Office of the Inspector-General of Intelligence and Security

Annual Report

For the year 1 July 2018 to 30 June 2019

Madeleine Laracy
Acting Inspector-General of Intelligence and Security
5 November 2019

CONTENTS

FOREWORD 2
EFFECTIVENESS OF OVERSIGHT 4
KEY ISSUES IN 2018-19 7
THE YEAR AHEAD 11
INQUIRIES 12
REVIEWS 14
COMPLAINTS 16
WARRANTS 18
CERTIFICATION OF COMPLIANCE SYSTEMS 19
OUTREACH AND ENGAGEMENT 25
OFFICE FINANCES AND ADMINISTRATION 27

OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

5 November 2019

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

Dear Prime Minister

Inspector-General's Annual Report 2018-2019

As Acting Inspector-General of Intelligence and Security I **enclose** my annual report for the period 1 July 2018 – 30 June 2019.

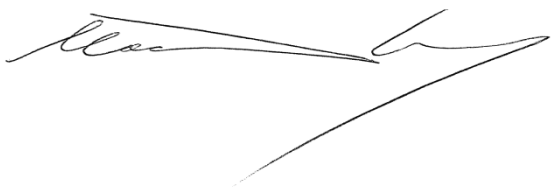
You are required, as soon as practicable, to present a copy of the Inspector-General's report to the House of Representatives (s 222(3) Intelligence and Security Act 2017 – "the Act"), together with a statement as to whether any matter has been excluded from that copy of the report. In my view, there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

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 as soon as practicable.

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

Yours sincerely



Madeleine Laracy
Acting 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

This report covers the last year of the tenure of Cheryl Gwyn as Inspector-General of Intelligence and Security. On 9 August 2019 Cheryl – now Justice Gwyn – was sworn in as a judge of the High Court of New Zealand.

During her five years as Inspector-General Cheryl transformed the oversight of New Zealand's intelligence agencies, the New Zealand Security Intelligence Service (NZSIS) and the Government Communications Security Bureau (GCSB). Cheryl is widely recognised – in Parliament, civil society, the news media, the international oversight community and the agencies themselves – as having set a formidable standard for independence, courage, integrity and rigour in the task of holding the agencies to account. She led the development of the office, which was given more resources and a wider mandate by legislative reform in 2013, from a part-time, one-person operation into a stronger, wider-ranging and more publicly-visible operation – still small, but with an impact belying its size. A considerable part of that impact was due to Cheryl herself, who demonstrates the kind of authority that comes from intellect, a redoubtable work ethic and a dedication to reason and principle.

Cheryl was Inspector-General for the full year covered by this report and I was Deputy Inspector-General. Although, with Cheryl's departure, the preparation of this report has fallen to me as Acting Inspector-General, I am confident that it reflects her assessment of the period as well as my own.

As no-one can forget, the past year saw a horrific act of terrorism committed in New Zealand. The alleged perpetrator of the attacks on the Christchurch mosques on 15 March 2019 is to be tried. A Royal Commission has been charged with investigating what happened and the performance of state agencies, including the intelligence agencies, in relation to the attacks. In deference to those processes you will read little about Christchurch in this report. Our office reviewed intelligence warrants relating to investigations following the attacks. We have provided information, and made ourselves available, to the Royal Commission. We await its findings and anticipate work arising from its findings and recommendations. Like all New Zealanders, we grieve for the lives lost, the pain inflicted on families, friends and community, and the arrival in New Zealand of such fear and hate. It is important that I acknowledge also the real distress felt within the intelligence community at this terrible event.

The law requires this report to specify the number of inquiries undertaken by the Inspector-General during the year.[1] Inquiries are a separate category of work from our operational review work. On a strict count the number of inquiries undertaken over the past year is six: four inquiries into complaints, plus our two major own-motion inquiries (into possible New Zealand engagement with CIA detention and interrogation 2001-2009, and into the role, if any, of the GCSB and the NZSIS in relation to specific events in Afghanistan in 2009-2013). I trust, however, that this report as a whole will provide a more illuminating account of our work.

The effectiveness of our oversight will primarily be judged by the quality of the work we do and whether it withstands public scrutiny. Cheryl and I have a superb team to thank for that work. Our

1 Intelligence and Security Act 2017 (ISA) s 222(2)(a).

reports reflect their rigorous analysis, persistence and attention to detail. I thank all members of our small team for the unstinting support and expertise they have offered us both.

EFFECTIVENESS OF OVERSIGHT

Independence and rigour

The Inspector-General provides independent oversight of New Zealand's two dedicated intelligence and security agencies, the New Zealand Security Intelligence Service (NZSIS, or 'the Service') and the Government Communications Security Bureau (GCSB, or 'the Bureau'), to ensure they act lawfully and with propriety.[2]

Lawfulness requires more than compliance with the statute governing the agencies, the Intelligence and Security Act 2017 (ISA). It also requires the agencies' conduct to be within the bounds of the general common law unless the agencies are specifically exempted, and to be consistent with fundamental rights including those affirmed in the New Zealand Bill of Rights Act 1990. "Propriety" is not defined in the ISA but has a broader reach than specific questions of legality. It encompasses whether the agencies have acted in a way that a fully-informed and objective observer would consider appropriate and justifiable in a free and democratic society.

An active and capable Office of the Inspector-General is essential to maintaining public confidence that the specialised, intrusive capabilities of the agencies are used appropriately, in the interests of New Zealanders. Oversight combines strict independence, verification, and transparency to increase agency accountability, increase public understanding of the agencies' work, and encourage the agencies to improve continuously their operational processes and standards.

Public reporting

Public reporting is a key element of effective oversight. The secrecy under which the intelligence agencies operate constrains the usual constitutional accountability mechanisms, such as access to the courts and access to information under the Official Information Act 1982 or Privacy Act 1993. The Inspector-General is uniquely placed to examine and publicly explain, within appropriate limits, the operational activities of the New Zealand agencies.

Publication does not just increase public awareness and interest, but is often a stimulus for the agencies to engage promptly and effectively with the requirements of oversight. Publication will often prompt the agencies to confirm their response to a recommendation in one of our reports; act to remedy an area of weakness or criticism; obtain legal advice; finalise and articulate their view on an outstanding issue; or in other ways "facilitate" oversight as the ISA requires.[3]

In the reporting year, in addition to the mandatory annual report, the Inspector-General published:

- Reports on:
    - An inquiry into complaints arising from reports of GCSB Intelligence activity in relation to the South Pacific, 2009-2015 (July 2018)
    - A review of the New Zealand security classification system (September 2018)

[2] ISA s 156.
[3] ISA s 17(d).

