Office of the Inspector-General of Intelligence and Security

Annual Report

For the year ended 30 June 2017

Cheryl Gwyn
Inspector-General of Intelligence and Security
1 December 2017

Contents

OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

1 December 2017

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

Dear Prime Minister

Annual Report 2017-2018

I **enclose** my annual report for the period 1 July 2016 – 30 June 2017.

You are required, as soon as practicable, to present a copy of the report to the House of Representatives (s 222(3) of the 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.

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.

You are also required to provide the Leader of the Opposition with a copy of the report (s 222(5) of the Act).

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

With your concurrence, and in accordance with s 222(8) of the Act, I confirm my availability to discuss the contents of my report with the Intelligence and Security Committee, should the Committee request my attendance.

Yours sincerely

C.M.G. Gwyn

Cheryl Gwyn
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) 817 0402

FOREWORD

My primary focus this year was on completing inquiries and reviews initiated in the previous period and consolidating a regular programme of review of agency operational activities.

My office also devoted a lot of attention to the New Zealand Intelligence and Security Bill.[1] I made oral and written submissions to the Foreign Affairs, Defence and Trade Committee.[2] My interest was in whether the legislation fully and clearly spelled out the powers of the intelligence and security agencies, the purpose of those powers and the controls on them; included necessary accountability and oversight mechanisms; and whether the legislation was generally consistent with fundamental rights and freedoms.

I was particularly interested also in the new provisions under which intelligence warrants are sought and issued and other mechanisms designed to give effect to certain powers in the Act. The legislation introduced "Direct Access Agreements" which permit an intelligence and security agency to obtain information from certain public sector databases, and Ministerial Policy Statements which govern how the intelligence and security agencies should undertake various generally lawful activities. My office contributed a great deal to the development of these new mechanisms for guiding agency activity, which became a substantial part of the year's work programme.

Our work was substantially disrupted by the November 2016 Kaikoura earthquake. Because of the requirement that we work in a "secure compartmented information facility", or SCIF, we were not fully operational for three or four months after the earthquake. Since then we have made good progress on completing outstanding work, although we continued to operate in constrained circumstances for the whole of the reporting year and beyond.

Shortly after the end of the reporting year the first Deputy Inspector-General, Ben Keith, completed his three year term and commenced practice as a barrister in Wellington. During his term Ben made a significant contribution to establishing the office as the properly resourced, independent and rigorous oversight body envisaged by Parliament when it enacted amendments to the Inspector-General of Intelligence and Security Act 1996 in late 2013. Ben's particular expertise in human rights law was especially valuable to our analysis of many agency activities.

The new Deputy Inspector-General, Madeleine Laracy, joined the office in September 2017.

I am pleased to have been reappointed as Inspector-General by the Prime Minister in May 2017, for a further three year term.

---

1 Now enacted as the Intelligence and Security Act 2017 (IS Act).

2 www.igis.govt.nz/legislation/

ROLE OF THE INSPECTOR-GENERAL

This reporting year under the IGIS Act

The Inspector-General oversees the two intelligence and security agencies, the New Zealand Security Intelligence Service (NZSIS or the Service) and the Government Communications Security Bureau (GCSB or the Bureau). I refer to them at times in this report simply as the agency or the agencies.

The Inspector-General's statutory role[3] during this review period has been to assist the Minister responsible for each of the agencies to ensure that their activities comply with the law.

The IGIS Act authorised regular inspections of the agencies to assess their procedures and compliance systems and, ideally, to identify issues before remedial action becomes necessary. The programme for general oversight and review of each intelligence and security agency was submitted by the Inspector-General for the Minister's approval.

The inspection role of the Inspector-General is complemented by an inquiry function. I have, and where necessary use, strong investigative powers akin to those of a Royal commission, including the power to compel persons to answer questions and produce documents and to take sworn evidence.

I can also inquire into complaints by members of the public, or employees and former employees of an intelligence and security agency, that the person has been adversely affected by any act, omission, practice, policy or procedure of an agency. I am obliged to independently investigate those complaints.

In order to carry out these functions I have a right of access to all security records[4] held by the agencies and a right of access to the agencies' premises,[5] including the Bureau's two communications interception stations: the high frequency radio interception and direction-finding station at Tangimoana and the satellite communications interception station at Waihopai.

My role is primarily after the fact – that is, after particular operations have concluded, or at least commenced – which is the most common method of intelligence oversight. The underlying rationale is that oversight bodies should review, but not direct or approve in advance, the management and operational decisions of intelligence services. This approach does not preclude the agencies briefing me on planned or ongoing operations. Although it is not my role to approve operations in advance, or to advise the agencies, there are situations where prior discussion with my office can help to ensure clarity about the legality and propriety of any planned activity, as well as making subsequent review more straightforward and effective.

---

3 Inspector-General of Intelligence and Security Act 1996 (IGIS Act), ss 4(a) and 11. The IGIS Act was the governing Act for the current reporting year. Under the IS Act, which substantially took effect from 28 September 2017, the Inspector-General's functions are set out in s 158.

4 IGIS Act, ss 2 and 20.

5 IGIS Act, s 21.

I can address the activities of only the NZSIS and the GCSB. I cannot inquire into the exercise of intelligence and security functions of any other agency, or receive any complaints about them.[6]

Changes to the Inspector-General's role under the IS Act

The Intelligence and Security Act (IS Act) does not change the Inspector-General's role in any material respect. It underscores the independence of the Office from executive government. Under the IGIS Act, the Inspector-General was responsible for "assisting" the Minister to ensure that the NZSIS and the GCSB are acting lawfully and properly. The Minister had a role in "approving" the Office's work programme.

Under the IS Act the role is described as:

- to ensure the agencies conduct their activities lawfully and with propriety
- to ensure complaints relating to the agencies are independently investigated
- to advise the New Zealand Government and the Intelligence and Security Committee on matters relating to oversight of the agencies

This change reflects the reality of my Office's operation under the IGIS Act: as a statutory officeholder I was not (and am not) subject to general direction by any Minister on how my responsibilities under the legislation should be carried out. The Minister in charge of the NZSIS and responsible for the GCSB was informed about the Office's proposed work programme and was able to make suggestions about it, but did not in practice "consent" to it.

The general role of advising the Government and the ISC is new and may encompass, for example, advising on any new legislation relevant to intelligence and security.[7]

In addition, my office will now have oversight obligations that correspond to the new functions, powers and obligations that the IS Act provides for the agencies, such as having regard to Ministerial Policy Statements when carrying out their activities; accessing information held by other agencies; and obtaining business records of telecommunications network operators and financial service providers.

Amendments to the Protected Disclosures Act 2000, made by the IS Act, provide for an expanded role for the Inspector-General.[8]

---

[6] The National Assessments Bureau (part of the Department of the Prime Minister and Cabinet) provides intelligence assessments explaining political and economic developments overseas, environmental, scientific, security and strategic issues and biographical reporting.
The New Zealand Defence Force includes a Directorate of Defence Intelligence, a geospatial intelligence section and individual service intelligence capabilities.
Immigration New Zealand, the New Zealand Customs Service and the New Zealand Police have intelligence units.

[7] Both Australia and United Kingdom have separate appointees who carry out this function.

[8] See more detail at page 21 below.

HOW EFFECTIVE IS OUR OVERSIGHT?

Purpose of oversight

External purpose

The intelligence and security agencies have lawful authority (if an intelligence warrant is issued) to do a whole range of things which, if carried out by any other citizen, would constitute criminal offences. For example, they have legal authority to covertly access computers, intercept phones and mail, break into people's homes to plant listening devices or cameras, and exchange highly personal or other information with domestic and foreign intelligence and security and law enforcement agencies.[9]

At the same time the secrecy of NZSIS and GCSB's activities, capabilities, and techniques inevitably makes it much more difficult for Parliament, the news media and the public at large to hold them to account as they can with other parts of the government or the public sector. This in turn can have a significant impact on the level of trust and understanding the public has in the value, role and effectiveness of the agencies.

In those circumstances external, independent and effective oversight is vital. That oversight function can only be exercised by people permitted to access the secret (classified) information the agencies gather, and to know the means by which they gather it. In New Zealand, apart from the Minister responsible for the agencies, the Prime Minister and a small handful of senior public servants, that external access is limited to the Commissioners of Intelligence Warrants (retired High Court Judges who, together with the Minister, have a role in authorising intelligence warrants) and the Office of the Inspector-General of Intelligence and Security.

