
# Office of the Inspector-General of Intelligence and Security

---

**Annual Report**

For the year 1 July 2020 to 30 June 2021

---

Brendan Horsley
**Inspector-General of Intelligence and Security**
11 November 2021

# CONTENTS

**OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY**

11 November 2021

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

Tēnā koe Prime Minister

**Annual Report 2020-2021**

Please find **enclosed** my annual report for 1 July 2020 – 30 June 2021.

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

P O Box 5609, Wellington 6140
enquiries@igis.govt.nz
Phone: 04 460-0030
@igisnz

# FOREWORD

I am pleased to present the 2020-21 annual report. This is my second annual report but it follows my first full year in the role of Inspector-General. It has certainly been an interesting, varied and productive 12 months. Once again I wish to thank my small team of hard-working investigators and office support staff for their continued high standard of work. They have continued to deliver on our work plan despite a number of significant staff movements.

I would like to single out the invaluable contribution of Graeme Speden, who has been acting Deputy Inspector-General for the bulk of this year. I also wish to thank the outgoing chair of my Advisory Panel, Angela Foulkes, for her valued counsel over the past year. I hope that by the time of publication of this report the appointment of a new Deputy and Advisory Panel member will be confirmed.

Over the year the office has conducted numerous reviews into the activities of the New Zealand Security Intelligence Service (NZSIS or the Service) and the Government Communications Security Bureau (GCSB or the Bureau) (together, 'the agencies'). We continue to strive for as much openness as possible in the public reporting of those reviews. There is an obvious tension between necessary secrecy (to protect agency sources and methods and information that could, in the wrong hands, harm New Zealanders) versus transparency (and consequential public scrutiny and assurance). The balance is not always easy to strike. However, in my view the balance is currently skewed to over-classification of information and under-reporting of intelligence activities. I remain supportive of both agencies (and the broader intelligence community) embracing transparency and reform of our security classification system.

One area of review that has raised interesting issues in different contexts is the intersection between law enforcement and the role of the intelligence agencies. The agencies have no enforcement function, but can report intelligence to the Police and in limited circumstances disclose information about crime that they discover incidentally while collecting intelligence. We have made recommendations to the NZSIS on how it assesses which is the right course of action. We have also said the law is clear that information about criminal offending obtained for the purpose of security vetting cannot be shared for law enforcement purposes. That restriction exists to encourage full disclosure by security clearance candidates, but can create obvious tensions for the Service, which conducts vetting. The issue will inevitably arise during the forthcoming review of the Intelligence and Security Act. I intend to publish more fully on these issues in the coming year.

This year has seen, I think, an increased awareness of the value of independent oversight within the intelligence sector and among those engaged with it. We now regularly present at the induction of new intelligence community staff and engage with academics, including speaking to their post graduate courses. We have been able to provide useful comment on the revision of the Ministerial Policy Statements that guide agency activities and on the form of the proposed new role of Inspector-General of Defence. The extent to which our feedback has been sought and considered reflects the objective and practical contribution we can offer.

There is significant change and reform occurring in the intelligence and security area. That work commenced over the past year and will mostly manifest in the year ahead. I look forward to making our knowledge and experience available and continuing our contribution to public understanding of the intelligence agencies and their activities.

Brendan Horsley
Inspector-General of Intelligence and Security

## THE YEAR AHEAD

The coming year will see the first independent review of the Intelligence and Security Act 2017 (ISA) since it was enacted. The ISA resulted from a wholesale overhaul of the legislation governing New Zealand's intelligence and security agencies. The reform replaced multiple statutes with a single comprehensive Act. The forthcoming review, originally required by the Act itself to begin in 2022, was brought forward in response to recommendations from the Royal Commission of Inquiry into the Terrorist Attack on Christchurch Masjidain. My office now has four years' experience of the Act in operation, gaining valuable knowledge about how it works and where it might work better. We anticipate contributing to the review, particularly regarding provision for effective and appropriate oversight.

We will continue to engage with other legislative reviews and administrative reforms where our knowledge and functions are relevant. This will likely include submitting on the Security Information in Proceedings Bill, which addresses how classified material is dealt with in court. We also anticipate contributing information and advice, as needed, to the Ministry of Defence-led process for establishing new oversight of military operations, in response to the findings and recommendations of the inquiry into Operation Burnham.

Sadly, at the time of writing this annual report New Zealanders had recently suffered another attack motivated by violent extremism. On 3 September 2021 seven people in an Auckland supermarket were stabbed by a person who was under close state surveillance because of his known extreme beliefs. My office will be contributing to a coordinated review, with the Independent Police Conduct Authority and the Department of Corrections Office of the Inspectorate, of how relevant agencies responded to the threat the attacker presented.

