Office of the Inspector-General of Intelligence and Security

Annual Report

For the year ended 30 June 2015

Cheryl Gwyn
Inspector-General of Intelligence and Security

21 October 2015

CONTENTS

OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

21 October 2015

Rt Hon John Key
Prime Minister of New Zealand
Minister for National Security and Intelligence

Dear Prime Minister

I **enclose** my annual report for the period 1 July 2014 – 30 June 2015.

You are required, as soon as practicable, to present a copy of the report to the House of Representatives (s 27(3) of the Inspector-General of Intelligence and Security Act 1996 – the Act), together with a statement as to whether any matter has been excluded from that copy of the report.

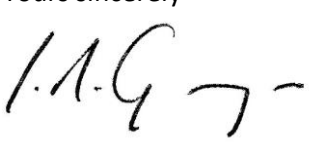
The Directors of the New Zealand Security Intelligence Service and the Government Communications Security Bureau have confirmed that publication of those parts of the report which relate to their agencies would not be prejudicial to the matters specified in s 27(4) of the Act, and that the report can be released marked "UNCLASSIFIED" without any redactions.

You are also required to provide the Leader of the Opposition with a copy of the report (s 27(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.

I also take this opportunity to seek your concurrence, in accordance with s 27(7) of the Act, to make myself available to discuss the contents of my report with the Intelligence and Security Committee, should the Committee request my attendance.

Yours sincerely



Cheryl Gwyn
Inspector-General of Intelligence and Security

Copy to:
Hon Christopher Finlayson QC
Minister in Charge of the New Zealand Security Intelligence Service
Minister Responsible for the Government Communications Security Bureau

Foreword

As at the end of the reporting year I had been Inspector-General for 14 months. I am pleased to present the first annual report of what is now a fully staffed and adequately resourced Inspector-General's office.

In last year's annual report I stated my intention to provide an informative description of my role and the activities of my office and to shed as much light as possible on what the intelligence and security agencies actually do. It's important that intelligence and security matters are open to scrutiny. Consistent with that intention, this report sets out our work over the last year in as much detail as possible. It will be supplemented by more detailed reports on specific inquiries as these are completed in the coming months.

In particular, my office is now in a position, for the first time, to give an informed certification of the extent to which the compliance systems of New Zealand's intelligence and security agencies are "sound", as required by the legislation governing my office. My objective in applying the certification requirement is that, if the agencies' systems are sound, errors will be avoided, so far as possible, and any errors made will be identified and addressed within the organisation and where necessary by my office.

What does the Inspector-General do?

The role of the Inspector-General of Intelligence and Security was introduced in 1996[1] to increase the level of oversight and review of the intelligence and security agencies. The office of Inspector-General was substantially strengthened in late 2013 through enhanced powers and institutional arrangements. The Inspector-General is responsible for two agencies, the New Zealand Security Intelligence Service (NZSIS or Service) and the Government Communications Security Bureau (GCSB or Bureau).

New Zealand Security Intelligence Service

The NZSIS is a civilian intelligence and security organisation. It is not a public service department and sits outside the State Sector Act 1988, but it is part of the broader State Services and, like the GCSB, is an instrument of the Crown.

The functions of the NZSIS are contained in the New Zealand Security Intelligence Service Act 1969 (NZSIS Act). It has three main functions:

- to gather information and produce intelligence that will enable it to warn the government about activities that might endanger New Zealand and New Zealanders, including New Zealand's economic well-being.
- to provide protective security, including security screening services.
- to collect foreign intelligence relevant to security.

During the reporting period the Prime Minister was the Minister in charge of the NZSIS until 13 October 2014. From 13 October, the Prime Minister became Minister for National Security

[1] Inspector-General of Intelligence and Security Act 1996 (IGIS Act).

and Intelligence and the Hon Christopher Finlayson QC became the Minister in charge of the NZSIS.

Government Communications Security Bureau

The GCSB is a civilian intelligence and security agency. It is a public service department. The Bureau's objective, contained in the Government Communications Security Bureau Act 2003 (GCSB Act), is to contribute to the national security, international relations and well-being and the economic well-being of New Zealand.

It has three statutory functions to achieve that objective:

- to provide information assurance and cyber security services, keep confidential government data secure and protect government agencies and some key private organisations from malicious cyber-attacks or hacking attempts.
- to collect and analyse foreign intelligence and provide that to the responsible Minister and any person or office holder (in New Zealand or overseas) who is authorised by the Minister to receive it.
- to cooperate with and give assistance to the New Zealand Police, the New Zealand Defence Force and the NZSIS in carrying out their lawful functions, subject to any limitations and restrictions that apply to the other entity.

During this reporting period, the Prime Minister was the Minister responsible for the GCSB and until 13 October 2014. From 13 October, the Hon Christopher Finlayson QC was the Minister responsible for the GCSB.

Role of the Inspector-General

The Inspector-General's statutory role[2] is to assist the Minister responsible for each of the agencies to ensure that their activities comply with the law.

The IGIS Act provides the legal basis for regular inspections of the intelligence and security agencies, to assess their procedures and compliance systems and, ideally, to identify issues before there is a requirement for remedial action. The programme for general oversight and review of each intelligence and security agency is submitted by the Inspector-General for the Minister's approval.[3]

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, or 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 have an obligation to independently investigate those complaints.

---

2 IGIS Act, s 4(a).

3 See at p 10 below.

In order to carry out these functions, I have a right of access to 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 - which is the most common form 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, there are situations where prior discussion with my office can help to ensure clarity about the legality and propriety of any planned activity.

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]

Why effective oversight is necessary

There are at least five good reasons why effective oversight of intelligence and security agencies is necessary.[7]

- National security activities involve the most intrusive powers of the State: electronic surveillance, search of property, information collection and exchange with domestic and foreign intelligence and security and law enforcement agencies, amongst other things. Oversight is necessary to help ensure that those powers are used lawfully.
- Oversight is a safeguard against incumbent governments using intelligence and security agencies to protect or promote party political interests.
- The secrecy surrounding intelligence and security agencies about what they do largely shields them from the processes of public accountability which apply to other public bodies in a democracy. Effective oversight can act as a proxy for that public accountability.
- The agencies are funded with public money and should be accountable for the use of this money.
- Oversight helps ensure that the agencies fulfil their mandate effectively.