Members of the public must be able to trust in the independence and integrity of the Inspector-General and his or her staff. The existence and public work of my office provides a form of indirect public view into the agencies themselves.

Internal purpose

Effective, independent oversight should also assist agency application of the law and, over time, minimise the risk of any illegality or impropriety in agency operations. It is important that the agencies, just like any other public bodies, operate according to best practice standards and in such a way as to give full effect to the New Zealand government's domestic and international obligations, especially human rights standards. Effective oversight is intended to support the agencies in this process, while at the same time being consistent with their operational objectives.

Key requirements for effective oversight

As I noted in last year's Annual Report there are some factors that are essential to effective oversight which can give confidence to the public. Those requirements are:

[9] See eg IS Act, ss 67, 68 & 69.

- *Independence:* from the intelligence agencies themselves and from the executive, is essential. The Inspector-General is an independent statutory officer, organisationally separate from the NZSIS and GCSB and (unlike US intelligence community Inspectors-General) there is no reporting line to the agencies. The office is at arms-length from the executive. The IGIS is not subject to general direction from the responsible Minister, the Prime Minister or other Ministers, on how the Inspector-General's responsibilities under the IGIS Act (and now the IS Act) should be carried out

- *Access:* total, unmediated access to *all* security information held by the intelligence and security agencies is essential for effective oversight. Generally, accessing material involves a process of consultation and discussion with agency staff, but ultimately it must be for the Inspector-General, rather than the agency Director-General, to decide what information the Inspector-General should see. That right was protected by the IGIS Act and continues under the IS Act.[10] Giving full effect to it requires the agencies to be adequately resourced and organised to respond to the oversight requirements in a timely way. In turn, the effectiveness of my office depends in large part on the timeliness with which I can obtain information and secure informative and reasoned responses from the agencies. The right of access is facilitated where there is a culture of openness to oversight within the organisation. I recognise that in practice that requires the agencies to trust that I will listen carefully to what they say and bring an informed perspective and a sense of fairness to the relationship

- *Resources:* sufficient, appropriate resources are essential. Currently the OIGIS comprises the Inspector-General, the Deputy Inspector-General, four Investigators, an Office Manager/Executive Assistant and an IT Manager/Security Advisor. The resources, while modest, have to date been adequate to carry out the office's review, inquiry and complaints work, but with the enactment of the IS Act I anticipate our resources will be stretched

- *Own-motion jurisdiction and investigative powers:* the complaints and review work are the bread and butter of the Inspector-General's work, but the ability to initiate an inquiry into the legality or propriety of agency activities, where that is in the public interest, and without the need for government request or concurrence, is vital for the independence and perception of independence of the office. That ability is enshrined in the legislation[11]

- *Mandatory public reporting:* annually and of specific inquiries, is an important aspect of effective oversight and of public accountability of the overseer. Public reporting is required by the IS Act[12] and the Inspector-General may publish the Office's annual work programme.[13] My approach has been to enhance transparency by publishing my reports or summaries of them even when I am not required to by law, and to encourage the agencies themselves to put as much material as possible in the public domain.

---

10 IGIS Act, s 20(1); IS Act, s 217.
11 IGIS Act, s 11 (1); IS Act, s 158.
12 IGIS Act, ss 25A and 27(6A); IS Act, s 188.
13 IS Act, s 159(3)(b).

Increased oversight means increased demand on the agencies

As I have noted previously, one effect of the expanded mandate and corresponding increase in resources for the Inspector-General's office is to place more demands and some strain on the agencies which must respond. I signalled in last year's annual report my expectation that, given increased funding, the agencies would this year be able to better manage the demands placed on them by systematic oversight and review, and to do so in a timely and efficient way.

While the agencies have developed a more systematic approach to responding to OIGIS requests for information, in this reporting year their resources were heavily committed to the legislative reform process, while having to carry on business as usual, with the unfortunate consequence that response times have again been slowed.

Measures of effectiveness

In the 2014/15 annual report I noted that the effectiveness of the Inspector-General's office can be assessed against four key measures:

- the breadth and depth of inspection and review work
- the time taken to complete inquiries and resolve complaints
- the extent to which the agencies, Ministers and complainants accept and act on the Inspector-General's findings and recommendations
- the extent to which there is a change to the agencies' conduct, practices, policies and procedures as a result of the work of the Inspector-General's office

Breadth and depth of inspection and review work

Our experience has been that there is considerable value in having a range of functions (review, inquiry, complaints) across both intelligence and security agencies. Information and insights obtained in carrying out one function frequently inform another. For example, investigation of specific complaints made by individuals has provided a detailed insight into general operational issues and systemic problems, and I have been able to take up those general or systemic issues under my wider functions.[14] Questions or issues that arise in respect of one agency may inform our approach in respect of the other agency.

My office's most regular engagement with the agencies arises from our review of all intelligence and interception warrants and access authorisations. My staff meet on a monthly basis with the legal teams from each of the agencies to discuss any questions about the warrant documentation. These discussions have led to steady, incremental changes in the type and volume of information included

[14] For example, individual complaints concerning NZSIS security clearance assessments led to the identification of a recurrent question of whether the procedures followed by NZSIS in making its assessments and recommendations were consistent with the legal obligation of procedural fairness: see Annual Report for Y/E 30 June 2015, at pp 15-18, www.igis.govt.nz/publications/annual-reports/. I have found that our regular warrant review process is valuable for identifying systemic issues which can themselves justify a wider review. For example, the review concerning privileged information arose from a warrant review.

in a warrant application for the Minister (and sometimes the Commissioner of Security Warrants) to consider.

Time taken to complete inquiries and resolve complaints

All of the complaints received during 2016/17 were completed within a maximum period of four months.[15]

As I noted in last year's annual report, I initiated a relatively large number of reviews and inquiries in the preceding year. All of those were, in my view, important and necessary, but the volume of work involved, together with the small size of the office, has resulted in undesirable delays in completing some reports. For some projects this was compounded by loss of staff members as we transitioned from an office staffed by individuals on secondment from various government agencies to permanent staff.

I acknowledge that inquiries must be completed within a reasonable period, for a number of reasons:

- if the matter is in the public interest, the public should know the answer to the questions posed as soon as possible
- likewise, the agency under scrutiny is entitled to have any issues about its performance evaluated and reported without undue delay, and
- to the extent the results of inquiries might lead to improvements in operational practices, improvements should happen sooner rather than later.

While it is not possible to have a hard and fast rule, our objective is to complete inquiries and reviews within a period of six to 12 months, depending on the nature and scope of the particular matter.

Equally, in hindsight, I recognise these early inquiries and reviews also involved a lot of groundwork, providing the foundation for familiarity with the agencies' operations. This has stood us in good stead for later work.

Discussions with the affected agency to arrive at an unclassified report of each inquiry for publication also adds to the time taken to complete and publish a report. I must ensure that any report does not disclose information that would prejudice the security and defence interests set out in the legislation.[16] What happens in practice is that the agency concerned may request the removal or redaction of material in a report if its publication would damage their work, for example by revealing their targets, methods, sources or operational capabilities. Other government agencies may also have a direct interest in ensuring that a report does not prejudice their statutory interests. For example, in the case of the inquiry into the GCSB's process for determining its foreign intelligence activity, I consulted with the Ministry of Foreign Affairs and Trade because my report had the potential to prejudice New Zealand's international relations.

[15] See more detailed statistics in the complaints section of this report.
[16] IGIS Act, s 25A; IS Act, s 188.

I consider requests for removal or redaction of material carefully. The agency must demonstrate clearly how publication of the material in question would be damaging before I agree to removal. My aim is to ensure that material is removed only where essential and that the unclassified, public report provides the necessary information for members of the public to understand the nature and circumstances of the incident or practice that I have reviewed and my conclusions and recommendations.

We are now in a position to complete the two outstanding inquiries (Inquiry into complaints regarding allegations of GCSB surveillance in the South Pacific; Inquiry into possible New Zealand engagement with CIA detention and interrogation) in a timely way. Two other longstanding matters (Inquiry into NZSIS warnings; Review of information collected under Customs and Excise Act and Immigration Act) are close to completion, and will be published before the end of 2017.

Extent to which agencies, Ministers and complainants accept and act on the Inspector-General's findings and recommendations

In this reporting year the NZSIS has continued to implement the recommendations contained in part one of my review of the holding and use of, and access to, information collected for security vetting purposes. It also accepted the recommendations contained in part two of that report, and has made strong progress in implementing most of them.