My office's work programme for 2021-22 was published in June 2021. It includes completion of an inquiry and two reviews that were under way in the past year, along with a number of new reviews. Several of these are "baseline" reviews, examining areas of agency activity that are relatively new or which have not previously been scrutinised by my office. These reviews build our knowledge of agency operations and help us identify any areas of activity that require further examination. In the coming year I also anticipate publishing unclassified reports of some reviews completed in 2020-21. As in the past, our policy is to report publicly on our work, to the extent possible while protecting sensitive information that cannot be disclosed without harm to the national interest and the ability of the intelligence and security agencies to function effectively.

## SIGNIFICANT ISSUES IN 2020-21

Every year issues arise that are not anticipated in our work programme. They 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 2020-21.

### Legal basis for GCSB requests for partner-collected data

Under the Five Eyes intelligence partnership the GCSB can request signals intelligence data collected by counterpart agencies in the United States, the United Kingdom, Canada and Australia. Since 2013 it has done this under warrants. Before 2013 such requests were made under statutory authority.

In 2020-21 the Bureau reached the view that the ISA did not in fact require it to continue seeking warrants for this purpose. Crown Law agrees. I differ from the Bureau on some relevant points of statutory interpretation but accept a warrant is not legally required.

In short, data collected by a partner agency can be presumed to have been collected lawfully by that agency, in accordance with the law of its country. If the Bureau requests a search of that data, it does so by agreement with the partner agency, which is lawful. A search request in the interests of national security 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. Provided the Bureau's search requests follow procedures ensuring they are carefully justified, therefore, I accept they will be lawful without authorisation. Warrants are not required for lawful activity.

Importantly, the Bureau proposes, as a matter of policy, to continue to seek warrants for requests to search partner-collected data relating to New Zealanders. That will ensure the basis for seeking the information is set out to the satisfaction of the responsible Minister and a Commissioner of Intelligence Warrants, and is open to subsequent review by my office.

At the end of 2020-21 the GCSB was yet to finalise policy and procedure to guide requests for searches of partner-collected data without a warrant, so was still conducting all such activity under warrants. The transition to warrantless activity will occur in the coming year. My keen interest is in whether the Bureau's new policy and procedure will ensure its use of its ability to benefit from Five Eyes partner capabilities will remain sufficiently open to oversight and ministerial supervision. To obtain warrants the Bureau must set out regularly, in some detail, how it intends to make use of its ability to request searches of partner data. If that process is to cease, there must in my view be substituted a process that ensures this important area of Bureau activity is conducted within plain sight of the Government and my office.

## NZSIS disclosure and use of vetting information

The conduct of security clearance assessments, or "vetting", is a core function of the NZSIS. Candidates for national security clearances are required to supply considerable information on their personal history and circumstances so the Service can assess whether they might present a security risk if given access to classified material. The sensitivity of the personal information candidates provide means it must be held securely, with tight controls on who can access it.

Section 220 of the ISA specifies that information obtained by or disclosed to the Service for a security clearance assessment may be used only for the purposes of that assessment, another clearance assessment, or counter-intelligence. Counter-intelligence is defined as intelligence activities carried out to identify and counteract the threat, or potential threat, of unauthorised disclosure of official information by a person who holds or has held a security clearance.

During a security clearance assessment a candidate might disclose, or the Service might otherwise discover, information about criminal behaviour – perhaps by the candidate, but also possibly by someone close to them. Disclosure of such information – eg drug use, or past criminal convictions – is sought from the candidate for its relevance to security risk. Candidates are encouraged to make such disclosures on the basis that the information will be used only for vetting purposes (or counter-intelligence).

In the past year the Service was confronted with the question of whether a candidate's disclosure of information about criminal behaviour was serious enough to be reported to the Police, despite the rule in the ISA. In a particular case the Service decided quickly in favour of sharing the information. On learning of this I was not persuaded, on the facts, that it had been necessary for the Service to report it before receiving advice from Crown Law on the scope for doing so. The Service subsequently proposed an interpretation of s 220 ISA that would allow disclosure to the Police, in the particular circumstances and more generally. I did not agree with that reading; nor, ultimately, did the Solicitor-General.

I expect s 220 to come under scrutiny in the forthcoming review of the ISA. Any proposal to relax it raises a difficult policy question: if the scope for disclosure to the Police is increased, in the interests of law enforcement, will that undermine security vetting by deterring candidates from being fully frank and open?

## Third party assistance to execute warrants

Under s 51 of the ISA the agencies can ask third parties (individuals or organisations) to assist with the execution of an intelligence warrant. The assisting party receives the same powers and immunities as the agency and becomes subject, while assisting, to the control of the agency Director-General. Section 51 requests form part of the legal basis for agency activities including communications interception, surveillance and collaboration with other government agencies for intelligence and security operations.