---

4 IGIS Act, ss 2 and 20.

5 IGIS Act, s 21.

6 Alongside the GCSB and the NZSIS:

- The National Assessments Bureau provides 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; and
- Immigration New Zealand, the New Zealand Customs Service and the New Zealand Police have intelligence units.

7 European Parliament, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union* (2011) pp 85-86.

The intelligence oversight framework in New Zealand

Effective intelligence oversight requires more than just one person or office. Effective oversight requires the successive involvement of the Directors, management and operational staff of the intelligence and security agencies; the Prime Minister and the responsible Minister; the Leader of the Opposition; the Commissioner of Security Warrants; the courts; Parliament, including through the Intelligence and Security Committee, responsible select committees; oversight agencies, including but not limited to my office; and the wider public, including through civil society and non-governmental organisations:

- *The Directors, management and operational staff of the agencies:* The agencies' leadership and internal service controls, management systems and operational practices are important safeguards. In New Zealand, the Director of each agency also has particular responsibilities, both in authorising the use of certain intelligence-gathering powers against statutory criteria and in upholding the agencies' obligations of political neutrality, which require still more than the conventional obligations of the wider public service.
- *The responsible Minister and the Minister for National Security and Intelligence:* The Minister in charge of the NZSIS and responsible for the GCSB is accountable to Parliament for the general conduct of the intelligence and security agencies. The Minister has a degree of control over and a right to demand information from the agencies. They must account for the use of their legal powers and for their financial performance. The Minister is also responsible for authorising specific operations, by way of warrant or authorisation. The Minister for National Security and Intelligence (a role currently held by the Prime Minister) does not have ministerial responsibility for the agencies but leads the national security sector and sets the overall framework in which the agencies operate.
- *The Leader of the Opposition:* Under the GCSB Act and the NZSIS Act, the two intelligence and security agencies are required to consult regularly with the Leader of the Opposition for the purpose of keeping him or her informed about matters relating to security. There is a related requirement of notification under the Terrorism Suppression Act 2002 and the Leader of the Opposition is also specifically recognised in the Intelligence and Security Committee Act 1996 and in the IGIS Act. That provision for the Leader of the Opposition is particular to national security matters and provides a check against misuse of the powers of intelligence and security agencies, supports the principle that national security should so far as possible be non-partisan and contributes to political accountability.[8]
- *The Commissioner of Security Warrants:* The Commissioner of Security Warrants must be a retired Judge. The Commissioner has joint role with the Minister responsible for the GCSB in authorising interception warrants or access authorisations if anything to be done is for the purpose of intercepting New Zealanders' private communications and jointly with the Minister in respect of

[8] As noted in my November 2014 inquiry report into the release of certain NZSIS information, *Report into the release of information by the New Zealand Security Intelligence Service in July and August 2011* (November 2014) 46-47, and further below for current arrangements.

NZSIS domestic intelligence warrants, where the warrant relates to a New Zealand citizen or permanent resident.

- *The Courts:* The actions of the intelligence and security agencies may be subjected to legal proceedings in broadly the same way as any public body, as may the agencies' staff.

- *Parliament*: The responsible Ministers are accountable to the House of Representatives. In addition, the Intelligence and Security Committee (ISC) has a role. The ISC is a statutory committee,[9] rather than a committee of Parliament as select committees are, but its members serve on the ISC in their capacity as Members of Parliament. The ISC consists of the Prime Minister, the Leader of the Opposition, two Members of Parliament nominated by the Prime Minister after consultation with the leader of each party in any government coalition and one member nominated by the Leader of the Opposition, with the Prime Minister's agreement, after consultation with the leader of each party not in government or in coalition with a Government party. Unless the Committee unanimously resolves to the contrary, all of its proceedings are held in private. The Committee considers the estimates for and conducts a financial review of the intelligence and security agencies. The Committee may also receive responses given by the responsible Minister to reports from my office.

  The House usually orders that no select committee can examine an intelligence and security agency.[10] However, intelligence and security legislation is in general considered by the responsible select committee, the Foreign Affairs, Defence and Trade Committee.

  The Inspector-General's annual report is presented to the responsible Minister(s) and the Prime Minister and the Prime Minister must present a copy of the report to the House of Representatives. This enables the possibility of questions from other Members of Parliament on oversight matters referred to in the annual report.

- *Independent institutions, such as the Controller and Auditor-General, the Privacy Commissioner, and the Office of the Ombudsman:* The Auditor-General (an Officer of Parliament) provides independent assurance that public sector organisations are operating and accounting for their performance in accordance with Parliament's intentions. The Privacy Commissioner (an independent Crown Entity) can investigate complaints about access to and correction of personal information held by the intelligence and security agencies; while the agencies have an exemption from many of the privacy principles under s 57 of the Privacy Act 1993, they are still subject to principles 6 and 7 – the rights to request access to information held about them by the GCSB and the NZSIS and, if they receive it, to request correction of that information. The GCSB Act also includes provision for the GCSB to develop a personal information policy in consultation with the Privacy Commissioner and the Inspector-General and the GCSB must report the results of audits conducted under the policy to the Privacy Commissioner. The GCSB and the NZSIS are subject

[9] Intelligence and Security Committee Act 1996 (ISC Act). See David McGee, *Parliamentary Practice in New Zealand* (Third Edition), pp 35, 79, 437.

[10] McGee, ibid, p 79.

to the Official Information Act 1982 and the Ombudsman's jurisdiction under that Act. The Ombudsman is an Officer of Parliament.

- *The public, including through media and civil society:* The public, including through NGOs and advocacy groups, play a role in intelligence oversight through their ability to analyse and critique government policies and activities. Academics and the media play an important role in scrutinising intelligence service conduct, including through investigation of claims of improper, illegal, ineffective and/or inefficient actions.

