Office of the Inspector-General of Intelligence and Security

Annual Report

For the year 1 July 2019 to 30 June 2020

Brendan Horsley
Inspector-General of Intelligence and Security
26 January 2021

CONTENTS

Foreword 2
The year ahead 3
Significant issues in 2019-20 5
Inquiries 9
Reviews 14
Agency implementation of recent IGIS recommendations 18
Complaints 21
Warrants 23
Certification of compliance systems 25
Outreach and engagement 33
Office finances and administration 35

OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

26 January 2021

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

Dear Prime Minister

Inspector-General's Annual Report 2019-2020

Please find **enclosed** my annual report for the period 1 July 2019 – 30 June 2020.

You are required, as soon as practicable, to present a copy of the Inspector-General's report to the House of Representatives (s 222(3) Intelligence and Security Act 2017 – "the Act"), together with a statement as to whether any matter has been excluded from that copy of the report. In my view, there is no need for any material to be excluded. The New Zealand Security Intelligence Service and the Government Communications Security Bureau have confirmed that publication of those parts of the report which 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)).

As soon as practicable after the report is presented to the House the Inspector-General is required to make a copy publicly available on the Inspector-General's website.

With your concurrence, and in accordance with s 222(8), I confirm my availability to discuss the contents of this report with the Intelligence and Security Committee when it next meets.

Yours sincerely

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

FOREWORD

I am pleased to present my first annual report as Inspector-General of Intelligence and Security (IGIS). Having only commenced in the role in June 2020, I can claim little credit for the excellent work the Office undertook and completed over the 2019-20 year. That credit must go to Madeleine Laracy, who was Acting IGIS over the period, and the (small) team of dedicated and professional staff who delivered so much over a disrupted and busy year.

In an important development for our Office, we have recently adopted a Te Reo Māori name that reflects who we are and what we stand for. Our chosen Te Reo Māori name is Te Pourewa Mātaki – the watchtower within the Pā. This acknowledges that we are within the somewhat exclusive intelligence community but we stand independently, we look over it and we look outward for the benefit of all.

The intelligence and security agencies necessarily operate in a world that is not readily visible to the general public. They have a mandate to exercise intrusive and far-reaching powers for the benefit of New Zealand. However that mandate or social licence to act will only exist as long as the public can be assured that the agencies are acting lawfully and with propriety. I see my role as one of shedding light on the agencies' activities; publishing my findings to the fullest extent possible; reporting the good with the bad; and providing the public with independent assurance the agencies are conducting themselves in a manner consistent with their lawful mandate.

The coming year will be an interesting one for both oversight and the agencies. Two separate and important external Inquiries have made recommendations concerning the collation and use of intelligence - including possible structural and legislative changes. The Inquiries have also commented on the importance and need for oversight. They have (as we have consistently done) adversely commented on the over-classification of information – as a barrier to public understanding and scrutiny. Consistent with those themes we will continue the drive for transparency and to better inform the public. I am also pleased that the Directors-General of both intelligence agencies have acknowledged the benefits to their agencies as well as the public in having robust independent oversight.

Finally, I am grateful for the support of my colleagues in introducing me to the intricacies of oversight of intelligence – it is a unique and challenging environment. I am also grateful for the comprehensive induction that the agencies have provided me with. To date I have been impressed with the professionalism, expertise and openness of all staff I have dealt with.

Brendan Horsley
Inspector-General of Intelligence and Security

THE YEAR AHEAD

The Government Communications Security Bureau ("GCSB") and the New Zealand Security Intelligence Service ("NZSIS") have come under additional scrutiny over the last two years as a result of Inquiries being conducted by the *Royal Commission of Inquiry into the Terrorist Attack on Christchurch masjidain on 15 March 2019* ("the *Royal Commission on Christchurch"*), and the *Government Inquiry into Operation Burnham* and related matters ("*Operation Burnham Inquiry"*). The fact of their involvement in these important external public Inquiries underscores their status as core Public Service departments, expected to contribute effectively and in an integrated way to a wide range of government objectives. The Office of the Inspector-General ("OIGIS") had a close working relationship with the *Operation Burnham Inquiry* given our own related, but separate, *Afghanistan Inquiry*. We have also, at our request, met with and provided information and opinions on certain matters to the *Royal Commission*. In the year ahead my Office will be well placed to provide an independent perspective on any recommendations from these Inquiries relating to the intelligence agencies.

The next 12 months will be a significant time for policy development. Under the Intelligence and Security Act 2017 ("the Act" or "ISA") the Ministerial Policy Statements ("MPSs") are due for review, it being three years since they were first issued.[1] There are currently 11 MPSs in place to guide the way NZSIS and GCSB undertake lawful operational activities. The Inspector-General has a key role in consultation on new MPSs or amendments to existing ones.[2] So far we have provided feedback to the Department of Prime Minister and Cabinet ("DPMC") in relation to its review of three MPSs: *Conducting Surveillance in a Public Place*; *Exemptions for NZSIS from the Land Transport (Road User) Rule 2004*; and, perhaps the most complex, the MPS on *Cooperation of New Zealand intelligence and security agencies (GCSB and NZSIS) with overseas public authorities* (*Foreign Cooperation* MPS). The *Foreign Cooperation* MPS provides important guidance for the agencies on how to ensure their information sharing with foreign partners is legally sound and consistent with the Minister's expectations. Information sharing activity is the bedrock of the Five Eyes arrangements, and lies at the heart of all international intelligence cooperation. If the expectations on New Zealand government agencies are not sufficiently clear, risks can arise. We have put considerable time into feedback on amendments to the *Foreign Cooperation* MPS, particularly given its relevance to findings and recommendations in our two most recent Inquiries.[3]

In addition to contributing to the review of the 11 MPSs, we are undertaking work now in anticipation of the independent review of the ISA which must commence five years after its enactment (September 2022).[4] This review will be a critical opportunity to take what we and the agencies have learnt from working under the ISA and use it to seek improvements to both the oversight and operational

1 ISA s 214(2).
2 ISA ss 211 and 212.
3 Inspector-General of Intelligence and Security *Inquiry into possible New Zealand intelligence and security agencies' engagement with the CIA detention and interrogation programme 2001-2009* (31 July 2019) (IGIS "*Senate Report*"); Inspector-General of Intelligence and Security *Inquiry into the role of the GCSB and the NZSIS in relation to certain specific events in Afghanistan* (June 2020) (*"Afghanistan Inquiry"*).
4 ISA s 235.

frameworks. I also anticipate that we will contribute in the next year to the reform of the Protected Disclosures Act 2000. The role of the Inspector-General is clear as the only "appropriate authority" for whistleblowers across the public sector, where they wish to make a protected disclosure in relation to classified information or information concerning the activities of the NZSIS or the GCSB. However, it is less clear what powers are available in the current statutory regime or in the Protected Disclosures (Protection of Whistleblowers) Bill ("Bill") for the IGIS to investigate or act on protected disclosures made by people. That position is highly undesirable. It is at odds with the policy aim of enhancing the protected disclosures regime and fostering an effective "speak up" culture across the public service. We intend to make a submission on the Bill. To that end we have recently published a more user friendly guide about our own role and processes to assist employees across the public sector who may have a disclosure to make to the Inspector-General www.igis.govt.nz/publications/protected-disclosures/.

In terms of our own substantive work, the Office's Work Programme for 2020-21 www.igis.govt.nz/assets/Uploads/Work-Programme-2020-21.pdf includes a number of operational reviews for completion, as well as five "baseline" reviews. I am confident that the baseline approach will prove to be an effective way of identifying whether there are areas of operational activity that require a more in-depth and resource intensive review, or whether a light-handed, even cursory, review in some cases will provide adequate information and assurance. The baseline reviews will facilitate our ability, given the small size of the Office, to look at a greater breadth of operational activity on the part of the agencies.