In 2019-20 we identified issues with the circumstances in which GCSB requests for assistance under s 51 had been made and the extent to which control had been exercised. We reviewed these arrangements and reached an understanding with the Bureau on what meaningful "control" of the assisting party entailed. Significant improvements were made to the way Bureau requests for assistance are made and supervised. The Bureau also initiated an audit of s 51 requests.

The Bureau audit was completed in 2020-21 and found issues with internal practices and controls. The agency implemented new policy on documentation of s 51 requests and management of third parties assisting under s 51. It improved record-keeping by establishing a register of s 51 requests. The GCSB also developed automated notification for relevant staff when a s 51 request is due to expire. I think these measures have the potential to reduce compliance incidents involving missing or lapsed s 51 requests, which can result in third parties inadvertently acting in support of the Bureau without proper legal authority. We will see if that occurs.

### 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, and one for access to New Zealand Customs' primary operational database (CusMod).[1] By law a DAA must be reviewed every three years, including consultation with me and the Privacy Commissioner. The Service notified my office in January 2020 that it was beginning reviews of the APP and CusMod agreements, both signed in March 2017. In my last annual report I noted the issues we raised with the existing agreements when consulted. The review concluded in March 2020 that both DAAs should be amended. We were supplied with revised draft agreements in December 2020 and provided comment, jointly with the Privacy Commissioner, in early 2021. At the end of 2020-21 the revised drafts were yet to be finalised. In all, by year end the review and variation of these agreements had been under way for a year and a half. I think it is clear that is not a timely process for updating the terms and conditions of the Service's access to substantial repositories of data, including personal information, about New Zealanders and others. The timetable is not wholly under the Service's control, however, and there is no statutory timeframe for completion of a review. This may be a matter for the forthcoming review of the ISA.

### Information sharing with foreign partners and human rights abuses

I reported last year on our engagement with the agencies concerning 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. Briefly, we questioned whether the agencies' joint policy was sufficiently protective of rights. Review of that policy was waiting on a review of the Ministerial Policy Statement (MPS) on Cooperation with Overseas Public Authorities, led by the Department of the Prime Minister and Cabinet.[2]

1 DAAs are publicly available via the NZSIS website.

2 Ministerial Policy Statements are issued by the Minister responsible for the agency or agencies, under ss 206-216 ISA. They guide the agencies and may specify matters to be included in agency policies.

In the past year my office provided detailed comment to DPMC on revision of the MPS, which was finalised in April 2021 and published on the NZIC website. The new MPS provides essential guidance for the intelligence and security agencies with, for example, a robust "risk assessment framework" for the agencies to employ when sharing information overseas, and a strictly limited set of circumstances in which any use of information likely obtained by torture would be considered reasonable and proper.

We have also engaged with the agencies on their revision of their joint policy statement on human rights risks in overseas cooperation. This was ongoing at year end, with five key areas in which we remained at some distance from their position. These concerned the terms employed in risk thresholds; specific criteria and definitions for overseas bodies; the handling of reports likely obtained by torture; and our suggestion that for transparency the joint policy could be made public.

### Ministerial authorisations for intelligence sharing

Under section 10 of the ISA the NZSIS and the GCSB may share intelligence with parties outside New Zealand, if the Minister responsible for the agencies has authorised them to do so. The ISA requires the Minister to be satisfied that in providing the intelligence the New Zealand agency will be acting in accordance with New Zealand law and all human rights obligations recognised by New Zealand law. To date, Ministerial authorisations have mostly been issued for sharing with governments of specified countries, rather than particular foreign agencies.

This year the question arose as to whether the NZSIS or the GCSB can agree to an agency in an authorised foreign country on-sharing New Zealand intelligence to an agency in a country not approved by the Minister. The NZSIS and the GCSB require a Five Eyes partner holding intelligence from the Service or Bureau to get the consent of the relevant New Zealand agency before on-sharing it to a non-Five Eyes agency (the 'third party'). They consider, however, that the third party need not be Ministerially approved. In their view the law only requires Ministerial approval of a third party they directly share intelligence with.

I disagree. The purpose of Ministerial authorisation is to ensure the Minister can assess any legal, human rights, political and reputational risks arising if the Service or Bureau knowingly shares intelligence with a foreign country or agency, before it happens. In my view, therefore, there should be a Ministerial authorisation for any 'third party' recipient of New Zealand intelligence, given that under current practice the relevant New Zealand agency will know the identity of the proposed recipient and have control over whether the intelligence can be shared. I informed the Minister responsible for the NZSIS and the GCSB of my view, given the Minister's role in the process.