The Bureau has accepted all recommendations contained in the inquiry report into the GCSB's processes for determining its foreign intelligence activity and the review report on Agents of a Foreign Power.[17]

Extent to which there is a change to the agencies' conduct, practices, policies and procedures as a result of the work of the Inspector-General's office

The Directors-General of both agencies have publicly acknowledged the impact of OIGIS scrutiny, at the level of detailed investigations on specific operations or warrants and also at a systems level. The Director-General of Security has referred to this as "the IGIS on my shoulder" effect.[18]

One specific area where we have identified a change to agency conduct is in relation to intelligence and interception warrants and authorisations. My staff meets monthly with the legal teams of each agency to discuss new warrants and authorisations that we have reviewed in the preceding month. The discussions generally focus on the applications for warrants submitted by the agency to the Minister (and where required the Commissioner of Security Warrants, now the Chief Commissioner of Intelligence Warrants). As a result of those discussions the applications submitted by both agencies have incrementally developed to include more information to assist the decision-maker in deciding whether the warrant sought is necessary and proportionate, and to address more squarely the conditions to which the warrant should be subject.

[17] See summaries at pp 12 and 13.

[18] Rebecca Kitteridge, Director of Security: *Protecting New Zealand as a Free, Open and Democratic Society: The Role of the NZSIS*, Victoria University of Wellington Public Office Holders Lecture Series, 3 June 2016.

I have continued to give presentations to new and existing staff of the agencies (two presentations in this reporting year) to help raise awareness of my role and the oversight and accountability framework generally.

Change is effected both through direct engagement with the agencies and through interaction with other bodies and with the public. For example, regular appearances before the Intelligence and Security Committee to discuss my office's annual reports help to keep the legislature appraised of intelligence and security issues from an oversight perspective and provide an opportunity for the members to ask questions about the work of my office.

Our interviews with Sir Michael Cullen and Dame Patsy Reddy as they conducted the First Independent Review of Intelligence and Security in New Zealand,[19] and subsequent in-person and written submissions to the Foreign Affairs and Defence Select Committee when it was considering the New Zealand Intelligence and Security Bill, provided an invaluable opportunity for my office to influence the development of the legislation governing the intelligence agencies.

Statutory advisory panel

The terms of appointment of the first members of the Inspector-General's advisory panel, Christopher Hodson QC and Angela Foulkes, were completed in October 2016. I am grateful for the support Mr Hodson and Ms Foulkes provided me and the breadth of experience, intellectual rigour and judgement they brought to the role.

The office of Inspector-General is in some respects an unusual and isolated role. It is valuable to have access to the independent perspective offered by the panel members. Unfortunately no new appointments have been made since October 2016.

Intelligence and Security Committee

The ISC may consider and discuss with the Inspector-General his or her annual report as presented by the Prime Minister to the House of Representatives.[20] The Inspector-General may, with the concurrence of the Prime Minister, report either generally or in respect of any particular matter to the ISC.[21] At the ISC's invitation I attended before it at a private hearing on 9 November 2016 to discuss my 2015/16 annual report.

[19] www.parliament.nz/en/pb/papers-presented/current-papers/documents/51DBHOH_PAP68536_1/report-of-the-first-independent-review-of-intelligence/ (the Cullen and Reddy report).

[20] IGIS Act, s 27; IS Act, s 61F.

[21] IGIS Act, s 27(7).

THE YEAR AHEAD

Work programme

The IGIS Act required me to prepare a programme of work for general oversight and review of the two agencies I oversee. [22] The bulk of the work programme is directed at the functions specified in the IGIS Act.[23]

The IGIS Act[24] required me to submit the work programme to the Minister responsible for each of the agencies[25] for approval. The IS Act will require consultation with the responsible Ministers on a draft work programme, at least 60 days before the beginning of each financial year.

In the course of the reporting year I made public the office's detailed programme of work: www.igis.govt.nz/publications/igis-work-programme/**.** My approach is to provide as much information as possible to the public about the work of my office, to promote a better understanding of what the intelligence and security agencies do and ensure that I am accountable to the public in my oversight role.

As the IS Act is implemented there will inevitably be questions for the agencies and the Inspector-General's office about what certain provisions mean and require, or allow for, in practice. I will need to reserve sufficient resource and time to deal with the unanticipated questions raised by the new Act, as well as overseeing the new functions, powers and obligations that the IS Act provides for the agencies, such as having regard to Ministerial Policy Statements when carrying out their activities; accessing information held by other agencies; and obtaining business records of telecommunications network operators and financial service providers.

The Outer Space and High-altitude Activities Act 2017 established a new responsibility for the Inspector-General. Under the Act, the Prime Minister may issue a certificate that activity or proposed activity regulated by the Act would pose a significant risk to national security. The effect of the certificate is to prevent the specific activity occurring. If a certificate is issued by the Prime Minister, the person affected by the certificate can make a complaint to the Inspector-General in accordance with the complaint procedures under the Intelligence and Security Act 2017.[26] The Inspector-General may send a report to the Minister responsible for the NZSIS or the GCSB as relevant, and if the Inspector-General does send a report, the Prime Minister may withdraw or confirm the certificate.

In the coming year I also intend to have a more systematic focus on engaging with the public (see p 34 for this year's activities).

---

22 IGIS Act, s 11(1)(e).
23 IGIS Act, s 11(1)(a)-(da).
24 IGIS Act, s 11(1)(e).
25 For the reporting period, the Hon Christopher Finlayson QC, who was both the Minister in charge of the NZSIS and the Minister responsible for the GCSB.
26 Section 56.

INQUIRY AND REVIEW POWERS

Inquiries

The Inspector-General can inquire into GCSB and NZSIS compliance with the law and into the propriety of particular agency activities.[27] Propriety is not defined in the legislation, but it goes beyond specific questions of legality; for example, whether the agency acted in a way that a fully informed and objective observer would consider appropriate and justifiable in the particular circumstances.[28] The Minister and Prime Minister may request that I undertake an inquiry, or I may initiate an inquiry of my own volition.

The factors I consider when deciding whether I will initiate an inquiry include:

- 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?

In the context of an inquiry the Inspector-General can use strong investigative powers akin to a Royal commission, such as the power to compel persons to answer questions and produce documents and to take sworn evidence. I also have a statutory obligation to publish a report on every inquiry I undertake.

Operational reviews

Reviews of operational activity form part of my office's regular programme of review of agency compliance systems.[29] While in rare cases a review might prompt a more formal inquiry, in general reviews are less formal and are aimed at strengthening agency practice and legal compliance. At the end of each review I provide a report to the agency Director-General and, in significant matters, the responsible Minister. I publish a summary of the outcome of each review, either in the relevant annual report, or as a stand-alone document.

---

27 IGIS Act, s 11(1)(a) and (ca); IS Act, s 158(1)(d).

28 For instance, in my pending report on how the NZSIS deals with privileged information, I have made comments about the best practice, as I see it, when undertaking activity which is not carried out under an intelligence warrant. Similarly, my office's input into the development of the Ministerial Policy Statements addressed questions of propriety as much as legality.

29 IGIS Act, s 11(1)(d)(ii); IS Act, s 158(1)(f).

INQUIRIES AND REVIEWS CONCLUDED IN 2016/17

Inquiry into NZSIS's applications for sensitive and complex warrants

This inquiry, initiated by the previous Inspector-General, concerned the lawfulness and propriety of a significant category of warrant applications made by the NZSIS. I formed the view that public disclosure of the particular operational detail of those warrant applications (which were made in 2014) would cause harm to national security, but I gave an account of my inquiry, the problems identified and the changes made in response, in my inquiry report of November 2016: www.igis.govt.nz/publications/investigation-reports/.

In short, my preliminary conclusions were that this category of warrants did fall within the lawful scope of the NZSIS's powers and it was consistent with propriety for the NZSIS to seek warrants of this kind. I found, however, that there were deficiencies in the warrant applications: they did not set out for the authorising Minister all material and available information relevant to the benefits and risks of the proposed activities or how those activities met the requirements of the New Zealand Security Intelligence Services Act 1969;[30] and they did not demonstrate how those activities were primarily directed towards the statutory purposes of the Act, as distinct from other, ancillary purposes.

As I noted in my 2015-2016 annual report, the NZSIS had accepted my provisional findings and recommendations and agreed to implement them in future warrant applications. My inquiry report was concluded after I had the opportunity to review subsequent warrant applications of the same kind. As a result of that review I concluded that the NZSIS had effectively implemented the recommendations and the subsequent applications met the requirements to disclose all relevant information and set out how the NZSIS believed the criteria for issue were met in each particular case.

