2021-22 the office had a total staff of six (excluding the Inspector-General and Deputy Inspector-General): an office manager, an IT and security manager, four investigators. Parental leave and delays between filling vacancies and staff commencing in role (mainly due to the time required for security clearances) accounted for the under-spend in staff salaries. At year end the office had a staff of eight, one of whom was seconded out of the office. The Deputy Inspector-General was not appointed until December 2021, accounting for the under-spend in the PLA.

The 2021-22 premises, rental and associated budget included a transfer of $100,000 from the previous year. It was anticipated that this would be used to fund a significant and necessary website and IT upgrade and to host the Five Eyes Intelligence Oversight and Review Council conference. The IT and website upgrades came in under budget, however, and the conference was held virtually.

Premises and systems

Since October 2019 my office has have 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 early 2020 as compliant with the requirements of the New Zealand Security Information Manual. The next assessment is due in 2023.

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 human resources advice and support, is provided by the Ministry of Justice. These arrangements are efficient and appropriate given the size of the office.

Te Pourewa Mātaki
Inspector-General of Intelligence and Security