The year in review – highlights

The principal work of the office during the reporting period comprised:

- The commencement and completion of one major inquiry, concerning the release of information by the NZSIS in July-August 2011;
- The continuation and/or commencement of four further own-motion inquiries;
- The receipt and investigation of a range of complaints;
- The review of all GCSB and NZSIS warrants and authorisations; and
- The ongoing assessment of the soundness of compliance systems and practices in the two agencies.

Inquiry into NZSIS release of information

This was the first inquiry since my appointment as Inspector-General and the first significant inquiry since amendments were made to the IGIS Act in 2013.

Twenty two individuals were summonsed and gave their evidence under oath or affirmation, and some appeared with legal representation. I searched in significant depth the electronic and physical records of the NZSIS and the Prime Minister's Office. As a result, the final report benefited from a substantial documentary record, including transcripts of phone conversations which proved particularly significant.

It was the first occasion where IGIS powers were exercised inside the parliamentary precinct including the office of the responsible Minister at that time, the Prime Minister. This order was executed in consultation with the Speaker, the Parliamentary Service, and the Office of the Clerk, and with notification provided to the Prime Minister, in accordance with the protocol set out in the Privileges Committee report on *Questions of privilege regarding use of intrusive powers within the parliamentary precinct*. It was vital that care was taken to ensure my powers were exercised appropriately and in accordance with the law.

The inquiry was a significant undertaking for the Office, which at that stage was not fully staffed. The inquiry demonstrated the unique and significant powers available to the Inspector-General when conducting an inquiry. I have summarised the findings and recommendations of that inquiry, which were accepted in full by the NZSIS, and the NZSIS's implementation of those recommendations below at pages 25-28.

Expanded IGIS office

In last year's annual report I signalled that I expected the set-up of the IGIS office premises and secure communications systems and the recruitment of a full complement of staff would be completed in the 2014/15 year.

I am pleased to say the task of establishing a fully functioning, secure and fulltime oversight office has been achieved. The office, since February of this year, has comprised the Inspector-General, Deputy Inspector-General, IT Manager/Security Advisor, EA/Office Manager and four Investigating Officers. Of the Investigating Officers, one is employed on a permanent basis. The other three are seconded for an eighteen month period – one each from the New Zealand

Police, Inland Revenue and New Zealand Customs Service. The secondments have allowed my office to acquire the skills and experience that are available in other agencies, while providing valuable development opportunities for the individuals, and allowing time in which I can assess the longer term staffing needs of the office. I am grateful for the assistance of the three seconding agencies.

On current arrangements, the Inspector-General has the equivalent of just over 1% of the staff and budget of the two agencies for which we have oversight responsibility. The current level of staffing and funding appears adequate to discharge effective oversight in line with the office's expanded responsibilities arising from the 2013 amendments to the IGIS Act and the new obligations in respect of NZSIS visual surveillance and urgent/emergency authorisations, introduced in late 2014 and described below.

The IGIS office now has a more developed website (www.igis.govt.nz) and a Twitter address (@igisnz) which are intended to provide more information about the work of the Office, how to make a complaint about the NZSIS or GCSB and also to allow my office to connect with more people and increase our exposure to relevant issues.

Statutory advisory panel

The two members of the Inspector-General's advisory panel,[11] Christopher Hodson QC (chair) and Angela Foulkes, were appointed in October 2014. The panel members have appropriate security clearances to enable them to have access to, and discuss with me, the classified material held by the NZSIS and the GCSB that my office must look at in order to carry out our review, inquiry and audit functions. I meet with the panel members on a regular basis, or to address particular issues as they arise, and I have been assisted by the experience and different perspectives they bring to the role.

Legislative changes

The Countering Terrorist Fighters Legislation Bill was considered under urgency in November-December 2014. The Bill provided for amendments to the NZSIS Act, the Customs and Excise Act 1996 and the Passports Act 1992.

As enacted, these amendments provided new powers for the Service to undertake surveillance without a warrant, where the process of obtaining a warrant would be impractical and likely result in a loss of intelligence, and for visual surveillance of private activity in private premises, where doing so is necessary for the detection, investigation or prevention of actual, potential or suspected terrorist acts, or facilitation of such acts. The maximum period for which surveillance may be undertaken without a warrant is 24 hours (reduced during the select committee process from the originally proposed 48 hours).

In the course of the select committee process the bill was amended to provide for increased oversight of urgent surveillance authorisations and visual surveillance warrants. As enacted:

- Where the Director authorises surveillance on an urgent or emergency basis, without a warrant, both the Minister and Inspector-General must be notified immediately after the Director issues the authorisation.

[11] IGIS Act, ss 15A-15F.

- Upon expiry of any emergency authorisation for warrantless surveillance, if no application has been made for an intelligence or visual surveillance warrant, the Director must report the relevant circumstances, including the nature of information collected, to the Minister (and where applicable the Commissioner of Security Warrants). Upon receipt of the Director's report, the Minster (and Commissioner) must refer the matter to the Inspector-General for investigation.

- Similarly, if an application for a warrant to follow an emergency authorisation is made but refused by the Minister and Commissioner, the Director must refer the matter to the Inspector-General for investigation.

- Whenever no subsequent application for a warrant is made or the application is refused, any records resulting from the emergency surveillance must be destroyed unless they are relevant to the detection of activities prejudicial to security or to the gathering of foreign intelligence information that is essential to security. Where records are retained for either of these purposes the Minister must refer the matter to the Inspector-General for investigation.

The NZSIS is required to provide a copy of any visual surveillance warrant to the Inspector-General as soon as practicable after it is issued.

The new provisions are subject to a sunset clause, having regard to the review of the intelligence and security agencies, their governing legislation and oversight legislation,[12] commenced in June 2015, which will consider the continued utility of these powers.

Appearance before the Foreign Affairs, Defence and Trade Committee

During its consideration of the Countering Terrorist Fighters Legislation Bill, the Foreign Affairs, Defence and Trade Committee invited me to attend before it in private to outline my role and jurisdiction and how the Inspector-General's oversight role might be relevant to the additional powers for the NZSIS that were proposed in the bill.