Inquiry into the GCSB's process for determining its foreign intelligence activity

I commenced this inquiry as a result of issues raised by the public about claims of GCSB assistance to the New Zealand Government's campaign to advance the Hon Tim Groser, then Minister of Trade, as a candidate for Director-General of the World Trade Organisation.

My report (www.igis.govt.nz/publications/investigation-reports/) found that the GCSB acted lawfully and properly within its statutory mandate and in accordance with the New Zealand government's foreign policy decision to support Mr Groser as a candidate. I did not express a view on whether, as a matter of policy, contributing to New Zealand's economic well-being was a proper statutory objective for the GCSB: that was a question for Parliament and had been considered in the Cullen & Reddy review and the Parliamentary consideration of the IS Act.

I recommended three modifications to GCSB's current practice where a GCSB customer makes a request for foreign intelligence assistance. These modifications should ensure requests are always clear, documented, and come within the New Zealand Government's foreign intelligence requirements. The Director-General accepted those recommendations and the modified practice is to be audited as part of the GCSB's 2017-2018 audit plan.

[30] New Zealand Security Intelligence Service Act 1969 (NZSIS Act), s 4(1)(bc).

The active role and support of the GCSB's Director-General ensured that this report marked a step forward in the degree of information about GCSB activities that I was able to publicly report on.

Review of NZSIS holding and use of, and access to, information collected for security vetting purposes

I commenced this review in January 2015 and my report on part one, concerning the use of security vetting information and physical holding of that information, was released on 7 April 2016.[31] The second part of the report, dealing with the security of electronic record-keeping systems, was concluded and published in May 2017.[32]

In the second report I addressed whether the four NZSIS electronic record-keeping systems used for security clearance information met New Zealand Government requirements for the storage of national security information and, if not, the extent to which such information had or may have been compromised or was at risk of compromise. I also considered whether logging of user access to electronic records was able to indicate any unauthorised access.

I found that that the electronic record-keeping systems used by NZSIS now comply with mandatory Government standards but that all four systems used for security clearance information were non-compliant for several years, until a corrective programme began in mid-2015.

I recommended that the NZSIS follow certain steps to avoid the possibility of any new systems being brought into operation without first ensuring their compliance. I made recommendations to address potential vulnerabilities in the agency's systems and to improve the internal controls on data access.

The Director-General of Security accepted all recommendations and as at the date of this report the Service has made strong progress in implementing the recommendations.

Determinations of "Agents of a Foreign Power"

I reviewed the GCSB's system for determining whether the private communications of a particular New Zealand citizen or permanent resident could be lawfully intercepted on the basis that the person is an 'agent of a foreign power'. Under the Government Communications Security Bureau Act 2003 the Bureau was prohibited from intercepting the communications of a New Zealander unless the person was acting as an agent or a representative of a foreign person or any foreign government, body or organisation.[33] The Bureau had internal policy and procedure to guide a decision about whether a New Zealander proposed as a target for interception could be regarded as an agent. This would have to be established to the Director's satisfaction before an interception warrant was sought. The process would also be applied retrospectively if new information indicated that a person whose communications had been intercepted under warrant was or might be a New Zealand citizen or permanent resident, when that was not known earlier.

We found that despite some shortcomings in policies, procedure and record-keeping, the Bureau's system generally resulted in robust decisions on whether a person could reasonably be regarded as

---

31 www.igis.govt.nz/publications/investigation-reports/

32 www.igis.govt.nz/publications/investigation-reports/

33 This prohibition was removed by the IS Act, with effect from 28 September 2017.

an agent of a foreign power. I examined records relating to 19 decisions dating between 2013 and 2016. Although the recorded justifications for some were more thorough than others I did not find any I considered indefensible. Retrospective decisions were rare. I made minor recommendations for improvement to the Bureau's system, which it has undertaken to act upon. My findings will also be relevant to the design of new systems for compliance with the nationality requirements of the IS Act. This is not a matter where I felt there was the need for any more extensive reporting than appears here.

ONGOING INQUIRIES AND REVIEWS

Inquiry into warnings given by NZSIS officers

I commenced this inquiry, about the giving of warnings by NZSIS officers to members of the public, in June 2014. The practice of giving warnings exposes a very fine line between, on the one hand, NZSIS officers legitimately attempting to influence behaviour and, on the other, improper attempts to enforce certain behaviour, or appearing to do so. The matters canvassed in the inquiry have been the subject of extensive discussion with the NZSIS in the intervening period. A classified report has been completed and provided to the Director-General of Security for final comment. I anticipate I will be able to complete the report and provide a copy to the Minister responsible for the NZSIS shortly, and after that release it to the public by the end of 2017.

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

In December 2014 the US Senate Committee on Intelligence published redacted findings, a conclusion, and executive summary of its report on the CIA's detention and interrogation programme. This report documented instances of torture and inhumane treatment of detainees in the period between 17 September 2001 and 22 January 2009.

My inquiry is into whether New Zealand's intelligence agencies knew or were otherwise connected with, or risked connection to, the activities discussed in the US Senate report. Although the report was prompted by historical events, the central questions about New Zealand's legal obligations in relation to torture, and how the intelligence and security agencies guard against the risk of unlawful behaviour, including the risk of complicity in torture carried out by the agency of some other country, remain current and significant.

The change in administration in the United States and other international developments highlighted the importance for the New Zealand intelligence and security agencies to have adequate safeguards in place now to prevent possible complicity in unlawful activity in the course of cooperating with both traditional and non-traditional partners.[34]

With that in mind, I brought forward the third aspect of the inquiry: an examination of what policies and guidance have been developed and implemented by the NZSIS and GCSB, and are in place now, to ensure that their staff comply with New Zealand's domestic law and international obligations when cooperating with other nations. My staff undertook a comprehensive review of current agency policies and also looked at how partner intelligence agencies have tried to ensure compliance with international legal obligations in this area. This analysis, together with a review of current New Zealand and international law, was presented to the agencies as a "discussion paper" in April 2017. As at publication of this annual report I am waiting for a full response from the agencies to the paper. It will ultimately form part of my final report on this inquiry. This work has also informed my office's

[34] Both during the election campaign and shortly after becoming President, Donald Trump made statements supportive of the use of torture. Also this year, the Supreme Court of the United Kingdom ruled that civil action could proceed against government agencies and individuals who, the plaintiffs claimed, assisted the CIA in its rendition and detention programme: *Belhaj & Anor v Straw & Ors, Rahmatullah v MOD & Anor* [2017] UKSC 3.

comments, at the drafting stage, on the Ministerial Policy Statement *Cooperation of New Zealand intelligence and security agencies (GCSB and NZSIS) with overseas public authorities.*

I anticipate reporting publicly on this inquiry in 2018.

Inquiry into complaints regarding alleged GCSB surveillance in the South Pacific

This inquiry stemmed from a number of complaints that individuals may have been adversely affected by alleged GCSB surveillance in the South Pacific. I have also examined under my general review power the broader context of those complaints, including what activities GCSB carries out, and subject to what protections.

I anticipate that, following consultation with affected parties, I will be able to complete this report in the first half of 2018.

Review of access to information collected under the Customs and Excise Act 1996 and the Immigration Act 2009

In both my 2015 and 2016 Annual Reports I noted that my office had been in discussion with the NZSIS over its access to information collected by Customs and Immigration respectively under the Customs and Excise Act 1996 and the Immigration Act 2009. The objective of those discussions was to ensure that there is a clear and properly regulated regime for any such access. I concluded a report in May 2016 in which I identified a number of issues requiring a response from NZSIS. I also recommended it seek legal advice.

My conclusion in that report was that the NZSIS unlawfully obtained Customs data up until mid 2016. I acknowledge that it took the Service considerable time to obtain legal advice on all of the issues that this matter raised, and that it was also legitimate for it to revisit or update earlier advice based on various legal developments. That in part explains the excessive timeframe involved in completing this report. However, other factors were involved too.

It was difficult to elicit a comprehensive and fully reasoned response from the NZSIS to my May 2016 report or ancillary correspondence. I found the agency was reluctant to engage with my office on the substantive issues. I also observe that while the Service is entitled to have a different view from me on the lawfulness of given activities, whenever lawfulness is in question it should be proactive in obtaining independent legal advice on the specific point. Ultimately in this matter the Service advised me of its final view as to the lawfulness of some of its access to information under the Customs and Excise Act as late as August 2017. On that I have a different view, as set out in the review report.

I have not been able to satisfactorily resolve with the Service the residual question whether NZSIS can lawfully treat immigration information collected by it previously as if it had been collected under the Direct Access Agreement with Immigration that is now in place (see below).