SIGNIFICANT ISSUES IN 2019-20

Many issues arise over the course of a year that are generally not anticipated in any specific item on the Inspector-General's work programme. They arise in meetings and discussions with the agencies, from their reports to us of compliance incidents, from our review of their policies or warrants, and through our own independent access to the agencies' intranet and document management systems. Debating and discussing issues as they arise often leads to improvements in agency operational practices and documentation. Reporting the issues increases the public's understanding of how the law applies to NZSIS and GCSB or is interpreted. Some of the issues we have spent considerable time discussing with the agencies this year are set out below.

Targeting New Zealanders

Under the ISA, NZSIS and GCSB can lawfully target New Zealanders under a Type 1 intelligence warrant. As a domestic security agency the Service has always been able to act against New Zealanders. The Bureau was, until the ISA was enacted, generally prohibited from targeting New Zealanders.[5] As well as removing that prohibition, the innovation in the ISA was applying a single warranting regime to both agencies.

In practice, the Type 1/Type 2 warrant distinction continues to raise issues:

- In our last Annual Report www.igis.govt.nz/assets/Annual-Reports/Annual-Report-2019.pdf we reported on the different interpretations taken by the agencies and our Office about the circumstances in which a Type 1 warrant is required under s 53 ISA. The Solicitor-General has provided advice that confirms the agencies' position. In implementing this advice, there have been occasions where, for almost identical target classes, one agency has sought and obtained a Type 1 warrant, and the other a Type 2 warrant. We have been unable to say that either approach is wrong, given the scope for subjective assessment that the law apparently allows. From our perspective this presents a troubling degree of uncertainty. We intend to raise this in the upcoming review of the ISA as a policy issue that needs consideration.

- When collecting against non-New Zealand targets, both agencies have increasingly used accompanying Type 1 warrants to cover any collection that may occur against a New Zealand person. Where collection activities are "covered" in this way, by paired Type 1 and Type 2 warrants, we are increasingly unsure of the value of the distinction between the two types of warrants.

- Both agencies have given us reason this year to consider the threshold in the ISA for obtaining warrants against New Zealanders. Both, but particularly the Service in the wake of the Christchurch terrorist attacks, have increased what they call "discovery" activity: the search for leads on possible activity of intelligence interest. Whatever method an agency chooses to conduct "discovery" involving unlawful activity against New Zealanders, it will require a

[5] There was always an exception for New Zealanders acting on behalf of foreign powers.

warrant. The legal question that arises is what degree of cause, or suspicion, or possible intelligence value, is sufficient to obtain a warrant against a New Zealander or a class of New Zealanders? The ISA requires that a Type 1 warrant, if sought for a national security purpose, is "necessary to contribute to the protection of national security" and "identifies, enables the assessment of, or protects against" at least one of a range of specified harms, such as terrorism or espionage. The proposed activity must also be necessary to a relevant function and proportionate to the warrant's purpose. In practice, the terms of the Act do not require that the target of a warrant is themselves a threat to national security, or closely associated with a threat, or even that they are a highly likely source of information about a relevant threat. There is no requirement for any standard of proof, such as "reasonable suspicion" that the person targeted is involved in, or otherwise associated with, any harmful conduct or threat. The threshold in the Act can be satisfied on less than reasonable suspicion, eg where targeting a New Zealander might possibly provide information about a relevant harm. We do not suggest that the agencies have sought, or been granted, warrants that are indiscriminate or sweeping in their scope or intent to collect information on New Zealanders, in search of targets. But we do flag "discovery" activity, and warrants for that purpose, as a matter that has required particular scrutiny this year and will continue to require close oversight.

Third party assistance to execute warrants

Under s 51 of the ISA the agencies are able to request the assistance of third parties (both individuals and organisations) to assist with the carrying out of a warrant. The assistant receives the same powers and immunities as the requesting agency and, in exchange, becomes subject to the control of the relevant Director-General. In the past year, we have identified issues with the circumstances in which requests for assistance under s 51, particularly by the Bureau, have been made and the way in which control has been exercised. Following our review of these arrangements the Bureau and our Office have reached a shared view, in principle, of what meaningful "control" by the Director-General requires, and significant improvements have been made to the way requests for assistance are made and supervised. The GCSB has also initiated its own audit into this area of activity. We await the outcome of this process.

Agency data and information management

The agencies acquire, process and analyse large volumes of data. The sources and types of relevant data are proliferating rapidly, as are the means of extracting information from them. As the agencies respond by expanding their collection and analysis capabilities, they must at the same time limit their information holdings to what is relevant to the performance of their functions. The limits of relevance are indeterminate, but clearly require discrimination as to what is kept.

Assurance that the agencies retain only what is necessary for them to perform their functions, and dispose of what is not, depends on a combination of policies, procedures and technology. This is still a work in progress in both agencies.

The Bureau, whose data collection systems, data holdings and computational analytic capabilities are extensive and sophisticated, is focused largely on technical improvement; it does not yet have the ability to label and categorise its data holdings to the extent necessary to apply records management rules comprehensively and consistently. The Bureau does not yet have a data retention and disposal

policy that can be applied effectively across its operations, although it has made progress towards this. Once the policy is settled, full compliance will still require further capability to automate data management. This remains a multi-year project.

The Service's data systems and holdings are comparatively much simpler, making data categorisation and rule application more straightforward. Its strategic focus, however, is on expanding and diversifying its data collection and analytical capabilities. The oversight interest is in ensuring that the development of effective policy and compliance systems keep up with this expansion. This task is at an early stage.

Information sharing with foreign partners and human rights abuses

We encountered two main issues on this topic across the year, neither of them new. One is the test pursuant to which the New Zealand intelligence agencies may *share* information with a foreign partner if there are human rights concerns. Our *Afghanistan Inquiry* disclosed evidence which suggested the threshold should be more protective of rights – ie. information should not be shared where, objectively, there is a real (not "fanciful") risk that it may be used to contribute to a serious breach of human rights. Both agencies articulate and apply a test of "clear causative link" in assessing whether their assistance gives rise to a real risk of mistreatment or torture. That is the threshold in their current, guiding, policy statement. We consider this sets the bar too high and this issue of the appropriate threshold is squarely under consideration in DPMC's consultation on possible amendments to the *Foreign Cooperation* MPS.

The second issue, also being considered in the *Foreign Cooperation* MPS review, is what obligations, if any, should be imposed on the agencies when they *receive* information which they reasonably believe may have been obtained from human rights abuses overseas, especially if there is no realistic risk their receipt of the information could contribute to any new or ongoing abuse. New Zealand law does not directly govern this, and the answer is more a question of public policy and propriety. At the business level, we recognise it might be a difficult operational exercise to identify, separate, and destroy such material. Over the year there were a number of incidents involving different countries and partners, as well as the recommendation in our 2019 *Senate Report*, which required the GCSB and NZSIS to undertake the exercise of identifying such material and making a decision on how or whether to retain it. We await the outcome of these incidents.

Inspector-General's process to safeguard international relations when finalising a public inquiry report – s 188 ISA

The IGIS must not and will not disclose classified material. He or she is also prohibited from prejudicing any of the other interests in s 188(2) ISA, including "international relations." From late 2019 we commenced discussions with the intelligence agencies, MFAT and DPMC on the process the Inspector-General will undertake to ensure that a public Inquiry Report from this Office does not disclose information that might cause harm to New Zealand's international relations. The starting point is that there must first be a proposed "disclosure" of information by this Office. We have made the point that a comment about material in the public domain through authoritative and reliable sources will generally not constitute a "disclosure" by the Inspector-General. Next, for the Inspector-General to be properly informed about whether a particular disclosure in a public Report is likely to prejudice international relations, the intelligence agencies may on occasion need a reasonable opportunity to

advise or consult their foreign partners about the proposed disclosure. MFAT will also likely have a role to play with regard to potential prejudice to New Zealand's international relations. It is in the public interest, however, to avoid any suggestion of improper interference in the independent Inspector-General's draft public Report and, accordingly, foreign consultation on any part of an IGIS Report needs to be carefully managed. Our Office decided this should happen pursuant to a clear and published statement of the roles and respective responsibilities of the Inspector-General and relevant government officials. My final statement of the Inspector-General's guiding principles and process was published in November 2020 and can be found here
www.igis.govt.nz/assets/Uploads/IGIS-Foreign-Partner-Consultation-Procedure.pdf
www.igis.govt.nz/assets/Uploads/IGIS-Foreign-Partner-Consultation-flowchart.pdf.