To the extent that it concerns interpretation of section 10 of the ISA, which does not explicitly address the question, this may be another matter for the forthcoming review of the ISA.

### Agency data management

Past IGIS annual reports have noted that the agencies' data and information management systems and processes face significant long-term challenges. This remains true.

The Bureau continues working towards an ability to label and categorise its data holdings so it can apply records management rules comprehensively and consistently. It still does not have a data retention and disposal policy that can be applied effectively across its operations, although it made

further progress towards this in 2020-21 and briefed my office on it. The Bureau's current policy has been identified by the Bureau's own auditing as difficult to implement and probably not fit for purpose. Efforts to comply with it result in the production of data retention assessments that appear to have little if any value. This is clearly unsatisfactory for an organisation whose core business is the acquisition, storage and analysis of data. The Bureau is well aware of this and I do not doubt its commitment to developing more relevant and effective policy. The law does not particularly assist: the ISA requirement to destroy "irrelevant" information as soon as practicable is problematic for an intelligence agency, as data can be valued for its possible relevance in the future. The requirement might well come under scrutiny in the forthcoming review of the Act. In any case I hope to see further progress in Bureau policy in the coming year.

The Service faced new data management challenges in 2020-21 as a result of a heightened commitment to "target discovery" – the identification of new investigative leads and intelligence gathering opportunities. Its approach includes more use of data analysis, based on the acquisition of more data. Initial efforts in the year under review rapidly expanded the Service's total data holding to a multiple of its previous total. The Service recognised that it would need to transform its data systems and processes to manage such volumes effectively. This transformation is in its early stages. It begins moving the Service further toward the kind of data analysis capabilities that have largely been the preserve of signals intelligence agencies like the GCSB. Such a shift is of obvious interest for oversight and we will continue to monitor developments.

## 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, eg the power to compel a witness to answer questions or produce documents.

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 seeking 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 this reporting year I initiated an inquiry into the history and current state 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 will be completed during the 2021-22 year.

### Review of NZSIS' handling of privileged communications and information

In December 2018 the previous Inspector-General reported publicly on a review of the Service's handling of privileged communications and privileged information. In the past 12 months NZSIS warrant applications have addressed more fully the potential for unintentional collection of privileged communications and information, where relevant, and how privileged material will be triaged and destroyed where necessary. During 2020-21 the agencies also revised a Joint Policy Statement that addresses privilege and the Service has issued a Standard Operating Procedure providing more detailed guidance for its staff on understanding, identifying and handling privileged material. These are positive developments, which address some elements of the IGIS' recommendations in 2018. Those recommendations included informing my office of any instances of the Service incidentally obtaining and then disclosing New Zealanders' privileged material, in the very limited circumstances where such disclosure is lawful. The Service agreed to do so. It reported none in the past year.

I anticipate engaging further with both agencies, but particularly the Service, on other aspects of policy and procedure addressed by the 2018 recommendations. These concern, for example, the common law protections of legal professional privilege; the application of privilege protections across all Service functions including with regard to communications and information received unsolicited; the practical breadth of religious privilege; and the approach to confidential communications made to journalists.

### Review of NZSIS and GCSB engagement with international partners

This year we undertook our second review of the way the agencies engage with their international counterparts. Our first, last year, surveyed a range of documented arrangements with partner agencies and assessed compliance with ministerial policy requirements designed to enable oversight

of such arrangements. This year we focused on agreements and procedures designed to safeguard the interests of New Zealand and New Zealanders when our agencies collaborate with those of other nations. We also surveyed how the agencies had responded to our first review. We provided a draft classified report to the agencies for comment at the end of the year and will finalise it early in 2021-22.

### Reviews of NZSIS and GCSB open source intelligence collection and online operations

By year end we completed classified reports on reviews of NZSIS and GCSB open source intelligence collection and selected online operations involving open source information. Broadly, information is "open source" if it is publicly available – although what counts as publicly available is not necessarily straightforward. A Ministerial Policy Statement specifies that it includes, for example, information on social media platforms that is open to public view, but not information on such platforms that is shared within closed groups or only with approved individuals.

Our review found that the NZSIS takes care to identify and manage key areas of compliance risk arising from its open source operations, but recommended some further development of its internal guidance material. This included guidance on when a reasonable expectation of privacy might arise in open source information; the privacy impact of persistent searching or the collection of large amounts of information; the assessment of collected information for relevance; and the implications of political neutrality for analysis and reporting of some open source data. Similarly the GCSB also generally manages legal and compliance risk from its open source operations appropriately, but could improve policy and procedure. In particular we recommended it develop guidance for a specific type of online intelligence collection not currently covered.