Overall, this is an unsatisfactory position. I reiterate the view I expressed in last year's annual report – to ensure it operates lawfully, the NZSIS must be able to deal with such issues in a much more timely way.

For the future, a right of direct access for NZSIS to the particular information collected under these Acts is provided for by the IS Act.[35] Under the Act's provisions Direct Access Agreements between the Minister in charge of the NZSIS and each of the Minister of Customs and the Minister of Immigration are now in force.

In the course of discussions with the Service about these issues the Service expressed some reluctance about disclosing its own internal legal advice on certain matters central to my investigation. This was contrary to the clear words of the legislation,[36] and longstanding practice, and impeded my ability to understand fully the operational situation at the particular time. As I set out earlier in this annual report, it is for the overseer to identify the information needed for effective oversight, not the agency in question. Historically legal opinions have been provided by both agencies to my office with the understanding that solicitor/client privilege is not waived by doing so. It is essential, in order to oversee the agencies' compliance with the law, for the OIGIS to know how the law is being interpreted and applied by the agency.

I intend to publish a report on this matter before the end of 2017.

Review of activity undertaken under s 8C GCSB Act

I had proposed to review all requests under s 8C of the Government Communications Security Bureau Act 2003[37] for advice and assistance received by GCSB in the 2015/16 financial year. Section 8C relates to cooperation between the Bureau and the New Zealand Police, New Zealand Defence Force, and NZSIS respectively. We had not started this review as at the end of the reporting year.

Review of NZSIS collection of data from financial services providers without warrant

The intelligence and security agencies have historically requested some information from telecommunications providers, financial services providers and utility companies outside the warrant regimes in the NZSIS Act and the GCSB Act. The agency to whom the request is made decides on a voluntary basis whether or not to provide the information sought. The review focuses on customer information provided by banks to NZSIS within a defined period. Given the extent of the information that is sought and provided without a warrant, and the special duty of confidentiality that attaches to bank client records, I examined the NZSIS request process to ensure that access mechanisms used are lawful and proportionate. I expect that this review will inform agency practice under the new statutory regime for obtaining business records of telecommunications network operators and financial services providers. In particular, it should clarify the limited range of information that can properly be sought by NZSIS from banks on a voluntary basis.

As at publication of this annual report a draft review report had been provided to the NZSIS for comment. I expect to finalise the report in early 2018.

---

35 IS Act, ss 124-133, which came into force on 1 April 2017: see s 2(1)(e).

36 IGIS Act, s 20; IS Act, s 217.

37 Government Communications Security Bureau Act 2003 (GCSB Act).

Review of the existing New Zealand security classification system

As part of the New Zealand Intelligence Community's broader Personnel Security (PERSEC) review, my office has undertaken a discrete review of the current New Zealand security classification system which operates across government to identify official information that needs special management to avoid risks that would arise if it was freely accessible. The system protects such information by controlling access to it, through a combination of protective markings, associated rules and procedures (eg handling requirements and rules restricting access to security-cleared personnel) and physical or technical barriers (eg locked storage, encryption).

Our review has looked at the system and its operation to identify changes that could be made to improve security, reduce costs and increase transparency.

As at publication of this annual report a draft review report has been provided to the NZSIS and the Department of the Prime Minister and Cabinet for comment and discussion.

Review of a sample of NZSIS recommendations in respect of citizenship and immigration

One of the NZSIS's statutory functions[38] is to make recommendations to the Department of Internal Affairs under the Citizenship Act 1977, and to Immigration New Zealand under the Immigration Act 2009, to the extent there are matters relevant to security. The terms of reference for this review are to select and review a sample of those recommendations, for the period 1 July 2015 to 31 December 2016.

The review includes identifying and considering the relevant statutory and policy frameworks (including relevant MOU and SOP) which govern these functions. The effect of the IS Act will also be noted. To date our focus has been on collecting the requisite data and information on the operational context, in order to select an appropriate sample. That aspect of the review has now been completed. I hope to have a draft report ready by June 2018.

Review of NZSIS treatment of privileged material

The NZSIS Act prohibits the NZSIS from seeking to intercept or seize privileged communications under intelligence warrants. The NZSIS Act protects legal, religious and medical privilege. The purpose of this review is to assess the effectiveness and appropriateness of the NZSIS's policies, procedures and practices in identifying and handling privileged communications, from the application for a warrant through to its execution, and including controls around inadvertent interceptions.

A draft report of this review was provided to the NZSIS in June 2017 to ensure factual accuracy and for discussion of any issues arising. I expect to complete that discussion, including how privileged material is to be dealt with in joint NZSIS/GCSB policy to be developed under the IS Act, and finalise my report by the end of 2017. I plan to publish a summary of the legal issues considered.

[38] NZSIS Act, s 4(1)(bc).

Review of selected 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.[39] This review will examine a specified number or proportion of adverse and qualified security clearance decisions over a specified period.

We had not started this review as at the end of the reporting year.

[39] NZSIS Act, s 4(1)(bb); IS Act, s 11 (3)(a)(i).

COMPLAINTS HANDLED BY THE OIGIS IN 2016/17

Any employee or former employee of the GCSB or NZSIS (although generally they have to exhaust any internal complaints procedures before the Inspector-General has jurisdiction) or any New Zealand person may complain to my office that they have or may have been adversely affected by an act, omission, practice, policy or procedure of the GCSB or NZSIS.

In many cases complaints or inquiries can be dealt with quickly and efficiently at an administrative level without the need for formal inquiry, which requires notification of the complainant's details to the Director of the agency complained about.

Complaints by agency and source	**GCSB**	**NZSIS**
Number of complaints	**1**	**5**
From members of the public	1	5
From intelligence agency employees or former employees	0	0

Description of the complaints and inquiries

One complainant was unhappy about what the complainant considered to be a blanket response from GCSB about information which it might hold on the complainant. I referred the matter to the Privacy Commissioner because it more clearly fell within his jurisdiction.

Three complainants were concerned that they were under surveillance by the NZSIS. In each case, at my request, the NZSIS confirmed to the complainant that it held no information about him or her. I was able to independently verify the correctness of those assurances.

Another inquiry, which I did not ultimately accept as a formal complaint, related to a concern that the complainant's mail had been intercepted by the NZSIS and/or one of its Five Eyes partners. A search of relevant records by my office indicated that there had been no national security activity of the kind suspected by the complainant.

The sixth complainant sought acknowledgement from the NZSIS of the complainant's previous status in a foreign organisation. I decided that the complaint was not within my jurisdiction.

The time taken to deal with those matters that were accepted and investigated as formal complaints ranged from 11 days to four months.

Privacy Act complaints

See the inquiry referred to above which was referred to the Privacy Commissioner.

Telecommunications (Interception Capability and Security) Act 2013 (TICSA) complaints

No complaints in relation to the TICSA were received by the Inspector-General during this reporting period.

Protected Disclosures Act 2000 and whistleblower policies

No protected disclosures were received by the Inspector-General during this reporting period.

Under the Protected Disclosures Act 2000 the Inspector-General is designated as the only appropriate authority to whom employees (both current and former) of the NZSIS and GCSB may disclose information about potential wrongdoing in a 'whistleblower' sense. Employees of both agencies may seek advice and guidance from the Inspector-General about making a protected disclosure, before doing so.

As well as the protections offered by the Protected Disclosures Act 2000, the IGIS Act also provides protections for any employee, bringing any matter (not just "serious wrongdoing") to the attention of the Inspector-General, against any penalty or discriminatory treatment by the employing agency for doing so, unless the Inspector-General determines that the employee was not acting in good faith in bringing the matter to his or her attention. The IS Act continues this protection.

The IS Act also extends the role of the Inspector-General in receiving protected disclosures. The Inspector-General is designated as the appropriate authority to receive protected disclosures about classified information, or information relating to the activities of the NZSIS or GCSB, from employees of public sector organisations which hold such information.

My office has developed a policy and guidance about making disclosures, which addresses how protected disclosures are to be handled by IGIS staff, taking into account the changes in the IS Act. The policy and guidance is published on the Office of the Inspector-General's website: www.igis.govt.nz/publications/igis-policies/ I have also written directly to the heads of public sector agencies, that deal with classified information, providing a copy of this material and offering support in the development of their own internal guidance.