    - A review of NZSIS handling of privileged communications and privileged information (December 2018)
    - A review of NZSIS requests made without warrants to financial service providers (December 2018, the "Banks report")
    - Warrants issued under the Intelligence and Security Act 2017 (December 2018)
- A progress report on our inquiry relating to the CIA's enhanced interrogation programme in Afghanistan, and progress reports and other procedural material relating to our Afghanistan Inquiry
- An account of information shared with the Royal Commission of Inquiry into the Attack on Christchurch Mosques
- Our 2018-19 work programme, with detailed notes to increase public understanding of the areas of agency activity under review
- Reports of the Inspector-General's meetings with the external Reference Group.

Some of the published reports arose from inquiries and reviews that were substantially completed in the previous reporting period and are summarised in last year's annual report.

Timeliness

Two major inquiries – into possible New Zealand engagement with CIA detention and interrogation between 2001 and 2009, and into what role, if any, the GCSB and the NZSIS had in relation to specific events in Afghanistan in 2019-2013 – required considerable resources from our team and from the agencies during the year. As a result, they have taken longer than anticipated to complete, with some impact on timeframes for other work (primarily operational reviews). With the CIA Inquiry complete, however, and the Afghanistan Inquiry due for completion towards the end of 2019, we anticipate being able to focus our resources more on operational reviews that can be completed in shorter timeframes.

Complaints received in 2018-19 have mostly been dealt with within a reasonably short time. Further detail on complaints is provided later in the report.

Impact

Effective oversight should have a discernible influence on the agencies' compliance systems and conduct. The work of the IGIS office in 2018-19 has had such an impact in several areas.

This has included, in particular, the approach taken by both agencies to applications for intelligence warrants. Our review of all warrants, and engagement with the agencies on what the law requires in warrant applications, has been more than usually intensive since the establishment of a new warranting regime under the ISA. The new legislation has raised issues about the quality of information required, analysis of necessity and proportionality, and the proper interpretation of key sections of the Act. Both agencies have substantially modified the structure and content of their warrant applications to address issues identified by the office of the Inspector-General and to comply

with advice from the Solicitor-General, sought by the agencies in response to legal questions we have raised. The process continues, particularly in relation to the overall approach taken by the Bureau to seeking authorisation of its activities.

We have also seen significant change to NZSIS' approach to the formulation of Business Records Approvals (issued under s 147 ISA) and to the use and recording of Business Records Directions issued subject to those Approvals (s 150 ISA). These are an important means by which the Service acquires personal information, often at the early stages of investigations, from providers of telecommunications and financial services about their customers. Similarly, our review of NZSIS requests made without warrants to financial service providers (the "Banks report") has had a clear impact on the Service's approach to seeking voluntary disclosure of personal information from banks.

Our inquiry into possible New Zealand engagement with the CIA detention and interrogation programme (discussed later in this report) prompted the development of comprehensive Crown legal advice, relevant across government, on the legal risks for New Zealand agencies cooperating with foreign partners in processes relevant to interrogation and detention. In consequence the Ministerial Policy Statement on cooperation of New Zealand intelligence and security agencies with overseas public authorities will be reconsidered.[4] The agencies are also reconsidering a number of consequently affected internal guidance and policy documents.

Meaningful acknowledgement and redress for complainants, when their complaints are upheld, is fundamental to the effective operation of our complaints jurisdiction. Where we reach the conclusion that redress is required we take care to develop recommendations for action by the relevant agency that are reasonable and practicable. To date all recommendations we have made in response to complaints have been accepted.

[4] The Ministerial Policy Statement is required by s 207 ISA. Section 209 requires the agencies to have regard to any relevant Ministerial Policy Statement in making any decision or taking any action.

KEY ISSUES IN 2018-19

It is especially important that the law and policy principles that govern intelligence agency activity and its oversight are accessible to the public and explained in a way that makes them understandable in their particular context. In New Zealand the relative lack of case law directly on point means that publication by the Inspector-General is one of the few routes to meet this public interest.

Numerous issues relating to the agencies' powers, their policies, the law, or the Inspector-General's powers and approach, arise and are discussed between our office and the agencies, in meetings and by correspondence, over the course of a year. This process of frank discussion, and at times vigorous debate, is necessary (especially in the absence of case law) to reach a robust position on what the law or propriety requires. This section summarises some of the more significant issues covered in our discussions during the reporting period.

When a Type 1 warrant is required

An issue signalled in our report "Warrants issued under the Intelligence and Security Act 2017" concerned an important and difficult question of statutory interpretation: is a Type 1 or a Type 2[5] warrant required when the agencies, in the context of targeting foreign communications, anticipate "incidentally" collecting New Zealanders' communications as well? For the agencies, the question has been answered with advice from the Solicitor-General, which they are bound to follow.[6] It is that a Type 1 warrant is not required. We maintain our view that a Type 1 warrant should be sought, as the process provides the extra protection of scrutiny by a Commissioner of Intelligence Warrants. We addressed the issue in more detail in an update on the Warrants report published shortly before this Annual Report. As the agencies are obliged to follow the Solicitor-General's advice, the focus of our discussions has shifted to the need to better identify, and as far as possible quantify, likely incidental collection of the communications of third parties when they seek a warrant. We are also emphasising the need for more robust information management processes after collection has occurred, eg governing the identification and destruction of unauthorised or irrelevant information.

NZSIS framework for obtaining voluntary disclosure of personal information

In our "Banks report"[7] we recommended that the NZSIS prioritise the development of a coherent framework giving staff clear, legally sound guidance on how to choose between the different information gathering mechanisms available to the Service: warranted powers; business records directions;[8] or requests for voluntary disclosure of information. The NZSIS has prepared a framework that in our view reflects all the relevant principles. More work, however, is needed to ensure that the framework can be applied to the full range of situations where the NZSIS seeks to obtain voluntary disclosure of personal information from third party agencies. Work is then required to embed that decision-making framework in the Service's operational policies and practices.

---

5 For a brief explanation of Type 1 and Type 2 warrants see the later "Warrants" section of this report.

6 The Solicitor-General's advice remains legally privileged.

7 A review of NZSIS requests made without warrants to financial service providers (December 2018, "Banks report").

8 Business records directions may be issued by the Service to telecommunications network operators or financial service providers to acquire information. See Subpart 4 of the ISA.