INQUIRIES

The Inspector-General can inquire into GCSB and NZSIS compliance with the law and into the propriety of particular agency activities. An inquiry may commence at the request of the Minister, the Prime Minister or Parliament's Intelligence and Security Committee; as a result of a complaint; or the IGIS may initiate an inquiry of his or her own volition. The ISA provides the IGIS with specific investigative powers for use in an inquiry, akin to those of a Royal Commission, eg the power to compel a witness to answer questions or produce documents. In deciding whether to initiate an inquiry the Inspector-General considers:

- Does the matter relate to a systemic issue?
- Are a large number of people affected by the issue?
- Does it raise a matter of significant public interest?
- Would the issue benefit from the use of formal interviews and other powers that are available in the context of an inquiry?
- Are recommendations required to improve agency processes?
- Is it the best use of my Office's resources?

Afghanistan Inquiry

Our *Afghanistan Inquiry* and its public Report www.igis.govt.nz/assets/Inquiries/Inquiry-into-events-in-Afghanistan.pdf (released July 2020) was largely completed by the Acting Inspector-General, Madeleine Laracy, before I commenced as Inspector-General in June 2020. The first half of this own-initiative inquiry addressed the role of the NZSIS and GCSB in events relating to NZDF Operation Burnham in 2010 and its aftermath.[6] The second half examined the agencies' response to human rights issues in Afghanistan in 2009-2013, especially in light of the publication of a number of official reports recording widespread mistreatment of detainees by certain Afghan authorities with whom the New Zealand intelligence agencies directly, or indirectly, shared information.

Report summary

Our report summary accompanied the publication of the public Report of our Inquiry. It is worth repeating:

- Intelligence support from the NZSIS and GCSB was essential to protect NZDF personnel in Afghanistan over 2009-2013. A Bureau team in Wellington was focussed on supporting NZDF activities in Afghanistan and both agencies at key points deployed personnel to Afghanistan.

- Both intelligence agencies made valuable contributions to the lead-up to Operation Burnham, carried out by NZDF on 21 August 2010. After the Operation they helped gather information relevant to assessing its outcome. In particular they helped identified whether any insurgents

6 www.beehive.govt.nz/sites/default/files/2020-07/20200717%20Report%20of%20the%20Government%20Inquiry%20into%20Operation%20Burnham.pdf

had been killed. Through this process both intelligence agencies were aware of allegations of civilian casualties.

- The agencies accurately reported to New Zealand partners the intelligence that came to their attention after Operation Burnham. Our inquiry found they could have done more to ensure that the reasonable possibility there had been civilian casualties was considered at an interagency level and reported to Ministers.

- After Operation Burnham both agencies continued to support NZDF efforts to find the insurgents targeted by the Operation, including Qari Miraj. Their work was material to Miraj's capture on 16 January 2011 by NZDF and the Afghan intelligence agency, National Directorate of Security (NDS) Department 90, which subsequently incarcerated him.

- By 2010 there was sufficient objective evidence to put the intelligence agencies on notice of a significant risk that the NDS including NDS 90 might seriously mistreat detainees, primarily to obtain confessions.

- Both agencies received a copy of Miraj's "confession" to NDS and learnt of an allegation that he had been tortured. They shared accounts of these matters with domestic partners but did not consider whether they should analyse the risks to Miraj's human rights or ensure there was wider Government consideration of the possibility he had been tortured. The NZSIS, consistent with the New Zealand Government's position, encouraged NDS to keep Miraj in custody.

- Throughout 2009-2013 the Bureau provided continuous intelligence support to NZDF in Afghanistan. The Service deployed personnel on two separate occasions over the course of NZSAS Operations Wātea and the later Awarua. At times the Service directly exchanged information with NDS, while information from the Bureau was capable of making its way indirectly to NDS.

- NDS was involved in arresting or otherwise capturing insurgents. Its detention facilities in Kabul and across Afghanistan were the subject of increasingly credible and authoritative reports of torture of detainees.

- In 2011, a United Nations Assistance Mission in Afghanistan report confirmed on-going and widespread serious mistreatment of detainees by NDS. Both intelligence agencies knew of the report. The GCSB responded by putting certain precautions in place. These were positive but needed to go further. The Service made no observable changes to its close relationship with NDS, which it had re-established when it re-deployed personnel in August 2012. Further reports and announcements confirmed the problem with NDS detention facilities. The approaches and safeguards the intelligence agencies put in place, particularly over 2012 and 2013 did not meet best practice.

- Our Inquiry finds that the intelligence agencies must take responsibility for identifying and managing risks arising from their participation in the wider New Zealand military enterprise. Those risks are not solely the responsibility of other parts of Government.

Our recommendations and the agencies' response

The formal response of the Directors-General to our Report addressed our two recommendations.

Our first recommendation related to the identification and management of risks arising from NZSIS and GCSB participation in multi-agency New Zealand military enterprises. Both agencies say they accept the recommendation in principle. The agencies note military operations are NZDF led. Accordingly, to the extent the recommendation requires the NZSIS and GCSB to ensure inter-agency planning takes place, this would require NZDF agreement.

The second recommendation reflects our view (consistent with the *Operation Burnham Inquiry's* findings) that agency policies and practices must reflect a precautionary approach to the identification of human rights risks in the context of foreign cooperation. In particular, it is not enough to have in place a limitation on intelligence sharing that applies only when the particular intelligence shared is likely to directly result in a real risk of torture or other serious human rights breaches. In our view, this threshold is too high and will almost never be encountered in practice. It creates a threshold of a direct causative link, essentially a "but for" link, before the agency needs to undertake due diligence for risk of human rights breaches to which its actions might contribute. We recommend the threshold should be a *real risk* the information *may contribute* to torture/abuse.

Our second recommendation, that the agencies' human rights test for information sharing should be more protective, has not been accepted by them at this time. The agencies' position is that any change to the policy threshold at which they mitigate risks in information sharing should only occur after the current review of the *Foreign Cooperation* MPS, led by DPMC. However, we think the more precautionary approach could be adopted now. Our recommendation is consistent with the threshold we recommended in last year's *Senate Report*, and with statements in the Government's own *Operation Burnham Inquiry* report. It is consistent with the Canadian Ministerial Directive on avoiding complicity in mistreatment by foreign entities ("substantial risk" of mistreatment) and with the United Kingdom's recently settled Principles relating to detention and the passing and receipt of intelligence relating to detainees ("real risk" of torture, rendition, et cetera).

Observations

We also made a number of observations as part of our Inquiry Report. We summarise these below:

- Quality of engagement of senior management: We consider that, during the period covered by this Inquiry, the senior levels of management in both agencies should have been more aware of the operational and legal developments arising both from their staff's deployed work and from their Wellington support to military operations activities. This would have required the Directors and senior managers to be more regularly and formally briefed by staff on a range of developing issues.

- HUMINT deployments: The classified report presents this observation in slightly different terms, but the general point is that particular challenges apply to overseas HUMINT deployments, especially in a theatre of war - like Afghanistan. We have concerns about the wisdom of deploying individuals without close support and supervision. This was particularly

the case in the first deployment under Operation Wātea. Service management was more responsive under the later Operation Awarua.