Appearance before the 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 (under s 27 of the IGIS Act).[13] The Inspector-General may, with the concurrence of the Prime Minister, report either generally or in respect of any particular matter to the ISC.[14]

At the ISC's invitation I attended before it at a private hearing on 27 May 2015 to discuss my 2013/14 annual report.

[12] See below, p 11.

[13] ISC Act, s 6(1)(f).

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

The year ahead

IGIS office setup

Some further consolidation of office systems is necessary in the next reporting year, including further development of the IGIS website to make it more informative and useful for members of the public and implementation of a document management system. This will facilitate clearer reporting on, for example, time taken to complete inquiries and resolve complaints.

Work programme

The IGIS Act[15] requires me to prepare a programme of work for general oversight and review of the agencies I oversee, the NZSIS and the GCSB. The bulk of the work programme is directed at the functions which are specified in the IGIS Act.[16]

I submit the work programme to the Minister responsible for each of the agencies[17] for approval.[18] The requirement for approval does not mean that the Minister does or must approve each specific item of my office's work, such as each inquiry into a complaint or each inquiry that I initiate of my own motion. I am required to independently investigate complaints relating to each of the agencies and I have specific powers to initiate my own inquiries into any matter that relates to the compliance by the NZSIS or the GCSB with the law of New Zealand or into the propriety of particular activities of either agency. Consistent with those powers and obligations, in practice the Minister is informed of the work programme and asked if he has any suggestions about it.

The current work programme (July 2015) is the first to be made public (http://www.igis.govt.nz/publications/igis-work-programme-july-2015/).

In addition to the regular functions required under the IGIS Act, the office will continue work on current inquiries[19] and complaints with a view to reporting on all of these matters in the calendar year.

We will undertake a comprehensive review of any visual surveillance warrants and any authorisations for urgent, warrantless surveillance in the next reporting year.

We are developing a procedure for unscheduled audits of the agencies' procedures and compliance systems[20] and I expect unscheduled audits will be undertaken in the next reporting period.

Thematic investigations

Thematic investigations are an important part of effective oversight. These focus on broad issues rather than specific events, although they sometimes arise from inquiries into specific

---

15 IGIS Act, s 11(1)(e).

16 IGIS Act, s 11(1)(a)-(da).

17 Currently the Hon Christopher Finlayson QC.

18 IGIS Act, s 11(1)(e).

19 See below, p 20.

20 IGIS Act, s 11(1)(da).

events which reveal more far-reaching concerns. To the extent that resources allow, I anticipate that in the coming year my office will look to more thematic investigations.

Legislative review

The NZSIS Act has been in effect for 46 years and the GCSB Act for 12 years. The legislation in relation to oversight – the IGIS Act and the ISC Act– was enacted 19 years ago.

While all of these pieces of legislation have been subject to some amendment over that time, there has been no overarching review of the legislation governing the agencies and the oversight function.

As part of the 2013 amendments to security and intelligence legislation, the ISC Act now provides for a periodic review of such legislation. In May 2015, the Hon Amy Adams, as Acting Attorney-General, appointed two reviewers, the Hon Sir Michael Cullen and Dame Patsy Reddy to undertake the first such review.[21]

The reviewers are to provide their report to the Intelligence and Security Committee by 29 February 2016. The Committee will consider the report and present it to Parliament. The Government response to the report is likely to include the introduction of legislation to amend the current framework.

As part of the statutory review framework, I am able to provide information to the reviewers both on request and at my own initiative. In general, it is not the role of the Inspector-General to comment on current or proposed government policy. However, there are some matters on which my office has particular experience because of our oversight of the activities of the intelligence community, which may assist the reviewers and the Intelligence and Security Committee, when it comes to consider legislative proposals. At that stage, my comments will be focused on whether any proposals for change:

- set out clearly the powers of the agencies, purpose of those powers and controls on them
- have proper accountability and oversight mechanisms
- pose any risks to legality or propriety
- are consistent with human rights
- address issues that I am aware of through my examination of NZSIS and GCSB operations

I am particularly interested in whether proposed policies and legislative changes place sufficient weight on maintaining the privacy of individuals and whether proposals reflect the concept of proportionality – that is, that the means for obtaining information must be proportionate to the gravity of the interests at risk or otherwise in issue.

In preparation for the legislative amendment phase of the review, I raise the following questions and issues for consideration:

[21] ISC Act, ss 21 and 22.

- To what extent (if at all) is it necessary to extend or otherwise modify the powers of the agencies?

  To answer this question it is necessary to have a picture of the effectiveness of the existing powers, both in terms of the demands faced by the agencies and the agencies' capacity, in practice, to use those powers. It must be convincingly demonstrated that present powers are insufficient before considering an increase in the current statutory powers. Any new powers must be commensurate with the scale and resources of the agencies, to ensure that they can properly utilise the new powers.

- Do proposals for enhanced powers include necessary accountability and oversight mechanisms?

- What additional obligations and safeguards are required around existing powers and practices, including emerging or evolving intelligence-gathering practices?

  As an example, if there is a technological need for collection of some categories of "bulk" or "unfiltered" data in order for relevant data to be identified and extracted,[22] then it is necessary to ensure that the legislative framework includes safeguards for that practice, including requirements for separation into relevant and non-relevant communications as soon as possible after interception; specified limits on retention of communications not known to be relevant; and destruction. Access to and use of intercepted data which is retained should be subject to conditions and restricted by both organisational and technical means.

Inspector-General's review 2014/15

Work programme

The annual programme of work for the IGIS office covers general oversight and review and the particular functions set out in the IGIS Act.[23]

Measures of effectiveness

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

[22] See, for example, the conclusions of the United States National Research Council *Bulk Collection of Signals Intelligence: Technical Options* (2015), defining (at S1) "bulk collection" as any collection of communications signals where "a significant portion of the data collected is not associated with current targets" and concluding (at S6-S7) that "[t]here is no software technique that will fully substitute for bulk collection", but that there was scope for better targeting and better automatic access controls; see also, among others, the United Kingdom Parliament Intelligence and Security Committee, *Privacy and Security: A Modern and Transparent Legal Framework* (2015) at ch 4.

[23] See p 2 above.