IGIS right of access to agency records and systems

Section 217 ISA states that the Inspector-General "must be given access to all security records … that the Inspector-General considers to be relevant to his or her functions or duties." In the course of our Afghanistan Inquiry it emerged that crucial records were held by the agencies in individual staff email accounts. We considered it necessary to search specified email files, which were not routinely accessible to us, and we wished to determine for ourselves the relevance of particular records. The agencies were reluctant to facilitate this, citing concerns that the files would contain private and personal communications of staff and considerable irrelevant material. We accepted that the motivation to protect staff privacy was genuine, but we were concerned that the mixing of personal and work related emails should not dictate IGIS access. The legal question is whether s 217 allows us unmediated access to all information storage systems in which security records might be held, or whether it is simply a right to be provided by the agencies with particular records from those systems on request. The Inspector-General expressed the view that s 217 must be interpreted to allow direct, unmediated access to all systems holding "security records" as defined in the ISA. Unless we saw a compelling legal opinion to the contrary, we expected this access to be provided. Ultimately, access to the staff email accounts proceeded on that basis.

The weight of the IGIS' view on the law

This issue, signalled in last year's Annual Report, concerns how the agencies ought to respond if the Inspector-General strongly questions the lawfulness of any current agency activity. Once a serious question of legality has been raised, the agencies agree it cannot be for them to determine whether their own activities are lawful. The Inspector-General reconfirmed to the agencies her approach: in the absence of relevant case law on the legality of particular agency activities, they should engage first with us on the merits of the issue. If they do not accept the Inspector-General's view (which they are not obliged to do), they must *promptly* seek advice from the Solicitor-General. The agencies are then bound to follow the Solicitor-General's advice. The IGIS, by contrast, is independent and not bound to adopt the Solicitor-General's view. The IGIS will not, however, say that the agencies are acting unlawfully if they act in compliance with the Solicitor-General's advice, which would provide sufficient basis for on-going activity of the relevant type. If, however, the Inspector-General expressed a firm view that an agency activity was unlawful and should cease, and the matter had not been referred to the Solicitor-General, the agency would be wise to suspend the activity until it has obtained legal advice.

The duty of candour in warrant applications

Issues arising from warrant reviews for the agencies have raised the question of the extent and nature of the information the agencies must disclose in a warrant application to satisfy the common law "duty of candour". The agencies agree that the duty applies, and our discussions concern what it means in practice. We have emphasised that the same duty of candour applies to the agencies as in any other context where a party, especially the state, seeks an *ex parte* warrant or decision (ie one sought and issued without the knowledge, participation or legal representation of the affected party). What information needs to be disclosed depends on the facts of the particular case, but the legal test is no different: the agencies must disclose to the Minister, and in the case of a Type 1 warrant, the Commissioner of Warrants, "all material facts" which bear on the issue of the warrant. To meet the

duty of candour the agencies need to think more broadly than the specific requirement in the ISA to, for instance, provide "details of the proposed activities". The duty requires them to set forth any matters of fact or law that, if brought to the attention of the decision-maker, might be material to whether the warrant should be issued, what may be done under it, and whether conditions should be imposed. An applicant must be careful not to decide themselves what the decision-maker "needs to know", and must bear in mind that a warrant is a prescriptive permission, not a high-level licence. That principle offers some measure of guidance on the detail that should be provided. The requirements of the duty of candour have arisen with the agencies in various contexts including:

- when it is appropriate for there to be conditions in a warrant
- the likelihood of intercepting privileged communications
- the role of parties assisting (under s 51 ISA) with the execution of a warrant
- where a known purpose in seeking the warrant is to share information with certain third parties
- where the agencies know there are limitations on their ability to minimise collection of incidental information or to control access to information after it has been shared with other agencies.

Agency retention and disposal of information

While designed to collect information relevant to the Government's intelligence requirements, intelligence activities can also result in the agencies acquiring private and personal information that is irrelevant to such requirements, or which loses its intelligence value over time. Sections 102-103 ISA are the primary provisions controlling how collected information is held, managed and destroyed. In short s 102 imposes a duty to destroy immediately any "unauthorised" information, unless a warrant is issued to authorise it retrospectively, while s 103 requires "irrelevant" information to be destroyed as soon as practicable. The agencies and the IGIS are agreed that, for s 102 to be effective, the scope of authorised activity must be clear from the combination of the application for the warrant and the warrant itself. The application of s 103 is more problematic, because judging when information collected for intelligence purposes is no longer relevant is not straightforward. If s 103 means that information may only be retained so long as it is necessary, rather than merely desirable, to keep it, that is still a difficult test to apply in practice. The practical effect of s 103 remains under discussion between our office and the agencies.

In common with other intelligence agencies and government departments, the Service and Bureau are having to manage rapid growth in the volumes of digital information they hold, while building and maintaining systems that can reliably store and manage files of multiple types. They increasingly need to be able to record the provenance of collected information in order to meet legal conditions on retention and destruction. Both agencies are developing information systems for this purpose, but still have considerable work ahead to put in place robust and reliable processes to give effect to their information management duties across the totality of their holdings. These processes must also be amenable to oversight.

Publication of agency position on the law

An issue raised a number of times this year, but not resolved, concerns the circumstances in which the Inspector-General may report the position of the Bureau or the Service on a matter of legal interpretation. Any agency information or advice that is legally privileged must not be disclosed by the IGIS, and we would not seek to do so unless the privilege was waived. That issue does not arise, however, in most circumstances where the Inspector-General would seek to discuss in a public report the agencies' formal position, as expressed to us, on what the law means for them. The fact that lawyers will generally have been involved, at some point, in assisting a Government agency reach its view does not make a factual statement of its approach to that issue a breach of the underlying legal privilege. The agencies have not asserted such a position but on occasion they have, in our view, come close to it.

The issue is important. If the agencies' position could not be disclosed, their understanding of how the law applies to them could never be publicly scrutinised. This would hamper what the IGIS could say publicly when exercising her legality jurisdiction, and would stymie public understanding and debate, and possibly even law reform. The interpretation of law, in the abstract, is not sensitive or classified; and public accessibility of the law governing the secret exercise of intrusive powers is a critical element in justifying the use of such powers.[9] By analogy, other Government agencies exercising intrusive or covert powers are routinely required to explain their interpretation publicly in submissions to the court, despite the fact their position has inevitably been informed, at some point, by legal advice. By contrast, examination by the court of intelligence agency activity is rare in New Zealand. We will keep this issue in our sights – claims of legal privilege should be kept within their strict legal confines. Statements of agency position may, however, be protected on appropriate occasion by understandings as to confidentiality, or in order to facilitate an effective relationship with oversight.