- Public sector records: There is a general obligation on all public sector agencies to keep "full and accurate" records in order to ensure accountability.[7] The GCSB and NZSIS now also have a specific duty to undertake their activities in a way that "facilitates" effective democratic oversight.[8] In this Inquiry we found the agencies have a considerable distance to go before they can satisfy the PRA standard or the facilitation obligation under the ISA. There were deficiencies in their management of important business records. The technological difficulties for the agencies in providing us with access to information understandably put pressure on them. We also appreciate the agencies were under multiple pressures over the last 18 months, including from two major external Inquiries. Ultimately, significant efforts were made by the agencies to retrieve the records necessary for this Inquiry. However, from the perspective of public sector accountability and the duty to facilitate a timely and thorough Inquiry by the agencies' primary oversight body, they should do better.

- Storage and use of emails: Access to the emails of staff in both agencies was a critical source of evidence for this Inquiry. The way in which staff used agency email accounts gives rise to two observations. First, where email is an appropriate form of record and communication for operational matters there must be processes in the agencies to ensure all relevant email records created by staff are filed and stored in a logical and retrievable way. Second, we saw a confined body of emails generated by some staff in the GCSB Wellington team that were distasteful and unprofessional. This was not the general tenor of that team's internal communications and we also saw an email that showed an appropriate management response. The Director-General of the GCSB has been clear that there is no place in the public sector culture for such communications.

- Duty to facilitate oversight: Emails are again the catalyst for an observation concerning the Inspector-General's powers and the correlative duty on the agencies to facilitate oversight. The Inspector-General must be given access to all "security records".[9] The IGIS' power to directly access emails was expressly challenged by the Directors-General in writing. The reasoning in support of this was not comprehensive or compelling, and was ultimately not pursued. A challenge to a fundamental element of effective oversight should not be made without significantly more detailed analysis. It would also be wise for it to be reviewed by Crown Law first.

- Transparency: classification and international relations issues: In respect of the NZSIS and GCSB, we share the reservations voiced by the *Operation Burnham Inquiry*, in the Observations section of its report, about over-classification of information, and the problems inherent with the concept of "foreign partner control" of historic factual information concerning New Zealand government agencies. We routinely see a tendency to over-classification by the intelligence agencies, where the likelihood of prejudice from disclosure has not been or cannot reasonably be made out. There is also the related problem of near-

7 Public Records Act 2005, s 17(1).
8 ISA, ss 3(c)(iii) and 17(d).
9 ISA, s 217(1).

permanent classification due to the lack of systematic classification review processes within the New Zealand government.

The agencies have responded positively to our observations. The current working relationship with both agencies is generally cooperative and constructive, and the agencies are responsive to requests for information.

Completion of this Inquiry means we currently have no inquiries in progress other than inquiries into individual complaints. This will allow our focus now to be on the reviews and other work signalled in the annual Work Programme.

REVIEWS

Reviews of operational activity form part of the regular programme of review of agency compliance systems. While in rare cases a review might prompt a more formal inquiry, in general reviews are less formal and are aimed at ensuring we have a good understanding of the way the agencies operate in particular areas, and strengthening agency practice and legal compliance. At the end of our review of operational activity we provide a report to the agency Director-General and often also to the responsible Minister. For the public we generally include a summary of the review in the relevant annual report, as below, or we may decide to publish a stand-alone document.

First review of NZSIS and GCSB engagement with international partners completed

We completed the inaugural review of the way in which both agencies engage with their international partners, a new item on our work programme. Given the close relationships and deep interdependence the agencies have with some of their international counterparts, particularly their Five Eyes partners, this is an important aspect of agency activity for our Office to understand and review. It will be a standing review in the years to come. What follows is the public account of this review.

Where the agencies' international cooperation is recorded in writing, much of their interaction occurs pursuant to smaller, discrete, arrangements that cover a particular area of operational activity or subject matter. Over the reporting period, we have been provided with and reviewed 18 arrangements; 12 between the NZSIS and its foreign partners and six involving the GCSB and its foreign partners. These arrangements cover a variety of subjects, and have provided us with new insights into the extent and nature of their cooperative activities.

In conducting this review, we considered the *Foreign Cooperation* MPS and the extent to which the agencies have had regard to it, as they are required to do.[10] Two requirements of the MPS are relevant to this review, they are:[11]

- to refer any new arrangement relating to cooperation and intelligence sharing they enter into with a foreign partner to the Intelligence and Security Committee of Parliament ("ISC") for noting; and
- to develop standard terms for ad hoc cooperation and intelligence sharing, which are recorded in an internal policy. These terms must be forwarded to my Office in draft for comment before being referred to the ISC for noting.

The *Foreign Cooperation* MPS came into effect on 28 September 2017. Since then neither agency has referred an arrangement to the ISC for noting. This is despite both agencies entering into significant arrangements with foreign counterparts since that date. Both agencies have asserted that on their

[10] ISA, s 158(2).

[11] Both of these requirements were originally proposed in the Hon Sir Michael Cullen, KNZM and Dame Patsy Reddy, DNZM *Intelligence and Security in a Free Society: Report of the First Independent Review of Intelligence and Security in New Zealand* (29 February 2016) at 59-60.

interpretation of the MPS they were not required to refer the arrangements to ISC. The nub of the interpretation issues, about which my Office and the agencies disagree, relates to the word "new".

From the agencies' perspective, "new" refers to arrangements with a partner with whom it has never previously had an arrangement, or arrangements with existing partners that are "sufficiently different" from arrangements in place with those partners as at September 2017. The agencies' view is based on a literal interpretation of the report of Sir Michael Cullen and Dame Patsy Reddy. While this is an available approach to interpreting the MPS, we think this approach has the consequence that very few, if any, new arrangements with existing partners (such as the Five Eyes partners) would be referred to ISC for noting.[12] Furthermore, it does not sufficiently reflect the purpose of the requirement to refer arrangements to ISC.

In reaching our view we emphasise the dual purposes of this requirement in the MPS: to empower ISC to exercise its oversight role and to support greater transparency. In light of these purposes, we think a broader interpretation should be taken to determining which arrangements require referral to ISC; we suggest *newly entered* arrangements be referred to ISC irrespective of whether they were entered into with new or existing partners. In furtherance of this we have recommended that the agencies refer two specific arrangements, that we have identified, to the ISC secretariat for provision to ISC, as soon as its membership in the new Parliament has been confirmed. The Directors-General have not accepted this recommendation in the terms in which it was made but have undertaken to review whether those two specific arrangements should be referred to the ISC for noting once the review of the *Foreign Cooperation* MPS has been completed.

In terms of the requirement to prepare standard terms for ad hoc cooperation with partners, neither agency has referred the relevant policy to my Office in draft for comment, or to the ISC for noting. The Service has known of its non-compliance with this procedural aspect of the MPS since September 2018 and the Bureau since May 2020 (at the latest). To remedy this issue, we have recommended the agencies provide the relevant policy to the ISC secretariat in order that ISC members can be informed of the policy as soon as its membership is confirmed. The Directors-General have indicated they will review the policy after the *Foreign Cooperation* MPS review has been completed and then refer their policy to ISC for noting.

Finally, we asked both agencies for access to the centralised repository of arrangements they hold which govern their relations with international counterparts. We were informed no such repository exists within the Bureau. The Bureau intends to create a repository for its international arrangements in 2021. The Service has informed us it has a register of its international arrangements. On closer inspection of the register, we found it holds some, but not all, of its international arrangements. While not required by law (or specifically required by the MPS)[13] the absence of a complete centralised repository is an issue for at least two reasons:

---

[12] This reflects experience to date despite the fact both agencies have entered very significant arrangements with their Five Eyes counterparts since the MPS was issued.

[13] The MPS requires the agencies to carry out their activities in a manner amenable to oversight (which includes the keeping of appropriate records). It took both agencies some time to compile the arrangements they had entered into with partners to provide to my Office to review. We think a centralised register is one way of giving effect to this aspect of the MPS.

1. It makes it difficult for the organisation to have visibility of the full range of obligations it owes under those arrangements and for Senior Leadership to exercise strategic oversight of the agency's international relationships.

2. It is an effective means of facilitating our oversight. In the future it would expedite our access to relevant documents.