- 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.

Agency engagement

As in the preceding year, I received the full cooperation of the NZSIS and the GCSB, with access to all premises, ICT systems, documents and employees.

I met regularly with the Directors of the NZSIS and the GCSB and their senior staff to discuss current issues and concerns and to highlight issues arising from my office's inspection and inquiry activities. The agencies have also used these discussions to brief me on emerging issues or potential concerns and how they propose to respond to them.

These discussions enhance my awareness of each agency's operational environment, and help me to understand their compliance risks and anticipate future areas of risk. They also provide a forum to reach a view on issues informally, where that is appropriate, without the need for extended and time-consuming formal processes.

As noted elsewhere in this report, I also met regularly with the GCSB/OIGIS Working Group, which was set up to assist the previous Inspector-General, but has evolved into a wider forum for discussion of technical issues, new developments, current or emerging risks, and how the Bureau proposes to respond to them.

In addition, in this reporting year I initiated an NZSIS/IGIS Liaison Group which meets regularly, also for the purpose of discussing current inquiries and reviews as well as emerging matters and risks.

Inquiries

The Inspector-General is mandated to carry out inquiries, on the Inspector-General's own motion, at the request of the Prime Minister, or Minister, or as the result of a complaint by a New Zealand person, by any current or former employee of the agencies or by the Speaker of the House of Representatives on behalf of one or more members of Parliament. All inquiries must be notified on commencement to the chief executive of the relevant intelligence and security agency and, where it is an own-motion inquiry, to the Minister. Where the inquiry stems from a complaint a copy of the complaint must be provided to the chief executive of the relevant agency.

The IGIS Act establishes certain immunities and protections for witnesses before an inquiry and provides for the use of strong coercive power, such as the power to compel the production of documents and information, to issue notices to attend before the Inspector-General to answer questions and to give evidence under oath or affirmation. Every inquiry is conducted in private. If at any time it appears that there may be sufficient grounds for making a report or recommendation that may adversely affect either the agency or an employee or any other person, they are given an opportunity to be heard.

The proceedings, reports and findings of the Inspector-General are challengeable only for lack of jurisdiction.[24]

The Inspector-General must prepare a written report, containing conclusions and recommendations, at the conclusion of each inquiry. The report is provided to the chief executive of the relevant agency, the Minister and, where relevant, the complainant. With the exception of reports relating to employment or security clearance matters, and any parts of each report that I consider necessary to classify and withhold from public disclosure on national security grounds, the report must be made public on the IGIS website.

Except where the IGIS report relates to an employment matter or a security clearance issue, the Minister must provide a response to the Inspector-General and relevant chief executive and may provide a response to the Intelligence and Security Committee.

The Inspector-General may also report to the Minister on compliance by the agency with his or her recommendations and on the adequacy of any remedial or preventative measures taken by the agency following the inquiry. My office will publish recommendations and the agencies' actions in response to those recommendations.

Inquiries at the request of the Minister or the Prime Minister

There were no inquiries requested by the Minister or the Prime Minister in this reporting year.

Inquiries into complaints by the Speaker

There were no complaints made by the Speaker in this reporting year.

Inquiries into complaints by New Zealand persons or agency employees

Superannuation

A complaint was received by a former employee of the GCSB concerning its delay in responding to the complainant's request for corrected information regarding his previous salary. The complainant required this information for superannuation purposes and referred me to a previous investigation carried out by a former Inspector-General, the Hon Paul Neazor CNZM, where he had addressed the underlying general issue relating to the complainant's particular request.

The matter was satisfactorily resolved by discussion with the Bureau's Director, without the need to commence a formal inquiry into the complaint.

Application for work visa

I received a complaint about the NZSIS's recommendation to Immigration New Zealand (INZ) that the complainant not be granted a visa to work in New Zealand. The NZSIS is mandated to make such recommendations under s 4 (1)(bc) of the NZSIS Act to the extent that there are circumstances in any particular visa application that are relevant to security. These recommendations contribute to INZ's good character assessment of visa applicants. While NZSIS may make recommendations, it is the INZ's decision to grant or deny a visa application.

[24] IGIS Act, s 19(9).

My inquiry into this complaint is almost complete. Some detail of this inquiry, which concerns sensitive information, may not be able to be released publicly.

Inquiries following complaints over NZSIS security clearance assessments

In the reporting year, I received eight initial complaints and queries concerning security clearance matters and commenced four inquiries as a result. Of the other four, three related to security policies applied by employers, rather than actions of NZSIS, and so were outside my statutory jurisdiction. The fourth requested that I reopen a previously concluded inquiry, which I considered but declined to do.

Under s 25A(2)(e) of the IGIS Act, I may not publish specific information from the inquiries into individual complaints concerning security clearance and employment matters. In summary, however:

- Three related to the refusal of a security clearance recommendation and one to the making of a "qualified" clearance recommendation. A qualified clearance is a security clearance at a lower level than sought and/or that is subject to conditions.[25]

- Three of the complainants were, prior to the adverse recommendation, employed in positions that required security clearances and all lost their employment as a result. The fourth was a prospective employee whose offer of employment was withdrawn as a result of the adverse recommendation.

- In the course of these inquiries, I identified systemic shortcomings in the procedures followed by the NZSIS. I have discussed those shortcomings and steps taken by my office and by the NZSIS separately below.

For the four inquiries, I proceeded from an initial assessment of the complaint as received to an investigation of NZSIS records and interviews of responsible staff, before preparing an inquiry report. At the end of the reporting year, I had prepared reports on three of these inquiries and had provided them for comment to the NZSIS, as required by s 19(7) of the IGIS Act.

The process of preparing and finalising those reports has been more protracted than I would have wished because of the time required for my office and for NZSIS to work through the systemic issues that I had identified.[26] However, I anticipate finalising all four current inquiry reports in this calendar year.

Procedural fairness obligations in NZSIS security clearance practices

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.[27] In several of the inquiries into individual security clearance assessments undertaken in the reporting year, I identified a recurrent question of whether the procedures followed by NZSIS in making its assessments and recommendations were consistent with the

[25] See New Zealand Government, *Protective Security Requirements* [5.1].