9 *Big Brother Watch and others v The United Kingdom* (58170/13, 62332/14 and 24960/15) Section I, ECHR 13 September 2018 at [306].

THE YEAR AHEAD

Compared to the past year, we anticipate spending a higher proportion of our time on short, focussed reviews of agency operational activity. In our view there is considerable benefit to the agencies and public confidence from prompt identification and timely reporting of operational issues. This may require a trade-off, on occasion, between resource-intensive investigations and an endeavour to follow a programme of shorter, smaller reviews covering a wider range of activities, including reviews carried out to achieve a baseline for more in-depth scrutiny in the future. That said, the discretion to investigate a topic exhaustively – by launching an own-motion inquiry if appropriate – will always be a necessary tool for the Inspector-General. The inquiries of that nature to date have been vital to our understanding of fundamentally important agency activities.

The work programme for the office for 2019-20, published on our website on 16 July 2019, describes the inquiries, reviews and other activities we expect to undertake or continue in the coming year. Briefly, these include:

- Our own-motion inquiry into the role of the GCSB and the NZSIS in relation to certain events in Afghanistan
- Consultation with, and contribution to, the Royal Commission of Inquiry into the Attack on Christchurch Mosques
- Reviews (some continuing or carried over from 2018-19) of:
    - GCSB conduct of operations to access information infrastructures, for the purpose of intelligence collection and analysis
    - a selection of operations under warrant involving the transfer by GCSB of raw data to partner data repositories
    - queries made by GCSB staff of partner data repositories
    - NZSIS's role in relation to recommendations concerning citizenship and immigration status applications
    - "open source" intelligence collection by both GCSB and NZSIS.

These reviews are additional to our routine review of all new intelligence warrants as they are issued; any new agreements entered by the agencies for direct access to public sector databases; business records approvals and directions; permissions to access restricted information; Human Rights Risk Assessments and Human Rights Risk Reviews; and selected assistance and cooperation agreements with foreign counterparts.

We will also continue to respond to complaints against the agencies, as they arise, while completing inquiries into complaints received during the past year that remain on foot.

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 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?

Inquiry into possible New Zealand engagement with CIA detention and interrogation 2001-2009 (concluded)

The former Inspector-General concluded the evidence gathering for this inquiry in the 2017-18 year, and before she left office in July 2019 she finalised both the classified and unclassified reports to the point where only minor matters needed attention. The unclassified report was published in September 2019.

Our inquiry followed the publication in December 2014 of the US Senate Committee on Intelligence's report of the Central Intelligence Agency's (CIA's) detention and interrogation programme, which involved torture and inhumane treatment of detainees in Afghanistan. Our report examines whether the New Zealand intelligence and security agencies knew about or were otherwise connected with, or risked connection to, the activities discussed in the Senate report. It finds that the NZSIS and GCSB had lines of connection to the CIA but were not complicit or otherwise involved in torture or ill-treatment of detainees. The report also examines whether the agencies' policies are adequate to safeguard against the risks of improper or unlawful behaviour when engaging cooperatively with partner countries.

The Inspector-General's recommendations include the need for the agencies to ensure that they have a clear mandate at ministerial level for activities with overseas partners that might engage legal or reputational risk to New Zealand. The agencies need to ensure that in supporting military deployments agency staff are adequately trained to identify in the particular context the relevant human rights obligations. While acknowledging that the statutory regime has changed and the agencies have improved the relevant training and support for staff, the report makes recommendations relating to the agencies' current suite of human rights policy and authorising mechanisms.

The report enhances the public accountability of the New Zealand agencies by adding significantly to the publicly available information about their activities, particularly about how they share information and cooperate with foreign partners and provide support to military operations.

Afghanistan Inquiry (current)

In March 2018 we commenced an inquiry into the role, if any, of the GCSB and the NZSIS in relation to specific events in Afghanistan in 2009-2013. Our preliminary inquiries, following the publication of the book *Hit and Run*,[10] indicated sufficient public interest to justify a focused own-motion inquiry. The intelligence agencies' role, if any, in events relating to Operation Burnham are within the scope of this inquiry, as is the agencies' response to human rights issues in Afghanistan in 2011-2013, including their response to the publication of certain official reports regarding the treatment of detainees.

Our inquiry is focussed on the knowledge and actions of the intelligence agencies and is not assessing the role and conduct of the New Zealand Defence Force. Some events and issues are inevitably common, however, to both our inquiry and the subsequently announced Government Inquiry into Operation Burnham. The Inspector-General entered into a memorandum of understanding with the Government Inquiry into Operation Burnham to align the scope of our respective Inquiries and to ensure there was a principled basis for any discussions between us. This has proved a useful relationship.

Progressing this inquiry has been a significant feature of our 2018-19 Work Programme and, as Deputy Inspector-General, I have had the privilege of leading that work. The evidence gathering has involved review of a very large volume of agency documents and records, including staff emails, as well as interviews with current and former staff from both agencies, including some who were present in Afghanistan at the time. Our inquiry continues as part of the 2019-20 Work Programme, with a view to completion of a classified report by December 2019, and with a public report to follow.

[10] Nicky Hager and Jon Stephenson *Hit and Run: The New Zealand SAS in Afghanistan and the meaning of honour* (Potton & Burton, Nelson, 2017).

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 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 each review we provide a report to the agency Director-General and, in significant matters, the responsible Minister. We publish a summary of the outcome of each review, either in the relevant annual report, or as a stand-alone document.

Review of a sample of NZSIS security clearance decisions

The NZSIS has a statutory mandate to conduct inquiries into whether particular individuals should be granted security clearances and to make appropriate recommendations based on those inquiries.[11] This review examined a proportion of adverse and qualified security clearance decisions over a specified period.

This review was completed by the Inspector-General in July 2019 and a report with findings and recommendations was provided to the Service. We noted the continued improvement in policy development and practice since 2015 as a result of our previous inquiries into specific complaints from those who had received adverse outcomes.

The review used the principles outlined in the IGIS's *Summary guide: Putting procedural fairness into practice in NZSIS security vetting*[12] to provide a framework for assessing the lawfulness and propriety of the Service's approach to these more complex clearance decisions, and the adequacy of its Vetting Policy and related procedures. The review evaluated how the relevant natural justice principles were applied across the cases selected for review. Overall, we found that NZSIS vetting staff were aware of the relevant principles and conscientious in seeking to apply them. We did not find any major deficiency in the security clearance processes reviewed. Six of the Inspector-General's seven recommendations were directed at modifications of practice and the remaining one recommended a notation be placed on a particular file for future reference to better ensure natural justice.