LEGISLATIVE DEVELOPMENT AND IMPLEMENTATION

As noted above, my office had extensive involvement in the process of fine-tuning the New Zealand Intelligence and Security Bill[40] and developing and giving effect to new mechanisms under the legislation. I made oral as well as detailed written submissions to the Foreign Affairs, Defence and Trade Committee.[41]

While most substantive provisions of the IS Act took effect as of 28 September 2017, a few came into force on 1 April 2017. They included the provisions which allow an intelligence and security agency to have direct access to databases storing specified public sector information. We provided substantial comment on the draft direct access agreements between the Minister in charge of the New Zealand Security Intelligence Service and the Ministers of Customs and Immigration respectively.

We were consulted on the development of all Ministerial Policy Statements[42] which were introduced in response to a recommendation in the Cullen and Reddy report. The report identified the absence of an authorising system for activities which are "not generally unlawful" as one of the three significant problems in the previous legislation[43] and recommended[44] that there should be a comprehensive authorisation regime for both agencies. The reviewers contemplated some form of authorisation for all of the agencies' intelligence collection and protective security activities that involve gathering information about individuals and organisations. They recommended the regime cover activities that are permitted under the general law and do not require an intelligence or interception warrant. It is intended that Ministerial statements of this kind will help to ensure that there is clear and objective guidance for how the agencies are to carry out their lawful activities and a greater level of oversight and accountability for agency activity previously conducted without any form of external authorisation.[45] As noted elsewhere, my office's contributions to the above activities became, in hindsight, a significant part of this year's work programme.

40 Now enacted as the IS Act.
41 www.igis.govt.nz/legislation/
42 Provided for in Part 7 of the IS Act.
43 At para 6.66.
44 At para 6.27.
45 At para 6.66.

WARRANTS AND AUTHORISATIONS

Government Communications Security Bureau

Register of warrants and authorisations

The Bureau is required to keep a register of all interception warrants and access authorisations.[46] The register must contain specified information which includes the purpose of the warrant/authorisation and its duration; whose communications may be intercepted and/or at what place; who is authorised to make the interception or obtain access; and whether any other person or body is requested by the Bureau to assist in giving effect to the warrant or authorisation.[47]

The Director-General must make the register available to the Minister or the Inspector-General when requested and if a warrant relates to the interception of communications of a New Zealand citizen or permanent resident, the Director-General must notify the Inspector-General as soon as possible after the information is entered in the register.

In accordance with that requirement, the Bureau maintains a register, which is available for review by my office and which we cross-check with our own review of warrants and authorisations.[48]

We have reviewed all 26 interception warrants in force in the reporting year and all 27 access authorisations issued under s 15A of the GCSB Act during the year.

During the course of the year's regular discussions with the Bureau's legal team about warrants and authorisations, we raised questions about a range of matters including:

- what controls the Bureau has over data collected and then shared with partner agencies
- GCSB's policy for dealing with possible New Zealand victims of cyber crime, where that issue arises in the context of the Bureau's information assurance and cyber security role
- how data retention periods are determined in relation to specific warrants
- what assessment is made of the risk of collecting privileged communications under certain warrants and how the risk is managed
- in the case of an operation undertaken jointly with the NZSIS, seeking clarification around which activity was undertaken by which agency and under what authorising instrument.

We have asked many other questions, and have found the Bureau open and willing in the way it engages with my office and me on these matters. At the same time, there have been delays in receiving substantive answers to some particular warrant questions, extending even to queries we have made in previous reporting years. The GSCB is aware of my concern at this delay, which has itself been a

[46] GCSB Act, s 19.
[47] GCSB Act, s 15E.
[48] See above, p 29.

matter for regular mention, and is committed to clearing the backlog in the 2017 calendar year and responding more promptly to future queries.

Director's authorisations

In addition to Ministerial interception warrants and access authorisations, the Director of the GCSB had power to sign an interception authority for the purposes of the Bureau's information assurance/cyber security and intelligence gathering functions, provided that the act is authorised by the GCSB Act or another enactment and does not involve physically connecting an interception device to any part of an information infrastructure or installing an interception device in a place.[49] That provision applied, for example, to carrying out permitted interception of non-New Zealand communications by high frequency radio signals by ships or other radio operators, as that involves interception of communications without a physically connected interception device.

The Director could not authorise such activity for the purpose of intercepting the private communications of a person who is a New Zealand citizen or permanent resident (unless and to the extent that person comes within the definition of a foreign person or foreign organisation).

The GCSB Act did not require that such authorisations be in writing, although the Bureau's practice was that they are written. Nor were these authorisations subject to the additional, more substantive criteria that applies to interception warrants and access authorisations.[50]

The requirement to keep a register of warrants and authorisations did not extend to Director's authorisations but during this reporting year, at my request, the Bureau did institute a system for prompt notification to my office of Director's authorisations.[51]

Two Director's Authorisations were issued and inspected by my Office during this reporting year. There were no issues with those authorisations.

New Zealand Security Intelligence Service

During the reporting year my office reviewed the 29 domestic intelligence warrants issued during the reporting period, as well as the 12 foreign intelligence warrants, issued under s 4A of the NZSIS Act. Those statistics include one domestic visual surveillance warrant issued and reviewed during the reporting period.

As a result of our warrant reviews over the reporting year, we discussed a range of questions with the NZSIS, including:

- the extent of detail provided in warrant applications – warrant issuers must be provided with all relevant and available information explaining not only the applicable statutory

[49] GCSB Act, ss 15(1) and 16(3).

[50] The outcome sought justifies the proposed intervention and is not likely to be achieved by any other means; there are satisfactory arrangements in place to ensure nothing will be done in reliance on the authorisation beyond what is necessary for the proper performance of a function of the Bureau and to ensure that the nature and consequences of acts done in reliance on the authorisation will be reasonable, having regard to the purposes for which they are carried out.

[51] The IS Act does not include an equivalent to s 16 GCSB Act authorisations.

constraints but also whether those constraints are engaged, how NZSIS will meet them and whether the warrant issuers should set specific conditions on the warrant

- whether NZSIS staff are provided with sufficient information and training to identify privileged communications in intercepted material (the NZSIS Act, and now the IS Act, protect privileged communications)
- the duration of a particular warrant – should it have been for a shorter period, having regard to the particular operational requirements?
- in relation to inadvertently intercepted material, how NZSIS deals with that possibility when it prepares a warrant application and how it handles such material if obtained
- in the case of an operation undertaken jointly with the GCSB, seeking clarification around which activity was undertaken by which agency and under what authorising instrument.

ASSESSMENT OF WHETHER COMPLIANCE SYSTEMS ARE SOUND

Purpose of and approach to certification

I must certify in each annual report the extent to which each agency's compliance systems are sound.[52]

I have applied a "positive assurance" approach which means that I have:

- Examined what compliance systems and controls, such as relevant policies, safeguards and audit/oversight/error-reporting measures, are in place
- Drawing upon my office's ongoing review work, examined a sample of each agency's activities. Because of the large volume of decisions and operations, I cannot scrutinise all activities – with the exception of warrants and authorisations – at all times and, in particular, must be selective about which activities to examine in depth
- Applied a materiality threshold: that is, I have sought to focus on whether compliance systems are sound in substance, rather than insisting upon any particular or formal arrangement, and whether identified shortcomings are material.

Certification of the soundness of the agencies' systems is therefore not the same as certifying every decision and action of the agencies was lawful and proper: rather, it is directed to minimising the risk of illegality and impropriety through training, guidance and awareness for staff, planning and operating safeguards; ensuring that breaches are brought to light, through effective audit and other oversight mechanisms; and ensuring those breaches are addressed, both in the particular instance and so far as they may disclose systemic shortcomings.[53]

There is a close connection between my office's specific review and inquiry work, which examines the legality and propriety of particular actions and practices, and the agencies' own compliance systems. To the extent that our review and inquiry work identifies breaches or problems, that may well indicate inadequacies in internal compliance mechanisms. Conversely, where compliance mechanisms are robust, that should lessen the likelihood of breach and also support and assist the rigour and transparency of my office's review and inquiry work.

I have described the compliance systems and some of the specific compliance measures, including innovations, taken by the GCSB and the NZSIS, together with my assessment of those systems, below. In addition, the wide-ranging inspections, reviews and inquiries carried out by my office during the reporting year have shown that the staff of both agencies have a desire to comply with relevant legislation, policy and practice and to achieve high standards in the work that they do.

The implementation and audit of effective and clear compliance safeguards is essential to ensuring that the agencies' staff are guided and supported, as well as ensuring wider public, political and legal accountability.

---

[52] IGIS Act, s 27(2)(ba). See also IGIS Act, s 11(1)(d). IS Act, s 158 (1)(f),(h) and s 222 (d)(c).