### Review of GCSB access to information infrastructures

We completed a review of GCSB's conduct of certain operations to access information infrastructures. The operations examined are classified to an extent that effectively precludes public reporting, but the review documented in detail the Bureau's compliance systems for controlling them and found they were generally effective and appropriate. We recommended some minor amendments to Bureau policy, a commitment to regular internal audits of aspects of the operations concerned, and direct access for my office to certain operational documents useful for oversight. The Bureau accepted and implemented the recommendations.

### Review of NZSIS access to CCTV

In June 2021 I reported publicly on a review of the Service's use of closed circuit television (CCTV). This was described in our 2020-21 work programme as a review of the Service's access to "a particular network system", as the fact of the NZSIS' access to a CCTV system was then classified. The Service subsequently declassified its access, enabling me to report publicly. Overall I was satisfied that the Service's use of its access to CCTV was lawful and carried out in a responsible and proper way. We recommended improvements to policy guidance on necessity, proportionality and privacy, the circumstances in which a warrant is required and the use, storage and destruction of information obtained. We also recommended better record-keeping of CCTV use, to assist with oversight. The Service accepted all recommendations in principle, for action in the coming year.

## Review of NZSIS and GCSB work under the Outer Space and High-altitude Activities Act 2017

The agencies conduct national security risk assessments of all licence and permit applications under the Outer Space and High-altitude Activities Act 2017 (OSHAA). Most of these assessments concern applications to launch payloads into space. They form part of a wider process of official advice for ministerial decisions on applications. Ultimately, if a significant national security risk is identified, the Prime Minister can issue a security certificate preventing a licence or permit being granted.

We reviewed the agencies' activity under OSHAA and I reported publicly on this review in April 2021. Overall we found their policies and procedures for activities under OSHAA are generally well-developed. I recommended some amendments to clarify how national security risk is to be assessed, and that the agencies publish more information about their role under OSHAA for the public. The agencies accepted my recommendations.

## Review of NZSIS visa screening

One of the Service's statutory functions is to provide advice about national security risks, including those associated with citizenship applications and border security. In accordance with this, it routinely assists Immigration New Zealand (INZ) with the screening of visa applications from people wanting to travel, work, study or reside in New Zealand. In 2020-21 we substantially completed a review of this activity, finalising a classified report shortly after year end. Our review found shortcomings in the Service's policies and procedures for screening and commenting on immigration visa applications, but also that the Service was well aware of them from an internal review and had made plans for remedial action. I made a number of recommendations intended to highlight matters that can be addressed within the Service's proposed programme of change, particularly in regard to revision of policy and procedure. I intend to report publicly on this review in the coming year and monitor the Service's progress with its planned improvements.

## 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. Under the ISA (s 104) it has discretion on whether to disclose such information to the Police. We reviewed how the Service makes decisions on disclosure, examining relevant policy and some examples from a counter-terrorism investigation. Our review highlighted the difficulty of these decisions, which involve balancing the national security interest in pursuing intelligence operations with the public interest in seeing crimes prevented or investigated: potentially, law enforcement action can disrupt intelligence collection. In the specific examples reviewed we found the Service generally approached these decisions in a considered manner and exercised its discretion appropriately, although some aspects of its decision-making would have benefited from further analysis and improved policy guidance. I anticipate producing an unclassified report on this review in the coming year.

## Reviews in progress

### *NZSIS and GCSB support for 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 agency activities relating to Afghanistan. It brings aspects of those inquiries up to the present, including considering whether IGIS recommendations relevant to support to military operations have been implemented. Research was largely complete at the end of 2020-21 and we will complete the review in the coming year.

### *NZSIS and GCSB role in first Control Order*

The first Interim Control Order under the Terrorism Suppression (Control Orders) Act 2019 was issued in May 2021. It is over 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 agenda to others. This baseline review examines what if any intelligence or information the agencies contributed to the Control Order application, which was made by the Commissioner of Police.

### *GCSB access to partner agency data*

We began in 2020-21 a review of the GCSB's access to data collected by its Five Eyes partner agencies. It examines the Bureau's systems and practices for ensuring that its access to partner data meets compliance requirements and is properly justified. A classified report will be finalised in 2021-22.

### *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, begun in 2019 but paused and resumed in early 2021, 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.

### *NZSIS information sharing with the Police*

This baseline review is examining how the Service works with the New Zealand Police on counter-terrorism investigations. We expect to complete it in the coming year.

# 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 necessarily be reported, to the complainant or publicly.

Each year my office receives a significant number of contacts from people expressing concern, without evidential foundation, 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.