NZSIS relationships at the border

This review focused on NZSIS' operational interactions with other agencies, as they bear on the treatment of people crossing the New Zealand border. It found that NZSIS's compliance systems for its operations at the border are generally effective and appropriate. It did not discover any evidence of unlawful or improper activities by the Service at the border. The review found that the Service maintains functional working relationships with border agencies, although some memoranda of understanding (MOU) with other agencies about relationships at the border are missing or out of date. Some were already under review by NZSIS. The review recommended improvements to MOUs and engagement with the relevant agencies to develop or revise agreements where necessary.

---

11 ISA, 11 (3)(a)(i).

12 Published November 2016 and available on www.igis.govt.nz.

2018 report and 2019 update on review of warrants

In December 2018 we published a report on intelligence warrants issued in the first nine months of the ISA. That report drew on our regular review of all warrants issued to the agencies. It identified a range of issues that had arisen regarding the agencies' interpretation of the warrant provisions of the Act and the structure and content of their warrant applications and warrants, some of which they had remedied and some of which were unresolved at the time of publication. (The "Key issues" section of this report covers some of these matters). In late 2019 we published an update on progress. It noted some further improvements in the level of detail provided by both agencies in their warrant applications; progress in an ongoing dialogue with the Bureau about the breadth of purpose of some of its warrants; the resolution of the Crown's position on whether a Type 1 warrant is required when New Zealanders' communications will be acquired as collateral on interception undertaken for a foreign intelligence purpose;[13] and a brief account of some IGIS findings of irregularity in warrants and warranted activity. Over the relevant period we have seen significant willingness on the part of both agencies to make changes in response to the issues we have raised and substantial improvements in the quality of warrant documentation.

[13] See the discussion of this matter under "When a Type 1 warrant is required" in the "Key issues" section.

COMPLAINTS

In this reporting year the office received 26 complaints, as follows:

Complaints received 2018-19		
From	**Against GCSB**	**Against NZSIS**
Members of the public	9	17
Intelligence agency employees or former employees	0	0
Total	9	17

Any New Zealand person 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.[14] 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.[15] The scope for public reporting on complaint investigations is accordingly limited.

Not all complaints require a formal inquiry. As is typical elsewhere, a substantial proportion of the complaints received in the reporting year were from members of the public expressing concern that one or both of the agencies had them under surveillance, or were using some kind of weapon against them. Complaints in this category lacked evidential foundation and were not capable of being upheld.

Some approaches to our office, expressed as complaints, are more accurately understood as requests for personal information under the Privacy Act 1993 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 Inspector-General if the response is unsatisfactory.

The most common subject of complaints that require more in-depth 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. Two vetting complaints received during the reporting year required substantive inquiries that were completed before year end. One was not upheld and one resulted in a recommendation for a partial re-assessment. An inquiry into a vetting complaint received during 2017-18 was completed. The complaint was not upheld, but the inquiry prompted a recommendation that the NZSIS take steps to improve its procedures for ensuring irrelevant and potentially adverse information does not taint decision-making on clearance recommendations.

---

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

[15] ISA ss 176(1) and 185(5).

Inquiries into two other complaints received in 2017-18 were completed in the past year. One, alleging unlawful and/or improper intelligence activity by both agencies against the complainant, was not upheld. The other, alleging various improper actions by NZSIS in relation to an individual could not be resolved on the basis of preliminary inquiries. We determined, however, that a more extensive inquiry would not necessarily provide the best, or any, remedy for the complainant's concerns. With the cooperation of the Service the matter was resolved to the complainant's satisfaction by further contact between the parties.

Two complaints were received during the reporting year regarding the NZSIS' relationship with the private security firm Thompson and Clark Investigations Ltd (TCIL). In substance the complaints asked whether the Service had cooperated with TCIL in a way that was unlawful and improper. The office investigated the concerns. What we found was consistent with the findings of the State Services Commission (SSC) investigation into the use of TCIL's services by Government agencies, insofar as that related to the Service.[16] We advised the complainants accordingly. In short, the SSC investigation found no evidence that NZSIS directly engaged TCIL, but found some communications between a Service officer and TCIL were inconsistent with the public service Code of Conduct.

Resolution of final classified and unclassified reports on one complaint received late in 2017-18, concerning whether the NZSIS had a proper statutory basis for undertaking alleged action against the complainant, was still in progress at the end of 2018-19.

[16] Doug Martin and Simon Mount QC "Inquiry into the use of external security consultants by Government agencies" (State Services Commission, 18 December 2018).

WARRANTS

In this reporting year the office reviewed 61 warrants issued to the agencies, as follows:

Warrants reviewed 2018-19					
	Type 1	Type 2	Practice	Removal	Total
NZSIS	23[17]	2	3	1	29
GCSB	18[18]	15	0	0	33
Total	41	17	3	1	61

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.[19] 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.

In the year under review one urgent Type 1 warrant was issued to NZSIS and one very urgent authorisation (for activity requiring a Type 1 warrant) was issued by the Director-General of GCSB. Each was the first of its type under the ISA. Both were confirmed by subsequent written applications.[20]

Under s 163 ISA the Inspector-General may conclude, from a review, that a warrant, or activity carried out under a warrant, is "irregular".[21] 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,[22] but the Inspector-General may recommend that all or any specified information obtained is destroyed.[23] During the year under review the Inspector-General found one Bureau warrant to be irregular[24] and activity under an NZSIS warrant to be irregular. The office also advised NZSIS that one of its warrants appeared to be irregular, which prompted the Service to correct an error.[25] Further information is available in our 2019 update on warrants, noted earlier in this report.

---

17 Including one urgent warrant.

18 Two warrants were revoked and reissued during the period. Each reissued warrant is counted in the total.

19 A New Zealander is a New Zealand citizen or permanent resident.

20 An urgent warrant can be issued in response to an oral rather than written application and is revoked automatically after 48 hours unless the agency follows up with a written application. A very urgent authorisation can be issued by the Director-General of an agency and is revoked automatically after 24 hours unless a written application is made. See ISA ss 71-82.

21 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.

22 ISA s 163.

23 ISA s 163(3).

24 The GCSB warrant was revoked, at the Bureau's request, between the Inspector-General's preliminary and final findings that it was irregular.

25 The prompt and willing correction of the error by NZSIS mean there was no final finding that the warrant was irregular.