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

Outline and assessment of GCSB compliance systems

Compliance framework & structure

I reported last year my view that GCSB now has an established and strong compliance framework and practice. At the end of the last reporting year the GCSB undertook a "refresh" of their approach to the operation of the compliance function. One of the outcomes sought was that compliance activity is "normalised" and Compliance and Policy team members are seen as professional advisors, rather than activity gatekeepers. The Compliance Manager and the staff in the team are experienced professionals, drawn from operational areas of the Bureau to ensure they have a technical understanding of the working environment and how compliance issues might arise. This in turn gives them greater credibility with staff and a higher likelihood that advice will be sought from the team and acted on. As a corollary of this, the Compliance team is coming to be seen as a place to gain valuable professional experience and as a career progression step.

Compliance audit practices

During the course of the year the Compliance and Policy team focused on auditing queries made using the Bureau's most significant query tool to ensure that the data collected under warrants and authorisations was accessed and used in a legally compliant and proportionate way.

The Compliance and Policy team reviewed the structure and content of query "justifications" – the information required in order to submit a query or search of stored data – to ensure they met best practice and the requirements of Five Eyes partner agencies. Similarly the team reviewed and developed the Bureau's own governing principles and requirements for querying GCSB data.

It also undertook an audit of the auditors and refresher training for auditors.

A dedicated auditor was appointed shortly after the end of this reporting year and an extensive audit plan for 2017-2018 has been prepared and confirmed by the Bureau's senior leadership team.

Self-reporting of incidents

As I have said previously, I regard the self-reporting of errors or other incidents as a sign of a healthy and mature organisation. Mistakes will inevitably occur in every organisation: what is important is that staff feel they can identify those mistakes without fear of reprisal. This allows steps to be taken to deal with the consequences of a particular incident as soon as possible and measures such as changes in policy and procedure and fresh training can be put in place to minimise future recurrences.

The GCSB uses a Compliance Incident Register to track and manage potential incidents discovered or reported during the course of the Bureau's business activities where an incident involves possible breach of a policy, warrant or authorisation or of the governing legislation. The Compliance and Policy Team investigate the incident, determine whether it was a breach, determine the remedial action required and work with the operational teams to implement the required remedial action. Where there is a potential breach of a warrant or authorisation or of the governing legislation, the Compliance and Policy team notify my office of the outcome of the investigation. The technical and complex nature of the Bureau's work makes this self-reporting function particularly important.

In this reporting year there were eight self-reported incidents notified to my office. Three of the resulting inquiries by the Bureau Compliance team have been concluded. They all related to overly broad queries of particular databases. I am satisfied that in each case the breadth of the queries was inadvertent; caused by a technical mistake; promptly notified by the analyst concerned; the data deleted and further training given where assessed to be appropriate.

The remaining five incidents, which are still under investigation by the Bureau Compliance and Policy team, ranged from possible inadvertent collection of communications of (non-New Zealand) Five Eyes persons to inadvertent retention of data obtained under a warrant for a period longer than that specified in the warrant.

There are two further compliance incidents, first reported to me in the 2015-2016 year, where the GCSB Compliance and Policy team has completed its investigation but the agency's report has not yet been finalised.

I am satisfied that the incidents were promptly reported and investigations commenced. While I would hope to see the reports on self-reported incidents finalised more promptly, in each case the incidents reflected inadvertence or factual or technical mistakes.

Interaction with IGIS office

As with the NZSIS, the Bureau's compliance practices also incorporate scheduled and *ad hoc* engagement with my office, including:

- notification of self-identified compliance incidents, as above, as soon as practicable after those incidents occur. Where necessary, we discussed proposed investigative and/or remedial steps with the Compliance and Policy Manager and sometimes the Chief Legal Adviser
- consultation with my office on novel or likely contentious actions or issues. While it would be inconsistent with my review and oversight role to provide prior "authorisation" for particular actions, consultation does provide an opportunity to identify obvious risk areas
- monthly GCSB/IGIS Working Group meetings. This Group was set up as a forum for the Inspector-General to discuss operational issues and processes, and compliance consequences, with compliance and audit staff and relevant operational managers. It has evolved into a forum where senior Bureau managers can also brief me about changes or issues in their area
- occasional compliance and policy reports which cover the development of operational policies and procedure, compliance training of staff, audit activity, Official Information Act and Privacy Act requests.

There is also a compliance component to the Bureau's wider engagement with my office, through:

- regular meetings with the Director-General of the GCSB and his senior staff, including in regular joint meetings with the Director-General and senior staff of the NZSIS
- monthly meetings with the Chief Legal Adviser to discuss any questions or issues identified in our regular review of warrants and authorisations
- consultation on draft policies and procedures.

My assessment

The Bureau has robust compliance measures. As a result errors are promptly identified and remedied. GCSB has comprehensive, and up to date policies and audit procedures. There is a strong culture of commitment to compliance and to reporting and learning from errors. Bureau staff in roles at all levels engage very constructively with my office.

In last year's annual report I noted two areas for monitoring:

- the importance of maintaining a rigorous internal audit practice, given changes in the structure and skills composition of the Compliance and Policy team
- finalisation of a comprehensive data retention and destruction policy.

On the first point, I have noted above the Bureau's regular audit practices as well as the appointment of a dedicated auditor.

As to the second, a comprehensive data retention policy, which gives effect to the GCSB's statutory obligation to assess collected data for relevance and destroy irrelevant data as soon as practicable after collection, was also finalised.

As noted above, some further focus is required around timeliness in the areas of queries about warrants and completion of internal investigations into self-reported incidents, but I consider that those issues do not call into question the overall efficacy of Bureau procedures and systems.

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

Outline and assessment of NZSIS compliance systems

In my 2016 Annual Report I noted the substantial structural and policy reforms the NZSIS had put in place that year. I also commented on significant improvements in specific activities and operations.

I nonetheless concluded that overall further work was required before I could assess NZSIS's compliance procedures and systems as "sound". I set out my expectation that the positive steps taken to date would be consolidated and that in a year's time NZSIS would be in a position to better manage the demands of systematic Inspector-General oversight and review in a timely and efficient way, without compromising operational activity. I identified several specific areas for development: regular tracking and analysis of any trend arising from self-reported incidents, full and timely records of operational activity and decision-making, and development and implementation of an audit plan.

Further substantial compliance reforms

I note below some specific examples of compliance reforms achieved in the last year which build on the achievements of the previous year. This is by no means an exhaustive list.

Implementation of 2015 Review of Compliance

All of the 45 recommendations made in the NZSIS's internal Review of Compliance had been implemented by 30 June 2017.

Development of operational policies and Standard Operating Procedures (SOPs)

A large number of policies and SOPs to guide the NZSIS's various operational activities have been developed. The review and drafting of SOPs was done primarily by operational staff, with involvement from the Service's Compliance and Legal teams, ensuring they are practical and workable.

Self-reporting of compliance incidents

At the suggestion of my office, since July 2016 the NZSIS expanded its register and reporting to me to cover all operational compliance incidents, not just inadvertent interceptions as in the previous year. The incidents are categorised in the NZSIS's quarterly Compliance Reports to my office which enables a ready assessment of any trends, as I recommended in last year's report.

The particular compliance incidents in this reporting period are discussed at pages 31-32 below.

Quarterly compliance reports

In this reporting year the NZSIS Compliance Manager instituted a quarterly *Compliance Report to the Inspector-General of Intelligence and Security* (Compliance Report) to provide my office and the NZSIS senior leadership team with updates on the Compliance programme and compliance incidents. I have found the Compliance Report a useful tool and my assessment is that the adoption of a compliance incidents register and encouragement to staff to self-report incidents means that errors are more likely to be promptly identified and appropriate remedies put in place.

Development of an audit programme

In May 2017 the NZSIS implemented a Compliance audit plan to June 2018. It includes ten audits across a range of NZSIS activity and teams, including areas of known risk, identified through previous compliance incidents and findings and recommendations from my office. The planned audits include some to give effect to obligations under the IS Act, such as audits of NZSIS compliance with the Direct Access Agreement to Advance Passenger Processing (APP) Database between the Minister in charge of the NZSIS and the Minister of Immigration and the Direct Access to the NZCS CusMod database between the Minister in charge of the NZSIS and the Minister of Customs.

Improved compliance culture

The changes introduced during this year and the previous year have all had the stated intention of both strengthening compliance systems and encouraging a strong compliance culture. I have observed

the effect of the changes across a number of areas of the NZSIS's operations. I note two by way of example.