Reviews of NZSIS and GCSB open source intelligence collection and online operations – in progress

Last year's annual report noted we had commenced separate reviews of NZSIS and GCSB open source intelligence collection and online operations involving open source information. Over the course of the past year we have made substantial progress on the review and hoped to have a draft report completed by the end of June 2020. However, in part owing to COVID-19 and the associated lockdown, our progress slowed. We now anticipate completing the review early in 2021.

At its simplest, "open source" information is information collected from publicly available sources. Given the potentially vast scope of agency open source intelligence collection and online operations, we have limited this initial review to two case studies to enable us to focus our assessment on whether their compliance systems are effective and appropriate for the particular activity. We are especially interested in the legal and privacy principles they apply when doing this type of work.

For open source intelligence collection we selected an NZSIS case study involving a contribution to a wider government response. For the Bureau we chose a case study involving the collection and analysis of publicly available information from various sources to identify a particular location relevant to a longstanding intelligence operation.

In terms of online operations, we have chosen case studies where the agencies have, separately, used assumed identities online for the purpose of covert intelligence collection. Otherwise lawful open source activities are specifically permitted under the ISA. Both agencies carry out online operations in different ways, which in turn impacts on the way relevant legal principles apply to their activities.

Review of access to information infrastructures – in progress

A review of GCSB's conduct of certain operations to access information infrastructures was substantially progressed in 2019-20. The operations examined are classified to an extent that effectively precludes public reporting, but the review documented the Bureau's compliance systems for controlling them in detail and found they were generally effective and appropriate. Recommendations will be finalised in 2020.

Review of access to a particular network system – in progress

We commenced a baseline review of the Service's access to a particular network system. The review is directed at understanding the extent of the Service's access, the use of such information captured by the network system and the lawfulness and propriety of the activities. As part of this work, we are engaged in ongoing consultation with the Privacy Commissioner given his expertise in this area, and the general parallels with surveillance activity undertaken by other parts of government. We anticipate reporting further on this review within the upcoming financial year.

Participation in reviews of NZSIS Direct Access Agreements

The ISA enables an intelligence agency to have direct access to certain public sector databases, by written agreement between relevant ministers. All Direct Access Agreements ("DAAs") must be reviewed by the signatory Ministers every three years, in consultation with our Office and the Privacy Commissioner.[14]

The NZSIS currently has three DAAs[15], for access to the Advanced Passenger Processing ("APP") database held by the Ministry of Business, Innovation and Employment; to the New Zealand Customs' Service's primary operational database (CusMod); and to births, deaths and marriages information held by the Registrar-General. We participated in agency reviews of the first two DAAs this year.

In the review of the APP agreement we queried the rationale for the NZSIS retaining a copy of APP data for 10 years, based on how it had used the data in the past 3 years. We asked why a review of the retention period was not conducted 12 months after the agreement was entered into (as required by the DAA). We suggested the Service should include reference to any APP information it holds when responding to requests for information under the Privacy Act 1993.[16] We sought clarification of the extent to which partner agencies can access APP data. We also questioned the accessibility of the DAA to the public.

When consulted on the CusMod DAA we expressed concern that although the DAA requires an audit at least once a year of NZSIS' compliance with the conditions on its access, only one full audit has been completed since the agreement took effect in March 2017. We suggested audit frequency should be tied to compliance levels, so poor compliance would trigger a re-audit on a shorter timeframe, while an acceptable audit result would allow continued annual auditing. We also proposed declassification of a large part of the Privacy Impact Assessment for the agreement, which we consider to be over-classified.

We have been informed by the Service that both the APP and CusMod DAAs will be amended. We will be consulted again regarding any proposed amendments.

[14] ISA, ss 124-133 and schedule 2..
[15] The terms of the DAA are available at www.nzsis.govt.nz/our-work/our-methods/working-with-other-organisations.
[16] From December 2020, the Privacy Act 2020.

AGENCY IMPLEMENTATION OF RECENT IGIS RECOMMENDATIONS

The Inspector-General can and usually does make recommendations as a result of inquiries and reviews. These are non-binding, but we seek to ensure they are practicable to implement and will add value. We seek and generally receive agreement from the relevant agency that they will be implemented. We report below the extent to which the agencies have implemented our more recent formal recommendations.

Inquiry into possible New Zealand engagement with CIA detention and interrogation 2001-2009 ("*Senate Inquiry*" published 2019)

The Inspector-General's *Report of the Inquiry into possible New Zealand intelligence and security agencies' engagement with the CIA detention and interrogation programme 2001-2009*, followed the 2014 publication by the US Senate Intelligence Committee's report on activities of the CIA.[17] Our report, published July 2019, found that NZSIS and GCSB had lines of connection to the CIA but were not complicit or otherwise involved in torture or ill-treatment of detainees. We examined whether the agencies' policies are adequate to safeguard against the risks of improper or unlawful behaviour when engaging cooperatively with partner countries. The report added significantly to the publicly available information about how the agencies cooperate with foreign partners and provide support to military operations. Our Report made eleven recommendations for the GCSB and NZSIS across seven key areas. We report below on the extent of their implementation.

The IGIS recommended[18] early reviews of the overarching guidance document, the *Foreign Cooperation* MPS, and of the NZSIS and GCSB's Joint Policy Statement on Human Rights Risk Management (JPS) which sits beneath it. We recommended the agencies address the deficiencies identified in our report within six months of its publication. Under the Act the MPS is due for review by DPMC after three years (September 2020). The review by the agencies of the JPS has not been commenced, as they consider the MPS review must be completed first. We do not agree that all aspects of the JPS revision need to await the new MPS. Separately, and in fulfilment of another recommendation, the agencies have delivered improved documents to better inform Ministerial authorisations for both information sharing with foreign countries and granting Approved Party status to selected partners.[19] We still await agency action regarding recommendations concerning their policy and practice to implement best practice advice eg, to monitor partner country human rights records, and to review historic files which may contain information obtained by the torture of detainees.[20]

One recommendation concerned record-keeping of government authorisations for GCSB and NZSIS support to military deployments, and another, the need for adequate GCSB and NZSIS training and support for staff supporting such operations.[21] The extent to which the agencies have implemented

---

17 Hence the short title of our own Inquiry and report: *Senate Inquiry Report.*
18 Recommendations A and C.
19 Recommendations B and D.
20 Recommendations G, H, I, K.
21 Recommendations E and F respectively.

these recommendations will be considered under the IGIS's baseline review in our Work Programme for 2020-2021 on "whether the NZSIS or GCSB currently provide any support to New Zealand military operations and, if so, the nature of that support".

Lastly, we recommended a whole of government approach to cooperation and information sharing when serious issues have been raised regarding a partner state or agency.[22] We maintain a watching brief on this area, revisited in our recently published report on our *Afghanistan Inquiry*.

Implementation of recommendations from the review of adverse and qualified security clearances

Last year we reported on the completion of a review of a sample of adverse and qualified security clearance recommendations made by NZSIS over a specified period. We advised that six of the seven recommendations were directed at modifications of practice and the remaining one related to a notation being placed on a particular file to better ensure natural justice. NZSIS accepted all the recommendations except for one practice related recommendation. In respect of this recommendation we have been unable to reach an agreed position with the Service. We are not presently pursuing the issue further as we are hopeful that the improved application of natural justice principles will, in any particular vetting case, mitigate our remaining concerns. We are willing to revisit the issue if a future investigation or review reveals that our particular natural justice concern has not in fact been addressed.