CERTIFICATION OF COMPLIANCE SYSTEMS

Our approach to certifying soundness

The Inspector-General must certify in each annual report "the extent to which each agency's compliance systems are sound."[26] Certifying the extent to which the agencies' systems are sound is not certification that every specific activity of the agencies was lawful and proper. Rather, it is directed at assessing the agencies' organisational approaches to minimising the risk of illegality and impropriety. The question of the extent of soundness recognises that some aspects of the agencies' compliance framework may be stronger than others.

In assessing soundness we consider the extent to which the agencies are enabled to identify correctly the standards their conduct must meet; and whether these standards are reflected in adequate processes, training and guidance for operational activity. We look at whether the agencies expose breaches through effective audit and other oversight mechanisms; and whether those breaches are addressed, both in the particular instance and in so far as they may disclose systemic shortcomings.[27] We look across the agencies' activities and:

- examine what specific compliance systems and controls are in place, such as relevant policies, safeguards and audit/oversight/error-reporting measures;
- draw upon our ongoing operational review work to pay attention to a particular sample of each agency's activities;[28] and
- apply a materiality threshold to errors or other shortcomings. (We are interested in the substance and materiality of shortcomings, rather than matters of mere form or minor "one-offs").

In recent years the practice has been to state an overall conclusion on whether each agency has sound compliance procedures and systems in place. That has the virtue of simplicity. It has the disadvantage, however, of requiring a blunt choice to be made and putting the focus on the overarching conclusion rather than on the detail. The law, however, does not require such a choice, and this statutory function can also be met by assessing the extent to which certain aspects of the compliance systems are sound. That recognises the range of factors at play and the fact that, at any one time, an agency is likely to be stronger in some respects and weaker in others. For this report I again state an overall conclusion, but this will not necessarily continue. In the coming year we intend to explore the possibility of moving to a 'dashboard' type assessment of strengths and weaknesses across a defined set of parameters.

Compliance strengths

In my assessment, the compliance systems of both agencies are sound to the extent that:

---

[26] ISA s 222(2)(c).

[27] See, among others, Department of Internal Affairs *Achieving Compliance: A Guide for Compliance Agencies in New Zealand* (2011) 25ff.

[28] Oversight can never be in the position where it has applied recent scrutiny to all agency activities.

- They approach compliance on the basis that compliance obligations are an integral part of all operational activity and must be naturally built into the way staff do their work.
- They foster a culture of self-reporting of compliance issues and, when mistakes are made, generally seek to learn from them.
- They have dedicated and effective stand-alone compliance teams. These teams see themselves as "enablers" of staff activity. They work especially closely with the agencies' in-house legal teams and management to identify and respond to areas of operational risk.
- The compliance teams have annual programmes of planned audits into aspects of their agencies' activities. Completed audits provide an evidence-based picture of staff compliance.
- The compliance teams are consistent, and generally prompt, in reporting to the Inspector-General any incidents they have identified as raising non-compliance with policy or law. They will subsequently investigate and prepare a report, usually with recommendations.
- The compliance teams are responsive to the Inspector-General and are open to investigating concerns expressed by the IGIS. With the support of their legal team they will consider non-compliance questions we raise.
- Both agencies put considerable focus on staff training. As part of their compliance arrangements they have put resources into the specialist design of accessible and operationally bespoke training modules. Core training topics, such as a module on human rights law, are compulsory for all staff across both agencies.
- Led by the compliance teams, both agencies have an extensive and generally robust suite of policies and guidance documents.
- Agency arrangements for scheduled and unscheduled discussions and meetings with our office, and for the delivery of briefings to our staff, are generally sound and cooperative. Staff across both agencies are willing to explain their work and answer our questions.

Other factors

While the systems and processes described above for ensuring compliance in the agencies are appropriate and generally embedded, there are areas of activity where those systems do not reach or are not as effective as they should be. This occurs where the compliance standards themselves, against which the legality and propriety of activity should be measured, are uncertain within the agency or the Inspector-General has raised a doubt about them. Examples might be where a Standard Operating Procedure or policy is not drafted or inadequate, or where an authoritative statement of the rules governing an area of activity has not been prepared, or where there is persistent uncertainty or dispute about where the line for legal conduct should be drawn. The timely response of the agencies to resolving such uncertainty is essential if the Inspector-General is to be confident their systems are legally compliant.

There have been on-going transitional issues arising from the enactment of the ISA, especially concerning matters of legal interpretation. Even once an interpretation issue or the scope of an obligation is settled, which can take many months, there is often a lag while internal arrangements

and guidance are put in place to give effect to it. More timely and better resourced responses to these issues remain areas for improvement for both agencies.

The agencies take their responsibilities to oversight seriously and generally seek to respond in a constructive and timely way to the demands placed on them by the Inspector-General. In the past year both agencies' legal teams, which take primary responsibility for interactions with our office, have improved in this regard, and the Service's legal team has made a particular effort to engage with us early and, on occasion, proactively. In respect of both agencies overall, however, there are exceptions, and some relate to especially significant matters. Examples are noted below in the discussion of each agency's compliance.

We have advised both agencies that work is overdue in establishing, across their information holdings, processes which give effect to obligations around the retention and management of collected personal information. Specifically, the agencies need to develop reliable and auditable processes for the on-going relevance testing of collected personal data, and for destruction if it is not relevant. This is a difficult, multi-year task but the agencies recognise it as a priority. So too is the agencies' substantive response to the recommendations made in our recent "CIA" report concerning changes to various authorisations and policies which bear on human rights protections.

There were unanticipated pressures on the NZSIS and GCSB in 2018-19 arising from the attack on the Christchurch mosques, the subsequent Royal Commission of Inquiry, the government Inquiry into Operation Burnham and the State Services Commission investigation into government agency dealings with the private security firm Thompson and Clark. Nonetheless, the Inspector-General found it necessary to emphasise to both agencies that responding to the demands of oversight needs to be a systemic and integral part of the agencies' own operations, and resourced as such. There are always unanticipated pressures and competing demands on government agency resources. They cannot be allowed to let oversight requirements be set aside, when the law clearly positions oversight as a fundamental discipline on the agencies' activities.[29] It is important that the agencies are *consistently* responsive to the requirements of oversight and that standard is not yet met.

GCSB

Overall, more timely response to the needs and requests of oversight and earlier completion of its own internal compliance investigations should remain a particular focus for the Bureau.