Vetting Transformation Programme

One of the Service's operational areas which has undergone significant change this year is the security clearance vetting team. Ten separate projects were initiated, under a "vetting transformation" umbrella. This work will streamline and, where possible, automate the vetting process, with a consequent reduction in the time taken to process an application; enhance the quality and consistency of assessments made during the process (including through development of overarching policies and a greater focus on staff recruitment, development and assessment); and establish a more collaborative and agreed risk approach with government agencies who put forward candidates for the vetting process. Separate emphasis is given to the implementation of IGIS recommendations relating to the vetting process and systems.[54]

This programme of work has already resulted in demonstrable improvements in vetting processes.

Operational teams

Other operational teams have developed policies and SOPs to govern their daily activities, together with revised training programmes and regular assessments of how staff are progressing. NZSIS staff have conveyed to me a sense that, through their direct involvement with the development of operational policies and SOPS and training to implement them, they now see compliance as a tool that enables them to do their job more effectively and with greater assurance that they are complying with the law at all times.

Self-reporting of operational compliance incidents

Such incidents are reported to me by the NZSIS Legal or Compliance team as soon as the incident becomes known to them. A full report is provided once an internal investigation of the incident is completed. At that point I have an opportunity to comment on the incident and the investigation, to ask questions and, if necessary, to make recommendations for remedial action.

A summary and categorisation of all incidents is included in the Service's quarterly Compliance Report to my office.

A total of ten incidents were notified to me in this reporting year, in the following categories:

- Interception of incorrect numbers, lines, data sets or equipment (eg a staff member accidently entering an incorrect telephone number)
- Numbers intercepted correctly but subsequently abandoned by the target and/or adopted by a non-target
- Organisations assisting NZSIS not being given the correct or most up to date documentation relating to the particular warrant

[54] See note 14 above.

- Failure to adhere to internal policy or procedures.

I was satisfied, sometimes after seeking further information or making suggestions as to remedial steps, that appropriate steps were taken in relation to each incident to mitigate the effect of the particular error and that overarching policies and processes were reviewed as appropriate. While the categories of incidents are the same as in the last reporting year, the number of incidents in each category is decreasing over time.

Interaction with IGIS Office

My office's engagement with the NZSIS principally occurs by way of:

- regular meetings with the IGIS/NZSIS Liaison Group, which provides a useful, regular forum for me and the Deputy Inspector-General to meet with senior NZSIS staff to discuss current IGIS Office inquiries and reviews and emerging issues
- monthly meetings with the Service's General Counsel to discuss any questions or issues arising from the review of all warrants
- discussions with relevant operational staff and members of the Service's legal team on specific issues.

There is also a compliance component to the Service's wider engagement with my office, through meetings with the Director-General, including in joint meetings with the Directors-General of both agencies and their senior staff.

My assessment

The NZSIS has made significant progress this year in completing the implementation of an expanded compliance structure and dedicated compliance staff. Implementation of all of the (self-imposed) requirements of the 2015 Internal Review of Compliance means that the organisation is now able to provide appropriate support for lawful operational activities and has the means to record, audit and review those activities. It is clear that NZSIS staff now more readily perceive compliance with legislation and policy as an inherent part of their work and a safeguard for them individually and for the organisation.

The development of the organisation's compliance structures and practice has allowed for more ready engagement with my office in relation to review of operational activities.

In last year's Annual Report I expressed the hope that the increased funding available to the agencies in the next reporting year would enable the NZSIS to better manage the demands inevitably placed on the organisation by systematic Inspector-General oversight and review, in a timely and efficient way, without compromising operational activity. However, for both the NZSIS and the GCSB, the development of the New Zealand Intelligence and Security Bill 2017 and significant work required in anticipation of the IS Act coming into effect, created a great deal of work and pressure, on top of operational demands, which had the effect of reducing response times.

There are still some specific areas that the NZSIS must address:

- now that the IS Act is in place it should be able to respond more quickly to oversight requests (whether in response to requests for further information, or for a reasoned and supported response to a proposition or draft document put forward by this office)

- There are some lessons from the last year, especially those highlighted by the APP/CusMod review. Chief among these are the need to be clear about, and proactive in, ensuring a legal basis for operational activity; promptly obtaining legal advice if there is any doubt, dispute or ambiguity; keeping the IGIS closely informed of progress on such issues and on the Service's analysis and proposals for handling the situation; and consistently taking an open and informative approach to engagement with the IGIS. In saying that, I acknowledge that there are many matters on which we do meet regularly and have open and valuable discussions. Both the Service and I are committed to fostering this approach.

Overall, I certify that the NZSIS has sound compliance procedures and systems in place. To the extent that particular measures or practices are under further development or review, I consider that those do not call into question the overall efficacy of Service procedures and systems.

OTHER ACTIVITIES

Intelligence and Security Oversight Coordination Group

The Privacy Commissioner, Chief Ombudsman, Auditor-General and I meet regularly as the Intelligence and Security Oversight Coordination Group. Each of us has a role in oversight of the intelligence and security agencies and it has proved useful to discuss areas of overlap in our responsibilities and broader issues of common interest. It is important to develop relationships of mutual support, coordination and cooperation between integrity agencies. This helps each of us to maintain our long-term independence.

Visits to regional facilities

My staff and I visit the GCSB's two communications interception stations, at Waihopai and Tangimoana, and the NZSIS's northern regional office, as part of my regular scrutiny of the activities of the agencies.

Public engagements

I look for opportunities for public engagement to talk about the Inspector-General's office because I think it is important to build public trust and confidence that we are scrutinising what the agencies do in a rigorous and independent way. We must ourselves be as transparent as possible. It is also important that we help to foster a public discussion about the role and activities of the intelligence and security agencies in New Zealand.

As at the date of publication of this report I had given one news media interview, spoken at four meetings within the Intelligence Community, three other government agencies and one group of senior consultants (contractors to both the public and private sectors). Two members of my staff and I also met for most of a day with a large Muslim community in Auckland, to let them know the jurisdiction and functions of my office and to hear their concerns and questions about the way in which the intelligence and security agencies, and other government agencies, interact with members of the community.

I also attended two meetings of the Five Eyes Intelligence Oversight and Review Council (FIORC). FIORC comprises the non-political intelligence oversight, review, and security bodies from the United Kingdom, United States, Canada, Australia and New Zealand. The purposes of the forum include to exchange view in subjects of mutual interest and concern, compare best practices in review and oversight methodology, explore areas where cooperation on reviews and the sharing of results can occur and to encourage transparency to the largest extent possible.

Shortly before this report was published I also attended the International Intelligence Oversight Forum (IIOF2017) in Brussels, organised by the mandate of the United Nations Special Rapporteur for Privacy, together with the Belgian, Dutch and Luxembourg Data Protection Authorities. IIOF was attended by representatives from more than 40 specialist intelligence and security oversight bodies, data protection authorities, NGOs and academics. It provided an opportunity for an update on recent law changes dealing with surveillance and an exchange of views on good oversight practices.

OFFICE FINANCES AND ADMINISTRATIVE SUPPORT

Funding

The IGIS office is funded through two channels. The first is a Permanent Legislative Authority (PLA) for the remuneration of the Inspector-General and the Deputy Inspector-General.[55] The second is the operating costs of the office which are funded from Vote: Justice (Equity Promotion and Protection Services), as part of the Ministry of Justice's non-Ministry appropriations.

2016/17 budget and actual expenditure

Total expenditure for the 2016/2017 year was $1.436 million, as follows:

	Actual ($000s)	*Budget*
Staff salaries/advisory panel fees; travel	631	*720*
Premises rental and associated services*	52	*117*
Other expenses	26	*60*
Earthquake Expenses**	172	*0*
Non-Departmental Output Expenses (PLA)	555	*570*
Total	**1436**	***1467***

Note:
*No rental and building expense were paid since November 2016, due to disruption to the office from the earthquake.
**Includes provision of $150k for future relocation and other costs arising from the 2016 earthquake.

Administrative support

Ongoing administrative support, including finance and human resources advice, is provided to the Inspector-General's office by the Ministry of Justice. The New Zealand Defence Force provides standalone IT support, on a cost recovery basis.

[55] IGIS Act, ss 8 and 15D; IS Act, Schedule 3, cl 9.

Office of the Inspector-General of Intelligence and Security
P O Box 5609
Wellington 6140
04 817 0402
enquiries@igis.govt.nz
www.igis.govt.nz

Follow us on Twitter @igis.nz