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 2020-21 | | | |
|---|---|---|---|
| **From** | **Against GCSB** | **Against NZSIS** | **TOTAL** |
| Members of the public | 6 | 12 | 18 |
| Intelligence agency employees or former employees | 0 | 1 | 1 |
| Complaints and queries not within IGIS jurisdiction | - | - | 30 |
| **Total** | **6** | **13** | **49** |

## Significant complaint inquiries

In the reporting year three complaints were noteworthy for the issues raised and depth of inquiry required.

### *A vetting process*

One complaint against the Service concerned an adverse vetting assessment resulting from a particularly lengthy process. The candidate applied for a security clearance early in 2018 and learned of the outcome 21 months later. The assessment was complex, considering a number of security

concerns, and was intense and stressful for the candidate, including repeated interviews. The complaint raised questions of procedural fairness, including the extent to which the Service took all reasonable steps to obtain relevant and reliable information; disclosed adverse information to the candidate and gave an adequate opportunity to respond; and made an objective and reasoned assessment of information obtained. It was also the first complaint received by my office about a vetting process involving assessment of the candidate by Service psychologists, prompting consideration of the semi-independent function they perform in the agency.

I partially upheld the complaint, finding that all parties to the assessment had acted in good faith, but the duration and intensity of the process had contributed to a decline in the candidate's mental health. At times in the process the Service had failed to meet its own standards of procedural fairness and the requirements of natural justice. I made eleven recommendations for change to Service vetting policies and procedures, to improve future handling of similar cases and ensure clarity for candidates. This included development of policy on the role of the Service psychologists in the process. The Service accepted the majority of these recommendations, although the Director-General declined my recommendation to acknowledge my findings on procedural fairness directly to the candidate. The Service has since implemented most of my recommendations. At year end, the policy on Service psychologists was under development.

### *A search*

A New Zealander complained of being searched and questioned by a Government agency, including a demand for electronic devices and their passwords. The complainant, who had some knowledge of NZSIS operations, believed the actions were undertaken on behalf of the Service. The complainant considered the actions unjustified and an abuse of the statutory powers of the agency that carried them out. I terminated my inquiry into this complaint when it was nearly complete, at the complainant's request. By that point, however, it had identified some issues I considered necessary to raise with the Service.

The agency that searched and questioned the complainant is one that commonly assists with Service operations. I found a lack of clarity in the arrangements between the Service and the agency for such assistance. Neither the Service's documentation nor operational staff were clear on the extent to which the assisting agency would be exercising Service powers, under Service control, or exercising its own statutory powers. These details matter because the powers of the agency and the Service differ: the lawfulness of what is done depends on which powers apply. I recommended the Service expedite work on a Memorandum of Understanding with the agency concerned, to bring more certainty to their working arrangements and reduce legal risk.

### *An historic operation*

A complainant alleged that in an operation about 30 years ago the NZSIS found information indicating that a serious crime was being committed, but did not pass it to the Police, despite at least one NZSIS officer proposing that the Police should be informed. A subsequent prosecution and conviction of the alleged offender, years later, confirmed that serious offences had been committed.

I reported publicly on my inquiry into this complaint in late 2020. In summary, my inquiry confirmed an historic instance of the Service obtaining information about serious criminal offending that it did

not pass on to the Police. The Service had (and still has) discretion about whether to provide Police with information about crime found in the course of seeking other information for intelligence purposes. In the case at issue its exercise of that discretion appeared questionable, but the records were too scant to support a definite finding. Some possible reasons against disclosure to the Police were at least conceivable and the NZSIS did not perceive the full scale and nature of the crimes of which the offender was later convicted. I did not find the Service acted improperly.

My inquiry highlighted the difficulty of determining when the Service should disclose incidentally obtained information on crime to the Police. This prompted me to conduct a review of the Service's framework for such decisions (see the "Inquiries and Reviews" section of this report).

## WARRANTS

In this reporting year my office reviewed 77 warrants issued to the agencies. This was a small increase on the preceding year (73).

| | Type 1 warrants | Type 2 warrants | Practice warrants | Removal warrants | Total |
|---|---|---|---|---|---|
| **NZSIS** | 20 | 5 | 3 | 1 | 29 |
| **GCSB** | 20 | 27 | 1 | 0 | 48 |
| **Total** | 40 | 32 | 4 | 1 | 77 |

This year was the fourth in which the agencies have been operating under the ISA, which enacted new warranting provisions applicable to both. Significant questions of legal interpretation concerning the requirements for warrants have largely been dealt with. Our reviews of warrants now more frequently raise lesser questions of clarity and detail.

Both agencies revised their standard format for warrant applications this year to make them more concise. This has been a welcome and effective improvement.