Implementation of recommendations from the review of NZSIS requests made without warrants to financial service providers

In November 2018 we released our public Report about the Service's practice of making requests to financial service providers (mainly banks) for the voluntary provision of customer information. Three recommendations arose from the review. In 2018, in response to our first recommendation, the Service improved its financial information register to ensure it kept a record of all requests made to financial service providers, including those made under s 121 ISA (the Act's recognition of the common law right of any person or agency to "ask" for information). More recently, further work has been done to ensure the register is complete. In response to our second recommendation, in 2019, the Service has developed the required framework to guide when the use of the following is more appropriate: a request under s 121 ISA, a business records direction, or a warrant. Our third recommendation concerned the retention of irrelevant information obtained through the voluntary request process. We advised that such information should be deleted, but the NZSIS said it needed a disposal authority to do so. In August 2020 we were advised that a disposal schedule (provided to Archives New Zealand in May 2019) has been approved by the Chief Archivist and can now be used. We are satisfied that these steps adequately implement the recommendations from this review. This is, however, an area that we will continue to monitor.

NZSIS relationships at the border

We reported on this review in last year's annual report. The NZSIS interacts with a range of government agencies at New Zealand's borders. Our review recommended creation of, or improvements to, the documentation and agreed arrangements that govern the main forms of NZSIS

[22] Recommendation J.

engagement with these agencies. The Service expressed an intention to update relevant Memoranda of Understanding (MOU) and to enter an MOU with New Zealand Customs early in 2020. To date this work is yet to be completed. We note that some delay was due to the fact that the Service anticipated that the work would be informed by the findings of the *Royal Commission on Christchurch*.

COMPLAINTS

Any New Zealand person[23] and any employee or former employee of the GCSB or NZSIS may complain to the Inspector-General that they have or may have been adversely affected by an act, omission, practice, policy or procedure of the GCSB or NZSIS.[24] An inquiry into a complaint must be conducted in private and the complainant must be advised of the outcome in terms that will not prejudice the security, defence or international relations of New Zealand.[25] The scope for public reporting on complaint investigations is accordingly limited.

Not all complaints require a formal inquiry. As is typical, a substantial proportion of complaints received in the reporting year were from members of the public expressing concern, without evidential foundation, that one or both of the agencies had them under surveillance, or was using some kind of weapon against them.

Many approaches to our Office, expressed as complaints, are more accurately understood as requests for personal information under the Privacy Act 1993/2020 or for information under the Official Information Act 1982. These contacts are generally advised to redirect their request to the agency or agencies that might hold the information, with a right of complaint to the Privacy Commissioner, Ombudsman or IGIS if the response is unsatisfactory.

A common subject of complaints that require inquiries is the conduct of security clearance assessments ('vetting') by the NZSIS. This is a consequence of the large number of assessments conducted each year by the Service, the complexity of some assessments, and the gravity of the employment consequences for candidates receiving adverse assessments.

An inquiry into a vetting complaint received during the 2018-19 year was completed. The complaint was upheld. This inquiry questioned whether the vetting recommendation given by the Service was evidence or prejudice based. While we did not find the NZSIS' vetting recommendation to be prejudice based, we found the evidence relied upon by the Service to assess the security vetting application was insufficiently reliable (because of its age). The inquiry resulted in two recommendations, both of which were accepted by the NZSIS.

One complaint that was received during the reporting period involved a matter that was outside the jurisdiction for the IGIS to investigate.

Another substantive complaint alleged that the Service was historically engaged in unlawful and/or improper activity. We did not find there was any conduct of that type.

---

23 As defined in ISA, s 4.

24 ISA, s 171. Employees and former employees generally have to exhaust any internal complaints procedures before the Inspector-General has jurisdiction.

25 ISA, ss 176(1) and 185(5).

We have also responded to judicial review proceedings in the High Court, where we were named as the second respondent. We considered that the basis for including the IGIS engaged a matter that was beyond the IGIS' jurisdiction. On our application, the IGIS was struck out from the proceedings.

Complaints received 2019-20		
From	**Against GCSB**	**Against NZSIS**
Members of the public	4	9
Intelligence agency employees or former employees	0	0
Total	4	9

WARRANTS

In this reporting year, the Office reviewed 90 warrants, including applications for amendments to or revocations of warrants. This was a significant increase on the number of substantive Type 1 and 2 warrants issued and reviewed the previous year (58).[26]

Warrants, amendments and revocations reviewed 2019-20							
	Type 1	Type 2	Practice	Removal	Revocation	Amend-ments	Total
NZSIS	22	4	3	0	6	0	35
GCSB	21	25	0	N/A	2	7	53
Total	43	29	3	0	8	7	90

Warrants are issued to enable the agencies to carry out activities that would otherwise be unlawful, including surveillance, search, seizure and interception. A Type 1 warrant is issued for any otherwise unlawful activity that is to be undertaken for the purpose of collecting information about, or doing any other thing in relation to a New Zealander or a class of persons that includes a New Zealander.[27] A Type 2 warrant is issued when a Type 1 is not required. Practice warrants are issued for testing or training purposes. A removal warrant is issued to cover the removal of any device or equipment (eg a listening device) that has been installed in premises under a warrant. Both Type 1 and Type 2 warrants can be amended or revoked at any time.[28]

In reviewing the warrants, we have identified and focussed on a number of themes. The key themes across both NZSIS and GCSB are the case put up by the agency for the proportionality of the proposed activity, the threshold for targeting an individual or class of individuals and, significantly, the management and retention of material obtained pursuant to warrant. There are also issues and themes specific to each agency. In relation to the Service, we have focussed on the identification of the risk of breaching privilege and the processes in place to ensure the protection of privileged material. We have also reached agreement with the Service that, as a matter of best practice, the conditions included in the warrant application should be reflected in the warrant document itself. For the Bureau, one of the themes we have continued to focus on is the scope and clarity of the target class.

[26] Noting, however, that our comparative methodology has changed. This year we have counted the 7 amendments and 8 revocations whereas these were not included last year (albeit re-issued warrants were).

[27] A New Zealander is a New Zealand citizen or permanent resident. ISA,s 53.

[28] ISA, s 84.

Irregular warrants

Under s 163 ISA the Inspector-General may conclude that a warrant, or activity carried out under a warrant, is "irregular".[29] The IGIS then has discretion as to whether to report the irregularity to the Minister and (in the case of a Type 1 warrant) the Chief Commissioner of Intelligence Warrants. A finding of irregularity does not invalidate the warrant or make the activity unlawful,[30] but the Inspector-General may recommend that all or any specified information obtained is destroyed.[31]

Our Office has previously expressed the view that a warrant will be irregular where there is a significant departure from standards of legality and/or propriety.

The first GCSB warrant our Office found irregular was a Type 2 warrant relating to an activity the Bureau undertakes with assistance from a foreign partner. In former Inspector-General Gwyn's view, the warrant application lacked a candid and accurate description of the capability being authorised, and an inaccurate description of the level of control, supervision and oversight the Bureau would have over the partner's assistance. It was also unclear the extent to which my Office could (or could not) exercise oversight over the relevant activities.

In conducting our review of the warrant, we also found there was a period of nearly 3 months in which the Bureau had not issued a s 51 request to the partner for assistance. In our view there was a strong likelihood the activity was unlawful for that time (although any unlawfulness would have been at the less serious end of the criminal spectrum). The Bureau has accepted it was too slow to put in place the s 51 request for assistance. While a serious matter, we decided this was not irregular for a number of reasons, including the fact of my Office's initial finding of irregularity in relation to the authorising warrant.

Both aspects of the respective IGIS' findings have directly resulted in significant improvements in the relevant Bureau policy and practice.

I also found irregular a Type 1 warrant the Bureau sought to renew against a small number of named New Zealanders without, in my view, sufficient explanation of the case for continued activities against them. The application also sought authorisation for continuation of a particular type of information gathering despite draft internal advice that it was unnecessary, and described the warrant as a short term extension of the preceding warrant despite it being sought for a longer term. The application was made under time pressure around the period of the Covid-19 lockdown but even making some allowance for that I found it fell short of the required legal standards.

I found one NZSIS Type 1 warrant irregular in respect of some of the New Zealanders named as its targets, for want of adequate demonstration in the application that the proposed activity against them (which was very limited) was necessary to contribute to the protection of national security. The warrant was sought retrospectively, when the Service became aware as a result of legal advice that certain actions it had already taken required authorisation. The circumstances were unusual and I was satisfied that this was the main source of the problem.