[26] My overall conclusions on those systemic issues are set out in the following section.

[27] NZSIS Act, s 4(1)(bb).

legal obligation of procedural fairness. That question had also been identified by previous Inspectors-General since at least 2008.

The NZSIS role is a significant one:

- A security clearance assessment is a critical safeguard for national security information. If NZSIS fails to identify that a candidate presents security vulnerabilities, there is a risk that information may be disclosed and national security harmed.

- An adverse or qualified security clearance assessment will in most instances have severe consequences for the individual concerned, both in the form of loss or denial of employment and in the loss of reputation and harm to professional and personal relationships. Such an outcome may also deprive the individual's organisation of a key staff member. While the Director's powers are recommendatory only, in practice the expectation is that a chief executive of an employing agency would not lightly decline to follow the Director's recommendation.

Further, the assessment of security clearance candidates is a significant aspect of the NZSIS's functions. There are, at any given time, some thousands of people who require New Zealand government security clearances in order to retain their employment. Staff responsible for security clearance assessments comprise approximately a quarter of the NZSIS.

Relevant legal obligations and comparative security agency practice

The obligations that apply to security clearance assessments are well-settled in caselaw[28] and are clearly reflected in the practice and procedure of other comparable jurisdictions, including Australia, Canada and the United States.[29] The three core obligations on NZSIS are:

- To obtain all available relevant information, taking all steps that are reasonable in the circumstances.

- To analyse all of that information – positive and negative – thoroughly and in a reasoned and objective way, considering reliability and relevance to potential security vulnerabilities. Where issues that require expert judgement arise, it must obtain appropriate expert assistance.

- In the event of a possible adverse or qualified assessment, to disclose all adverse information that it may rely upon and all adverse inferences that it proposes to draw, to the candidate and give the candidate an opportunity to respond.[30]

---

[28] *Greene v McElroy* (1959) 360 US 474, 508; *Thomson v Canada* [1992] 1 SCR 385, 402; and *Home Office v Tariq* [2012] 1 AC 452, [27].

[29] United States Government, *Directive 5220.6: Defense Industrial Personnel Security Clearance Review Program* [4.3]; Australian Government, *Personnel Security Guidelines: Vetting Practices* [6.1]-[6.2]; and Canada, *Standard on Security Screening* Appendix D, 2.

[30] In certain exceptional circumstances, it may be permissible not to disclose particular adverse information: in such cases, NZSIS is subject to an additional obligation of utmost good faith in investigating and assessing the thoroughness and reliability of that information before relying upon it.

My office's inquiries into individual complaints and review of overall NZSIS practices identified that NZSIS did not always obtain all reasonably available information. While NZSIS undertook certain routine record-checking, such as Police and credit rating checks, it principally relied upon information provided by candidates and by referees, both those nominated by the candidate and others (non-nominated referees) whom NZSIS identified as likely to provide information relevant to potential security vulnerabilities. It did not, in general, seek relevant documentary records, such as employer files where a concern over workplace conduct had arisen.

NZSIS did undertake some assessment of the reliability and relevance of information obtained. Security clearance assessments were made as a series of written recommendations by responsible officers for review by more senior staff. Recommendations were, on some occasions, questioned or sent back.

However, NZSIS did not generally take steps to investigate possible bias (positive or negative) towards a candidate and the decision-making record was often not commensurate with the gravity of these decisions. Where matters of expert judgement arose, NZSIS officers sometimes sought expert assistance, but on other occasions were left to rely upon their own non-expert assessments, for example in relation to clinical judgements and to financial audit matters. It did not disclose adverse information or inferences to candidates for response.

For the most part, these shortcomings reflected NZSIS practice, rather than errors made by individual NZSIS officers, who were attempting to comply with NZSIS practices as they understood them, sometimes with inadequate resources and in the absence of adequate guidance. I acknowledge the difficulty of the task faced by NZSIS vetting staff and their desire to do the best possible job.

Steps taken

After a series of discussions with NZSIS vetting and legal staff, the Director agreed that it was necessary to make changes to NZSIS practices. In future NZSIS will:

- obtain all reasonably available relevant information;
- ensure an appropriately full record of the reasoning on which the decision is based; and
- disclose adverse allegations and inferences to candidates and provide an opportunity to respond, other than to the extent that a specific legal exception to that obligation applies to particular information.

I welcome the Director's commitment to effecting the necessary changes.

Outcomes for complainants

In the individual complaints that I have received during the reporting period, I have considered whether the inconsistency between NZSIS practices and procedural fairness obligations meant that the security clearance assessment was unsound, taking account of the particular content of that assessment. Where I have found that the assessment was unsound, I have identified appropriate remedies under s 11(6) of the IGIS Act. As one part of those remedies, I am pleased

to acknowledge the agreement by the Director of the Service to give apologies to affected individuals.

Inquiry into complaints regarding GCSB activity in the South Pacific

In March 2015 various New Zealand news media published allegations that the GCSB had undertaken communications interception activity in the South Pacific. These allegations followed the publication by news media outlets of alleged classified NSA documents released by Edward Snowden. Following the March 2015 New Zealand media publications I received complaints from several individuals alleging possible personal adverse effect on account of the alleged activities, or complaining more generally about alleged activities of the GCSB in the South Pacific.

I concluded that some of the complaints raised the possibility that the complainants had, or may have been, adversely affected by an alleged act, omission, practice, policy, or procedure of the GCSB[31] and on 25 March 2015 I commenced an inquiry into those complaints.[32]

A small number of complainants did not agree to a copy of their complaint being provided to the Director of the GCSB upon commencement of my inquiry.[33] Although this has meant I have been unable to inquire into the specifics of their complaints, the general questions they raised are encompassed within the inquiry.

With respect to each complaint of adverse effect that I have been able to inquire into, I have sought to investigate and consider whether communications from or to the complainants was or may have been collected by the GCSB while the complainants were at relevant South Pacific locations during specified time periods. In exploring those heads of specific inquiry, I have also sought to identify, more generally, the GCSB's current (and some former) collection practices and procedures, including how it gives effect to legislative safeguards, as well as current procedures and arrangements for sharing and retention of communications data.