The GCSB's legal team put significant effort in 2018-19 into clearing a longstanding backlog of our warrant queries. Resolution of our queries bears on the Bureau's overall compliance, in that our review and question process often results in clarification and agreement about standards and specific matters that need to be addressed in future warrants. With respect to more recent reviews the GCSB is generally now responding to our questions and comments within a couple of months, which is a distinct improvement, and it permits our warrant reviews to be more effective and efficient. On some key matters, however, the Bureau's response has been unjustifiably delayed. In particular, and of most

[29] The purpose of the ISA includes "ensuring that the functions of the intelligence and security agencies are performed … in a manner that facilitates effective democratic oversight" (s 3) and both agencies have a corresponding duty to facilitate effective oversight (s 17).

concern, while beginning to make important changes to its warrant applications as a result of our discussions, the Bureau took nine months to respond to a letter from the Inspector-General raising fundamental issues about its approach to warrants for some major components of its intelligence activities.[30] The issues were difficult and will require on-going discussions, but a quicker response is imperative when there are significant legal issues at stake regarding extant warrants.

In the year under review the Inspector-General found one Bureau warrant to be irregular for lack of sufficient operational detail and reached a preliminary view that another was irregular for deficiency of information on one of the activities for which authorisation was sought.[31] In both cases these findings were based on a view that the Bureau had incorrectly assessed the requirements of the law. They did not reflect any disregard for those requirements or unwillingness to comply. I do not consider therefore that these findings weigh significantly against the overall soundness of the Bureau's compliance systems. The issues with one of the warrants in particular reflected genuinely challenging questions of interpretation arising under the new legislation.

Our Afghanistan inquiry required substantial work by GCSB to retrieve many historic records, including entire repositories, and make them capable of access. While these efforts contributed reassurance and useful material to our fact-finding process, we were at times frustrated by a failure to promptly facilitate our access to relevant documents and systems. An issue about our right to access historic staff email repositories, in particular, was noted earlier (in the 'key issues' section of this report). The combination of the Bureau's initial reluctance with respect to email access, and the genuine technological challenges it faced, set our inquiry's progress back some time. Additionally, the Inspector-General was compelled to write to the Bureau at one point, requiring better cooperation.

The functions of the Bureau's Compliance and Policy team include internal auditing. Auditors within operational teams are required to audit 10 per cent of all queries that staff make of databases of intercepted communications data. The audit involves confirming the information was collected lawfully under a specific warrant, and ensuring that the justification for access is appropriate. Every week, the Compliance and Policy team does what it calls a "super audit," examining 10 per cent of the audited 10 per cent. The Bureau's stated aim is to ensure that the audit process serves as a learning tool for operational staff and allows systemic shortcomings to be addressed. In addition, pursuant to an Audit Plan the Bureau conducts audits of specific areas of operational activity. The Bureau did not achieve everything on the 2018-19 Audit Plan but it did complete three audits and shared the resulting reports with the Inspector-General. This process gives us an opportunity to assess if there is some aspect we wish to look into further. The completed audits reviewed different areas of Bureau operations and their compliance with relevant authorisations and warrants.

The GCSB has resourced itself with two dedicated operational policy advisor positions. This will give it the capacity to amend and write new policy in a timely fashion, which will help it deal with matters such as the development of better internal processes for the on-going relevance testing of collected personal data, as noted above.

In this reporting year there were 13 self-reported incidents notified to our office by the Compliance and Policy team which became aware of them through either self-reporting by Bureau staff or partner

[30] See our report "ISA warrants – update".

[31] Further detail on these warrants and the meaning of irregularity is in the earlier 'Warrants' section of this report.

agency audit. As at 30 June 2019 investigations into seven of these have been completed, and 16 historical (pre-July 2018) compliance investigations and six historical compliance "surveys" remained open.

Overall, I certify that the GCSB has sound compliance procedures and systems in place.

NZSIS

For the Service the mosque attacks on 15 March led to a period of unprecedented pressure on almost all staff across the agency. This included the NZSIS legal team, with whom we interact regularly for oversight purposes. Despite the pressure, the legal team managed to maintain its regular scheduled meetings with our office. It generally managed to respond to questions arising from our regular reviews of warrants within days of us raising them, which was impressive. This year the Service has exhibited a determination to raise issues or new activities early with the Inspector-General where it anticipates we will have questions. It has been willing to talk things through with us, at the level of principle, and to make appropriate changes to its approach as a consequence.

Outside the context of our warrant reviews there were some undue delays. In particular, in response to a formal recommendation from the Inspector-General it took the Service almost 12 months to prepare a coherent framework of principles to differentiate between, and govern its use of, the different information collection mechanisms in the ISA. This work is fundamental to ensuring the Service makes appropriate choices between the lawful collection mechanisms available to it. While the framework is now done, consequential work to embed it in policies and training has yet to be completed.

Like the Bureau, the Service made considerable efforts to retrieve records for our Afghanistan inquiry. It was also, however, at times unduly slow to provide access to information. As with the Bureau it was initially reluctant to facilitate our right to access historic staff email repositories, as discussed in the 'key issues' section of this report.

In the past year the Inspector-General determined that activity under one of the Service's warrants was irregular, in that the degree and context of the privacy intrusion was of a wholly different order from what the application for the warrant contemplated. The Service disagreed. Subsequently we advised the Service that another of its warrants appeared to be irregular, in response to which the Service acknowledged and corrected a mistake.[32] As with the findings of irregularity in relation to Bureau warrants noted above, we do not consider that the issues with these warrants reflected any serious disregard for the requirements of the law or any unwillingness to comply. In respect of the first warrant the Service genuinely, if mistakenly in our view, believed its activity was within the scope of the warrant. In the case of the second warrant it promptly recognised and dealt with an error.

For the Compliance and Risk team the operational demands on other staff meant some of its planned work programme this reporting year was delayed, including planned audits of certain holdings. The Compliance and Risk team put its focus on developing improved training modules, particularly in respect of the most important training topics which are compulsory for all staff.

[32] Further detail on these warrants and the meaning of irregularity is in the earlier 'Warrants' section of this report.

The Service has direct access to information held on three external agency databases.[33] This year it received a very poor audit report on its compliance in 2017-18 with the conditions on its access to the CusMod database, the primary operational database of the New Zealand Customs Service. Where adequate records were kept of NZSIS access to CusMod they showed appropriate use, but the audit found that just over a third of NZSIS's numerous searches of CusMod during the audit period were incorrectly recorded in the NZSIS register or not recorded at all. While the audit results were concerning, the Service's response was appropriate. It firmly reiterated to staff the importance of keeping full records of access; reviewed the relevant processes and tools supporting CusMod access; and arranged for further staff training. It engaged frankly with the Inspector-General and the Office of the Privacy Commissioner on the audit and its remedial actions. A follow-up "light audit" of further CusMod access showed significant improvement in recording of access to the database.