---

[29] Irregularity is undefined but the approach of the Inspector-General is to identify a warrant or activity as irregular if it involves a significant departure from the requirements of the ISA or from well-recognised legal principles.

[30] ISA, s 163.

[31] ISA, s 163(3).

CERTIFICATION OF COMPLIANCE SYSTEMS

Our approach

The Inspector-General must certify in each annual report "the extent to which each agency's compliance systems are sound".[32] This is not a certification that every action of the agencies has been lawful and proper. It is an assessment of the agencies' approaches to minimising the risk of illegality and impropriety.

As signalled in the 2018-19 annual report, this year we have changed how we make this assessment. Formerly we stated an overall conclusion on whether each agency had sound compliance procedures and systems in place. That had the virtue of simplicity, but the disadvantage of requiring a blunt choice to be made. The law does not require such a choice. As the agencies' compliance systems develop, it becomes increasingly important to pay attention to details. An effective compliance system has several dimensions. In any given year an agency might be stronger in some respects and weaker in others. For this reason we have developed a template for our assessment that specifies the matters we consider. We rate each agency on five main headings, rather than stating a single assessment.

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

[32] ISA, s 222(2)(c).

- 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 2019-20

Our assessment of the compliance systems of both agencies for 2019-20 follow, applying the framework above. For each heading we give the rating for each agency, then a summary of the information underlying our assessment.

Operational policy and procedure

GCSB	**Well-developed**
NZSIS	**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. The Service rationalised a number of operational policies and procedures in the year under review to reduce their number and make them more concise. The Bureau, having revoked a number of outdated policies in 2018-19, further assessed its operational policies early in 2019-20 and identified a substantial number as requiring detailed review or substantial amendment.

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. Neither however has a system that dependably provides access to policies that are relevant and current. Planning for improvement of the Service's intranet portal for policy was began in 2019-20 and was still in progress at year end. The Bureau's systems continue to hold a number of policies whose currency is unclear as they have passed their review dates, in some cases by several years.

Specialist policy staff?

Both agencies had the equivalent of one full-time dedicated policy advisor/policy review staff available over the reporting period. This was the normal complement for the Service and half the normal complement for the Bureau. Both agencies, but particularly the Bureau, also have subject matter experts who contribute substantially to operational policy.

A programme of policy review?

The Service commissioned a review of its operational policies in 2018-19 and in the year under review undertook some of the recommended changes. The Bureau established an internal leadership group in early 2019-20 to review operational policy and began identifying and prioritising necessary updates.

Timely remediation of any deficiencies in policy or procedure?

While both agencies have in the past year taken steps to try to provide more leadership and direction to policy development, both rely on a very few specialist policy staff to drive policy work. Progress is modest with such limited resources. In the Bureau it was further limited in 2019-20 by under-staffing of policy roles.

Internal compliance programmes

GCSB	**Under-developed**
NZSIS	**Well-developed**

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

Both agencies bring consistent principles to the promotion of 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. Both also have relevant policies in place, eg on risk management. To that extent both have the elements of a strategic approach to compliance. Neither has a compliance strategy that is documented as such and endorsed by its senior leadership, but both propose to develop one.

Specialist compliance staff?

Both agencies have small specialist compliance teams, made up of experienced and capable staff. They provide advice on operational policy questions; create, revise and advise on operational policy; carry out audits; and investigate and report on self-reported compliance incidents. NZSIS compliance staffing is modest for the size of the organisation, with limited audit capacity until recently. The GCSB compliance team was seriously under-staffed for most of the year under review.

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

NZSIS had a very modest plan for six audits/reviews in 2019-20. A late start, limited audit resources and diversion of compliance staff to Covid-19 related work in the last quarter of the year meant only one item was completed by year end.

The Bureau carries out regular routine audits of queries (searches) of signals intelligence databases and prepares an audit plan each year designed to provide, over time, a systematic review of all its operations and activities. It prepared a sound audit plan for 2019-20 but did not implement it. By year end it had completed three audits carried over from 2018-19 and one spot audit. It did not prepare an audit plan for the year to July 2020 but proposed 11 audits for calendar 2020, none of which were completed by July. Some disruption to audit work was caused by Covid-19 but the primary issue was under-staffing of the compliance team, causing audit staff, once appointed, to be diverted to other work.

Both agencies' under-delivery on audit plans repeated a pattern established in the preceding two years.

Timely remediation of any shortcomings found by audits?

Neither agency has completed enough of its planned audits to ground a firm assessment of whether their action on audit recommendations is generally timely. Audit recommendations are seldom made with clear timeframes for execution; nor does either agency systematically track implementation of audit recommendations.

Few of the audits completed by NZSIS have resulted in recommendations requiring significant work. Where changes to policies, procedures or systems have been recommended they seem largely to have been actioned. In 2019-20 there was little relevant work to be done in this area given there was little audit work completed during the year, or the year before.

GCSB's implementation of audit recommendations is difficult to assess. Some have certainly been actioned; some have not, or are in train. Although past attempts within the Bureau to track action on audit recommendations have faltered, a new effort to do so is under way.

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

Both agencies' compliance staff report to senior leadership and seek to identify any systemic issues underlying compliance incidents. Both have limited capability to provide analytical reporting on statistics and trends, but are establishing record keeping systems to facilitate this.

NZSIS compliance team maintained its normal level of reporting to senior leadership in 2019-20, except for an interruption due to the Covid-19 lockdown.

GCSB senior managers engaged individually with the compliance manager on relevant issues in 2019-20 but the senior leadership team received very little formal reporting. This was mainly due to very limited resourcing of compliance for much of the year, but also to a recognised lack of capacity to provide meaningful statistical analysis of compliance incidents and trends. Such analysis would be of particular value for the Bureau, as it operates a broad range of collection and analytical systems giving rise to diverse and complex compliance issues.

Proactive measures to maintain or improve compliance?

In 2019-20 the Service completed its analysis of results from a 2019 survey of staff awareness of compliance obligations under the ISA. It identified one area in which improvements are required. GCSB emphasises the provision of advice from compliance staff, particularly on operational planning and the preparation of operational guidance documents, as its main proactive effort to promote compliance.

Self-reporting and investigation of compliance incidents

GCSB	**Well-developed**
NZSIS	**Well-developed**

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

The levels of self-reporting in each agency and the nature of the incidents reported (which in both agencies includes possible, not just self-evident breaches) indicate well-established cultures of willing self-reporting.

Established policies and procedures for responding to compliance issues?

The Service has relevant policy that is up to date. Policy is high-level, so in practice the assessment and investigation of compliance incidents is significantly at the discretion of the compliance manager and dependent on their skills and experience.

The Bureau's documentation of compliance policies and procedures is significantly out of date. There are well established practices for responding to compliance issues, but these are heavily reliant on the institutional knowledge and skills of relevant staff.

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

Both agencies, encourage self-reporting of compliance issues. Reporting and investigation records indicate that breaches and suspected breaches of compliance obligations are willingly reported. Analysis and investigation of reported incidents is focused on identifying any systemic issues, not on assigning individual blame.

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

In both agencies straightforward compliance incidents are usually analysed promptly. More complex incidents are investigated thoroughly, with an effective focus on identifying systematic issues and remedies. Service investigations typically take several months given the modest resources for undertaking them. Bureau investigations vary widely in duration and complex incidents may take several months to resolve. In the year under review Bureau compliance investigations were particularly subject to delay, given the short staffing of the compliance team.

Timely reporting of compliance incidents to the IGIS?

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

Training

GCSB	**Well-developed**
NZSIS	**Well-developed**

A training strategy including comprehensive induction and refresher training programmes?