As I noted at the time of announcing this inquiry, I have undertaken the inquiry into these complaints in the context of my broader review power. I anticipate that public reporting on the inquiry/review, while having due regard to the requirements of security, will provide the public with more information about the Bureau's functional activities, the legal framework within which it must operate, the legislative and policy safeguards that are in place and how the Bureau operates within those limitations.

As at the end of this annual reporting period work on this inquiry is continuing. I expect to be able to report on the inquiry in this calendar year.

Other complaints

Privacy Act complaints

No Privacy Act complaints were received by the Inspector-General during this reporting period.

---

[31] IGIS Act, s 11(1)(b).

[32] As well as inquiring into the individual complaints this work encompasses a broader review of GCSB collection, retention and sharing of communications data, and controls on such activity (see below).

[33] As required by s 19(1)(b) of the IGIS Act.

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 whistleblowers policies

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

In February 2015 the Inspector-General received a media enquiry regarding the number of protected disclosures received by the office of the Inspector-General in the preceding ten years. On review of the files held by the office it appears that no protected disclosures were received by any of the Inspectors-General in that 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 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 Office of the Inspector-General has not previously had a formal policy for dealing with protected disclosures. We have now developed a policy, which includes:

- how protected disclosures are to be handled by IGIS staff;
- how an employee of the NZSIS or GCSB may make a protected disclosure;
- what constitutes a protected disclosure;
- the definition of 'employee';
- what confidentiality assurances the Inspector-General can provide; and
- the protections afforded to 'whistleblowers' and the limits on these.

The GCSB and NZSIS are cooperating to develop a shared policy and common procedures for protected disclosures for the New Zealand Intelligence Community as a whole. My office is consulting with both agencies to ensure that there an appropriate interface between my office and the agencies for my office to have access to information and personnel, in the event of a protected disclosure.

Own-motion inquiries

Criteria for own-motion inquiries

I may initiate an inquiry into any matter that relates to the compliance by the GCSB or the NZSIS with the law of New Zealand or into the propriety of particular activities of one of the agencies. "Propriety" is not defined in the IGIS Act, 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.

The factors I consider when deciding whether to start 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?

I initiated the following own-motion inquiries during the reporting period.

Inquiry into the Government Communications Security Bureau's process for determining its foreign intelligence activity

I commenced this inquiry in response to the issues that were raised early in 2015 around a bid by the Hon Tim Groser MP, the Minister of Trade, to become Director-General of the World Trade Organisation. I explained at the time that while it is unlikely that I will be able to publicly confirm or deny the specific allegations relating to the bid, I would in any case inquire and report more generally into how the GCSB determines, within its statutory constraints, what foreign intelligence activity to undertake and what policies and procedures are in place to regulate its activities.

The work on this inquiry is progressing well and I hope to be in a position shortly to publish an unclassified report that will address these issues.

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

On 9 December 2014, the US Senate Committee on Intelligence published redacted findings, 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.

A number of other countries involved with the detention and interrogation programme were identified by the US Senate Committee Report but the names of those countries have been redacted. There have also been official statements by intelligence agencies, inquiry findings and allegations made about various instances and/or risks of engagement with the CIA programme by a number of governments, including those of Australia, Canada and the United Kingdom.

As a result of the Senate report and related material, I identified a public interest in inquiring into whether New Zealand's intelligence agencies and personnel knew or were otherwise connected with or risked connection to the activities discussed in the US Senate Report. To address that interest, I commenced an own motion inquiry. My decision to do so does not suggest or presuppose that New Zealand agencies or personnel were in any way connected with those activities.

My inquiry, which is ongoing, includes an examination of whether there was any such engagement by the New Zealand intelligence and security agencies and whether there were and/or now are any safeguards in place or other steps taken to address any connection or risk of connection to such activities. To date, my inquiry has reviewed numerous intelligence community documents and is in the process of interviewing both past and present staff of the Bureau and Service who may have relevant knowledge and experience, and the agencies have assured me of their full cooperation. I also anticipate that members of the public who have any relevant information may approach my office.

My intention in this inquiry is to provide, so far as possible, clarity around past events and to assess relevant standards then and now in place. It is important for the confidence not only of the New Zealand public, but also for any staff from the intelligence and security agencies who are required to work in complex and difficult environments, that there is appropriate guidance about the legal and ethical standards required of them.

Reporting on own-motion inquiries carried over from 2013/14

Review of complex/sensitive category of Service warrant applications

In early 2014, the previous Inspector-General commenced an inquiry into a category of NZSIS warrant applications, made and granted in that reporting year, that appeared to be relatively complex and sensitive. I will conclude and report on that inquiry before the end of this calendar year. Within the reporting period, however, I made several provisional findings and recommendations and those findings and recommendations have been accepted by NZSIS, so are appropriately set out here.

I have found that much of the relevant operational detail was and remains sensitive, and would cause harm to national security if publicly disclosed. It is therefore not included in this report. Even without going into that detail, however, it is possible to give an account of the inquiry, the problems identified and changes made.

The starting point is that whenever NZSIS seeks a warrant, it must do so in full and fully reasoned terms, disclosing all relevant information and setting out how the NZSIS believes that the requirements for the issue of a warrant are met.[34] That task was particularly demanding for this category of warrant applications because:

- The relevant warrant applications related to information-gathering that had been proposed and undertaken in cooperation with other agencies. Some of the intelligence material sought under the warranted activities was principally useful,

[34] NZSIS Act, s 4A and also, for example, *R v Williams* [2007] 3 NZLR 207 (CA), [224](b), (k), (l) & (m) (warrant application must be as specific as the circumstances allow; must disclose all relevant information and give reasons for any statement of belief; and set out how the application meets the statutory criteria).

at least in a direct sense, to those other agencies rather than to the NZSIS itself. NZSIS may cooperate with other public agencies, whether in New Zealand or elsewhere, "as are capable of assisting … in the performance of its functions": that is, such cooperation must serve the functions of NZSIS and is not an end in itself;[35]

- The involvement of other agencies was also relevant to an assessment of whether the material sought was necessary to NZSIS for the purposes of security[36] and whether its value justified the proposed warranted activities; and

- The warranted activities carried risks of unusually serious and uncertain adverse consequences in the event of disclosure of those activities or of the material obtained.