A total of 11 self-reported compliance incidents were notified to us by the NZSIS this year. All incidents were notified soon after they were identified. Incidents notified within the first half of the year were investigated and reported on by NZSIS and resolved to the Inspector-General's satisfaction by year end. Investigations of incidents notified in the second half of the year were in most cases well advanced by the end of the reporting period. The Service's completed investigations of self-identified compliance incidents were thorough, reasonably timely and recommended appropriate remedial action where necessary.

Overall, I certify that the NZSIS has sound compliance procedures and systems in place.

[33] Direct access is enabled under s 125 ISA. The Service has entered agreements for direct access to the New Zealand Customs Service's 'CusMod' database; the Advance Passenger Processing (APP) database managed by Immigration New Zealand; and the Births, Deaths and Marriages database administered by the Registrar-General. The agreements are public documents, available on the NZSIS website.

OUTREACH AND ENGAGEMENT

Summarised below are some of the engagements we have been part of this year. The Inspector-General also appeared before the Intelligence and Security Committee to discuss her 2017-18 Annual Report, and we both participated in a wide range of public speaking events.

Meetings with foreign oversight counterparts

The Five Eyes Intelligence Oversight and Review Council (FIORC) comprises the non-political intelligence oversight and review bodies from the UK, USA, Canada, Australia and New Zealand. One of its purposes is to encourage transparency to the largest extent possible and to enhance public trust. This year we met in Canberra, hosted by the Australian Inspector-General, Margaret Stone. Key topics of discussion were the maintenance of the independence (actual and perceived) of oversight bodies, and how oversight bodies can acquire or access specialist technological expertise.

We attended the International Intelligence Oversight Forum (IIOF) in late 2018. The meeting is an initiative of the UN Special Rapporteur on the right to privacy, Professor Joseph Cannataci, who also chairs it. The Special Rapporteur's mandate arose from the international concern that followed the Snowden leaks in 2013. The IIOF was attended by representatives from many countries, mainly European. Major themes were the implications of two landmark judgments of the European Court of Human Rights in 2018 concerning bulk collection of personal information; the means to secure independence for oversight bodies; the limitations on domestic oversight bodies once information is shared by intelligence agencies with foreign counterparts; and the need for appropriate technological training of oversight bodies and the issuers of intelligence warrants. The Inspector-General delivered a paper on forms of cooperation and engagement that support the effectiveness of oversight bodies.

Statutory Advisory Panel

The primary role of the Advisory Panel is to provide advice to the Inspector-General.[34] 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 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 the Inspector-General and I met with the Panel seven times. In particular, the Panel offered detailed comments on specific issues arising from our draft reports, and from our draft Work Programme for the 2019-20 year.

Reference Group

Material relating to the Inspector-General's Reference Group, including the membership and summaries of our discussions, are on our website. We met twice this year. The Group has no access to classified or otherwise sensitive information, nor is that necessary for it to fill a useful function.

[34] ISA s 168.

It is well recognised internationally that best practice for oversight involves ensuring there are sufficient means for the oversight body to understand the scope of community views on issues relevant to intelligence agency oversight. It is important that oversight does not speak solely with specific interest groups or communities, eg the intelligence community, lawyers, or politicians. All of our Five Eyes counterparts, and many of our European colleagues, have developed "outreach" programmes, which involve multiple points of connection to community representatives. To varying degrees these initiatives include commentators, journalists, academics, civil liberties representatives, and critics. The Reference Group assists to keep us in touch with legal, social and security developments in New Zealand and overseas, and provides a thoughtful view on what it is most useful for an oversight body to communicate to the New Zealand public.

Canadian secondment

In August 2018 a senior staff member of Canada's Security Intelligence Review Committee, the oversight body for the Canadian Security Intelligence Service, commenced a one-year secondment with us. The secondee boosted our small team from 8 people to 9, and made a distinct contribution to our work. The arrangement itself was novel. We know of no other oversight bodies that have had secondments from foreign counterparts. It required the New Zealand agencies (which themselves regularly second staff from their foreign counterparts) to support it, which they did admirably. The secondment has set a precedent, and its value is already sought to be replicated elsewhere. Given the isolated nature of oversight work, it is hugely valuable to have a person in the team who can draw on a directly relevant foreign point of reference on matters of law or the conduct of the agencies' operational activities.

Other Integrity Agencies

The Inspector-General maintained her involvement in the scheduled meetings of the Intelligence and Security Oversight Coordination Group, with the Privacy Commissioner, the Chief Ombudsman and the Auditor-General. In addition to discussions on subjects of shared interest, the meetings develop relationships of mutual support, coordination and cooperation between integrity agencies. This helps each agency maintain its independence and effectiveness.

As Deputy Inspector-General I attended in April a meeting of representatives from New Zealand integrity agencies hosted by the Chief Human Rights Commissioner, Paul Hunt. The occasion for the meeting was the visit to New Zealand of Kate Gilmore, the United Nations Deputy Human Rights Commissioner, in the wake of the events in Christchurch of 15 March 2019. Ms Gilmore stressed the need to maintain a common focus on human rights in times of national stress. There is obvious value in independent agencies of this type coming together to identify themes in common and to learn who is doing similar or related work.

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 Inspector-General of Intelligence and Security), as part of the Ministry of Justice's non Departmental appropriations.

The independence, effectiveness and reach of oversight bodies is dependent on adequate funding. The budget for the permanent staff of OIGIS extends to approximately eight people: the Inspector-General and Deputy Inspector-General, three or four investigators, an office manager/executive assistant and an IT manager/security advisor. If the office is to grow in proportion to the growth in the intelligence agencies, and OIGIS is to have the capacity to review the breadth of their activities on a timely schedule, there will need to be additional funding. We sought and received an increase in budget for 2019-2020, but with the office's planned shift in October 2019 to permanent premises, that budget increase will go almost entirely to increased rent.

2018-19 budget and actual expenditure

Total expenditure for 2018-2019 was $1.470 million, as follows:

Office of the Inspector-General of Intelligence and Security 2018-19 Budget		
	Actual ($000s)	***Budget***
Staff salaries; advisory panel fees; travel	760	*798*
Premises rental and associated services	39	*42*
Other expenses	36	*37*
Non-Departmental Other Expenses (PLA)	635	*636*
Total	**1470**	***1513***

Administrative support

The New Zealand Defence Force provides IT support to the office, for some of our systems, 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. Inspector-General Gwyn and I have been especially grateful for the assistance provided to us this year by key personnel in the Ministry of Justice's finance 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