Some warrants issued to the Service this year for seizure of particular types of datasets raised significant questions. I was concerned that the NZSIS had specific datasets in mind when it sought the warrants, but did not identify them in its applications. The duty of candour requires the agency to inform the decision-maker of all material facts and in my view required the Service in this instance to specify those datasets. I was concerned also that the warrants defined the targeted classes of datasets so broadly as to be almost general-purpose. I suggested they could better meet the statutory requirements if they specified the particular intelligence themes for which the Service expected the targeted datasets to be useful. The Service accepted that the warrants, which were novel, required improvement. It undertook to revise its approach in any further applications for authorisation to acquire datasets of the relevant types.

## 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.

In the last annual report we introduced a multi-factor template for this assessment, rating the compliance systems of each agency on five main headings. We continue that approach in this report. 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 we 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 2020-21

Our assessment of the compliance systems of both agencies for 2021-21 follows, applying the framework above. For each heading we give the rating for each agency, then summarise the information underlying our assessment.

### Operational policy and procedure

| GCSB | NZSIS |
|---|---|
| Well-developed | Well-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. Both agencies, however, have a significant number of policies and/or procedures overdue for review. The Service is addressing some of these in a rationalisation process continuing from 2019-20. The Bureau has a senior governance group overseeing policy development and rationalisation. Typically, when examining a particular area of operation in either agency, we find it has relevant policy with some improvement needed.

*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. Last year we noted neither had a system that dependably provided access to policies that are relevant and current, but both have since made improvements. The Bureau is updating its intranet policy pages to remove obsolete policies from circulation. This remains a work in progress. The Service completed a redesign of its intranet portal for policy and procedure and promoted it to staff as the authoritative source of guidance, although it is not yet a complete or fully accurate resource.

*Specialist policy staff?*

Both agencies increased their specialist policy staff: the Service to two, supported by a contractor, and the Bureau to three. Both, but particularly the Bureau, continue to rely also on subject matter experts in operational roles to contribute substantially to operational policy.

*A programme of policy review?*

The Service continued a policy simplification project begun last year, following a review of its operational policies in 2018-19. The Bureau's leadership group for operational policy governance met regularly and began developing a policy stocktake tool and terms of reference for a review of operational policy.

*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.

## Internal compliance programmes

| GCSB | NZSIS |
|---|---|
| Well-developed | Well-developed |

Last year we assessed GCSB internal compliance programmes as "under-developed", the only area (for either agency) assigned that rating. Key factors included serious under-staffing of compliance roles, significant under-delivery on the internal audit programme and limited written reporting on compliance issues to senior leadership. Change in each of those areas, as noted below, has improved the overall rating for the Bureau this year.

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

Last year we noted both agencies had the elements of a strategic approach to compliance, 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. Neither had a compliance strategy documented as such and endorsed by its senior leadership, but both proposed to develop one. In 2020-21 GCSB progressed but did not complete development of a formal compliance strategy and revised, but did not finalise, its compliance policies and procedures. 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 the Service recruited new policy staff, enabling compliance staff to work more on compliance tasks and less on policy. The GCSB remedied the serious under-staffing of compliance positions that occurred in 2019-20.

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

Last year the Service completed one of six planned audits/reviews. This year it had no formal audit plan but committed to seven, including four carried over. Those four and one more were completed. One was in train at year end and one postponed. Overall the Service's audit programme remains limited.

In addition to routine audits of searches of signals intelligence databases, the Bureau proposed 11 audits for the calendar year 2020. At the end of the year it had completed five of them, along with one from its 2019-20 audit plan. One more audit from the 2020 plan was completed in early 2021. To try to remedy a pattern of under-delivery on audit programmes in past years, the Bureau's 2021 audit plan proposes a more limited schedule of six audits, including three of those uncompleted in 2020. These are to be supplemented by "unscheduled" audits, to be completed as time and resources allow; a small number of spot audits; and follow-ups on previous audit recommendations. In the past year Bureau audit staff were given responsibility for compliance incident investigations, which seems likely to impinge on their capacity to implement the audit programme.

*Timely remediation of any shortcomings found by audits?*

Assessing the Service's responsiveness to internal audits remains difficult given the limited execution of audit plans in recent years. Some recent audit recommendations have been implemented, however, and the Compliance team has introduced a means of tracking progress on them.

This year the Bureau also began tracking action on audit recommendations, dating back to 2018-19. This work showed uncertainty about internal acceptance and action on some earlier audits but a reasonable level of action on more recent recommendations.

Both agencies increasingly 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. GCSB Compliance began to remedy this in the past year, including a model of statistical reporting on compliance incidents and activity in one report, but has yet to repeat this. NZSIS Compliance maintained its normal level of reporting to senior leadership, with limited statistical content. Both agencies share their internal compliance reporting with the IGIS routinely or on request.