Both agencies run induction and refresher training. In the year under review they developed and adopted a joint learning and development strategy, whose implementation is to include bi-annual training needs analyses. The Service developed and adopted an operational training strategy in 2019-20. The Bureau has mandatory training courses for compliance with the ISA and in 2019-20 began reviewing and developing some key elements of its programme. GCSB does not yet have an operational training strategy as such.

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

The training needs analyses proposed under the agencies' joint Learning and Development strategy should achieve this but are yet to occur. In 2019-20, the Service's work on its operational training strategy began identifying gaps in training and a need to diversify how training is delivered. The Bureau continued to establish, review and update training programmes case by case.

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 reserved for the purpose.

Responsiveness to oversight

GCSB	**Well-developed**
NZSIS	**Well-developed**

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

The agencies' engagement with this Office is generally cooperative and constructive, but still not consistently so. Interactions with agency staff are typically routine, professional and reasonably efficient. This Office has become stricter with timeframes for producing information and much is provided promptly, or reasonably so, without question. Over time both agencies have become readier to acknowledge where they can and will improve their systems and practices. In some respects, cooperation on the major *Afghanistan Inquiry* completed in the year under review was not always satisfactory. While some tension is unavoidable in the oversight relationship, this Office at times finds the agencies overly defensive.

The Service has become more proactive in briefing this Office on new activities or procedures that have implications for oversight, seeking comment where appropriate. This has been of real value.

The Bureau provided some particularly good briefings in the year under review. The short-staffing of its compliance team caused delays on some investigative and policy questions.

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

Both agencies engage regularly with this Office on legal issues arising from our reviews and inquiries. Interactions with the Bureau on some legal questions were protracted, although this was in part due to difficult issues requiring the Bureau to seek advice from Crown Law.

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

Both agencies commit resources to dealing with oversight. Operational staff, when made available, are generally frank and informative. Both agencies tend to rely heavily on their legal and compliance teams as points of contact for the IGIS. The small size and consequent heavy workloads of those teams at times limit their ability to respond to requests and queries from the IGIS. In the year under review both agencies faced unusual demands from the external *Operation Burnham Inquiry* and the *Royal Commission on Christchurch*, as well as significant IGIS inquiries, creating some tension over whether responding to IGIS oversight was sufficiently resourced.

Timely and effective implementation of accepted IGIS recommendations?

Our system for tracking agency implementation of IGIS recommendations requires further development and the timeliness of agency actions can be difficult to assess from outside. Some recommendations for the Service from reviews and inquiries in recent years have been implemented or are in train, at variable pace. Accepted recommendations arising from warrant reviews have generally been acted on promptly. The Bureau has been subject to fewer recommendations from inquiries and reviews and many seem to have been implemented. Recommended changes to warrants have generally been subject of more extended debate and consideration, but some substantial changes have resulted.

OUTREACH AND ENGAGEMENT

Meetings with foreign oversight counterparts

For us, relationships with foreign oversight bodies who conduct a similar role to ours, mainly in Europe or in Five Eyes countries, provide an invaluable point of reference for our own oversight practice. From reading each other's published reports and annual reports, and exchanging ideas in person where possible, we identify best practice approaches to oversight, common concerns and challenges, and independent reassurance about the value of the issues we are each pursuing. For 2019 it was arranged that two important meetings for intelligence oversight bodies would be held sequentially in London. The Acting-Inspector-General, Madeleine Laracy, attended those meetings.

The International Intelligence Oversight Forum is chaired by the UN Special Rapporteur on the right to privacy. The meeting reflected a wide breadth of issues and perspectives as it was attended by intelligence oversight bodies from around the world. Key topics of discussion were different models of oversight and their relative strengths; the challenge of maintaining independence in oversight while also being connected to intelligence agencies; the need for agencies to have strong internal compliance systems as well as external oversight; and, the crucial proposition that oversight cannot rely on vague principles, but needs to be guided by specific and detailed legal standards.

The Five Eyes Intelligence Oversight and Review Council ("FIORC") comprises the non-Parliamentary intelligence oversight and review bodes from the UK, USA, Canada, Australian and New Zealand. One of FIORC's common purposes, confirmed in the FIORC Charter, is to encourage transparency about the work of oversight to the greatest extent possible and to enhance public trust. This year's workshop was hosted by the then UK Investigatory Powers Commissioner, Sir Adrian Fulford. Major themes were the value of transparency and publishing in building trust and accountability; the fact of increasing data retention by intelligence agencies and the legal and oversight issues that raises; and problems with international intelligence sharing, including human rights abuses. A significant development at the October 2019 Council meeting was the agreement to set up three working groups, led by officials from each of the FIORC countries, to compare perspectives on the principles that should govern intelligence agency activity in three specific areas: international intelligence cooperation and human rights abuses; artificial intelligence/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.

Advisory Panel

The primary role of the Advisory Panel is to provide advice to the Inspector-General.[33] The Panel does not have an oversight role. Instead, through having an objective but informed view on the issues and material the IGIS is looking at, it can debate matters with us and enhance our thinking. The Panel's two members (Angela Foulkes as Chair and Lyn Provost) have security clearances for access to

[33] ISA s 168.

classified information, which is necessary to have informed discussions. The Panel may provide advice in response to a request from the IGIS, or of its own motion.

This year we met with the Panel seven times. As in previous years, the Panel discussed challenging issues with us as they arose, and engaged with us on the content of our draft reports, offering detailed comments particularly on the themes that stood out for them. As a new Inspector-General, I have appreciated the insights of the Advisory Panel.

Other integrity agencies

Our closest working relationship with other integrity agencies tends to be with the Office of the Privacy Commissioner, and we have continued over the course of the year to share information with the Privacy Commissioner where that is appropriate, or to seek that Office's expertise on particular matters. We have also found it useful and supportive to attend regular presentations for public sector leaders co-hosted by the Auditor-General's Office and Transparency International which cover a range of issues concerning the integrity of the public sector. The Acting Inspector-General and I also maintained involvement in the scheduled meetings of the Intelligence and Security Oversight Coordination Group, which is comprised of the Inspector-General, the Privacy Commissioner, the Chief Ombudsman and the Auditor-General.

Public presentations

We have both accepted opportunities to speak to university and public sector groups, as well as to address staff working in the intelligence agencies. The Acting Inspector-General gave a television interview (Newshub, September 2019); presented the 2019 Annual Report to the Intelligence and Security Committee; and appeared as a witness before the Justice Select Committee in respect of its *Inquiry into the 2017 general election and 2016 local elections.*

OFFICE FINANCES AND ADMINISTRATION

Funding and resourcing

The IGIS Office is funded through two channels. A Permanent Legislative Authority covers the remuneration of the Inspector-General and the Deputy Inspector-General. Operating costs are funded from Vote: Justice (Equity Promotion and Protection Services), as part of the Ministry of Justice's non-Ministry appropriations.

2019-20 budget and actual expenditure

Total expenditure for 2019-2020 was $1.584 million, as follows:

Office of the Inspector-General of Intelligence and Security 2019-20 Budget		
	Actual ($000s)	***Budget***
Staff salaries/advisory panel fees; travel	770	826
Premises rental and associated services	358	378
Other expenses	16	67
Non-Departmental Output Expenses (PLA)	440	644
Total	**1584**	**1915**

Our premises and systems

In October 2019 we moved to a new Office located in Defence House, Bowen St, Wellington. We had worked out of temporary premises as the 2016 Kaikoura earthquake significantly damaged the previous Defence House. The new Office is comfortably set up for the needs of our current staff. There is little scope for an increase over time in the size of our team given the fixed size of our Office.

The security of the IGIS Office and its computer network were assessed by an independent security consultant in early 2020 and were found to meet all requisite standards and were accredited as such. This is a three yearly requirement of the New Zealand Security Information Manual and provides assurance to the government and the public that all information held, is suitably protected.

Administrative support

The New Zealand Defence Force provides some IT support to the Office, on a cost-recovery basis. 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 our Office. I am especially grateful for the ongoing assistance provided to us this year by personnel in the Ministry of Justice's finance, legal and communications teams.

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