*Proactive measures to maintain or improve compliance?*

The Service established a regular intranet blog post on compliance issues, with an associated message board for staff feedback. It also introduced a new intranet mechanism for self-reporting of compliance incidents.

The Bureau reorganised its compliance team to assign compliance incident investigations to audit staff, to enable compliance advisors more time for providing advice and training.

## 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 willing self-reporting.

*Established policies and procedures for responding to compliance issues?*

Service policy on handling compliance issues was due for review in mid-2020 and that remains under way. The policy is high-level, so assessment and investigation of compliance incidents continues to depend significantly on the skills and experience of compliance staff.

The Bureau's documentation of compliance policies and procedures remains significantly out of date: a review of it was progressed but not completed this year. Practices for responding to compliance issues are well established but reliant on the institutional knowledge and skills of relevant staff.

*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. Part way through 2020-21 the Service compliance team began aiming to resolve all compliance incidents within one month, but due to a backlog did not achieve this. Most incidents requiring investigation took between six 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 Service adopted an operational training strategy in 2019-20 and has a compliance training 'framework' comprising a set of mandatory courses on statutory and policy obligations for all staff. The Bureau has mandatory training in compliance with the ISA for all staff, which it updated in the past year. Staff whose work involves requests to Five Eyes partner agencies to search collected data, or undertake new collection, must complete regular training on compliance with both New Zealand and partner agency legal obligations.

*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 compliance investigations, and in response to IGIS recommendations. The Service developed training in 2020-21 for protective security roles, expanding on existing courses for investigators and case officers. The Bureau began revising its compliance and risk training.

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

Both agencies have specialist staff developing and delivering training. Training facilities are not extensive but much training does not require significant infrastructure. The Service introduced more online training this year. Much of the Bureau training is online.

### 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 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. Responses from the Service to questions and requests have been reasonably timely. In the later part of the year Bureau responses on a number of matters were delayed.

*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. Where issues arose in the past year (eg NZSIS disclosure and use of vetting information; GCSB requests for partner-collected data – see the 'significant issues' section of this report) the agencies' legal positions were readily available.

*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. I continue to encourage the agencies to allocate sufficient resources for oversight as part of 'business as usual'.

*Timely and effective implementation of accepted IGIS recommendations?*

Most recommendations for the Service and the Bureau from reviews and inquiries in recent years have been accepted, 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. This year my office contributed to working groups, set up in 2019, that completed papers on issues arising for oversight from international intelligence cooperation and human rights abuses; intelligence applications of artificial intelligence and machine learning; and whether there are gaps in oversight as a result of the international reach of the intelligence agencies compared with the domestic scope of the oversight function. New Zealand was to host the annual FIORC conference during the past year, but the coronavirus pandemic intervened: instead we are to host a virtual conference in late 2021.

## Advisory Panel

The ISA establishes a panel of two people to advise the Inspector-General. This year Angela Foulkes departed from the panel after serving almost seven years. Her counsel has been greatly appreciated. The remaining member, Lyn Provost, now chairs the panel and a further appointment is pending.

Ms Foulkes' departure highlighted the issue with such a small panel: a vacancy, or mere absence, leaves a panel of one. The panel and I agree a third member would be valuable. This would require an amendment to the ISA.

## Other integrity agencies

Among the other integrity agencies, we work most frequently with the office of the Privacy Commissioner. This year we collaborated on matters including comment on revised Direct Access Agreements for the Service and privacy questions arising in relation to the Service's use of CCTV (see the 'significant issues' section of this report regarding both matters). We 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 11 speaking opportunities during the year, to academic, public service and intelligence sector audiences.

# FINANCE 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 2020-2021 was 17 percent under budget:

| Office of the Inspector-General of Intelligence and Security 2020-21 Budget | | |
|---|---|---|
| | Actual ($000s) | *Budget* |
| Staff salaries/advisory panel fees; travel | 826 | 891 |
| Premises rental and associated services | 407 | 527 |
| Other expenses | 2 | 44 |
| Non-Departmental Output Expenses (PLA) | 503 | 644 |
| **Total** | **1740** | **2,107** |

For most of 2020-21 the office had a total staff of eight: the Inspector-General, Deputy Inspector-General (or, in the latter half of the year, an investigator acting in that role), an office manager, an IT and security manager, and four investigators.

## Premises and systems

Since October 2019 we have operated from secure premises in Defence House, Wellington. Our staff is near the maximum number 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.

**Office of the Inspector-General of Intelligence and Security**
P O Box 5609
Wellington 6140
04 460 0030
enquiries@igis.govt.nz
www.igis.govt.nz

Follow us on Twitter @igisnz