I reached three provisional conclusions in my investigation of these warrant applications.

First, the warrant applications did, in broad terms, establish the need for and value of the information that would be gathered under the warrants and set out the risks of the proposed warranted activities. Under the NZSIS Act, that is necessary in order to enable those involved in authorising the warrant, to make their respective assessments.[37]

Second, further relevant information was available to the Service, but was not included in the warrant applications. The applications also lacked a sufficient assessment of the connection between the activity for which each warrant was sought and the requirements of the NZSIS Act, particularly in relation to the cooperative nature of the activities proposed in the warrant application. There were therefore risks that, if that additional material and a more robust assessment had been provided:

- the application might not have in fact met the statutory criteria; and/or

- those involved in authorising each warrant might have reached different conclusions on these applications.

In order to address those risks, I reviewed relevant background materials, required NZSIS to compile the further relevant information and considered that information against the statutory criteria. I concluded that while the warrant applications should have included that further information and provided a more robust assessment of that information, it would nonetheless have been open to the Minister and, where required, the Commissioner to issue the warrants as sought. In particular, while the further information permitted a more detailed and more focused basis for the applications, it did not contradict what had been put before them.

I advised the Minister and NZSIS of these provisional conclusions and the Commissioner of Security Warrants was also informed. I made recommendations that any future warrant application of this kind should include the fuller information that I had identified and more robust assessment of that information. NZSIS has accepted the conclusions and recommendation and has acted on the recommendation in applications for new warrants in this

[35] Contrast s 8C of the GCSB Act, which permits the GCSB to provide assistance to other agencies in the pursuit of their functions.

[36] NZSIS Act, ss 2(1) and 4A(3).

[37] NZSIS Act, ss 4A(3)-(4) and 4B.

category made after the end of the reporting period. I will comment on those new warrant applications in my inquiry report.

Inquiry into warnings given by NZSIS officers

In June 2014, I commenced an own motion inquiry into the giving of warnings by NZSIS officers to members of the public. My decision to commence that inquiry arose from significant concerns raised by my predecessor, the Hon Andrew McGechan QC, in his report dated 28 May 2014 concerning complaint 2013/2014-1.[38]

I had expected to conclude that inquiry in the course of this reporting year, but have not been able to do so. Operational demands, personnel changes and inadequate record-keeping practices around operational decisions and actions have posed difficulties for the NZSIS in responding. This is an unsatisfactory outcome. Warnings are a potentially useful tool: if the Service can, by an appropriately framed statement to one or more members of the public, prevent a threat to national security, that may be of real benefit. However, it is important to clarify the legal parameters of such warnings: the intended and/or unintended impacts of an overt statement by NZSIS upon the recipient are potentially significant and the practice involves an overt action that may expose the Service to practical and/or legal risk.

I will report on this inquiry before the end of the calendar year.

General reviews

During the reporting year my office began three reviews of specific areas of operational activity, as part of our ongoing review of the compliance systems of the NZSIS and the GCSB.[39]

GCSB activity in the Pacific

The complaints into GCSB activity in the Pacific[40] also raise wider questions regarding the legality of the GCSB's practices in the collection, retention and sharing of data and the controls on those activities. In order to address those wider questions, I decided to carry out the inquiry into the specific complaints within the broader context of my programme of review of GCSB procedures and compliance systems under s 11(1)(d) of the IGIS Act.

I will report on those wider questions at the same time as I report on the outcome of the specific complaints.

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

On 27 January 2015 I commenced a review of the Service's systems for storing, using and controlling access to information that the NZSIS compiles for the purpose of assessment of candidates for New Zealand government security clearances (known as vetting).

The review was undertaken for four reasons:

---

38 Available at http://www.igis.govt.nz/publications/investigation-reports/.

39 Under s 11(1)(d)(ii) of the IGIS Act.

40 See above, p 18.

- the scale of security clearance vetting undertaken by the NZSIS;
- the breadth and sensitivity of information potentially relevant to security clearance decisions;
- the exceptional scope of information-gathering for security clearance procedures; and
- the need for clarity around any use of security clearance information for any other purpose.

My review examines the Service's practices and safeguards governing the secure storage, accessibility, and use of information about security clearance candidates.

Since I commenced the review, the need for confidence and clarity in the security of such information has been highlighted by the disclosure that the United States' systems for its security clearances were the subject of a reported data breach of personal details of more than 22 million people compiled from background checks over at least 15 years.

As at the end of this annual reporting period work on the review is continuing. I expect to be able to publicly report on the finding of the review before the end of this calendar year.

Access to passenger/border control data

During the reporting period my office has been in discussions with the NZSIS about NZSIS powers to access data obtained under the Customs and Excise Act 1996 and the Immigration Act 2009. That issue in part arose from an initiative by NZSIS and in part from the enactment of an information access provision in the Customs and Excise Act as part of the urgent 2014 amendment. The Office of the Privacy Commissioner has also been part of the discussions regarding Immigration Act data.

The point of the discussions is to ensure that – as with other public agencies' information sharing – there should be a clear and properly regulated regime where it is necessary for NZSIS to access another agency's data. I expect this review to be concluded within the calendar year.

Implementation of recommendations: inquiry into release of NZSIS Information

One of the measures of effectiveness of the work of the Inspector-General's office is the extent to which the agencies, Ministers and complainants accept and act on the Inspector-General's findings and recommendations. The IGIS Act provides for me to report on compliance by the intelligence agencies with recommendations and on the adequacy of any remedial or preventative measures taken.

In November 2014, I reported on my inquiry into the release of certain information by the NZSIS under the Official Information Act 1982.

In my report, I had found that the information released was incomplete, inaccurate and misleading and that the NZSIS process for handling OIA requests was inadequate. In relation to the issue of political neutrality, I had not found any partisan political motive on the part of the NZSIS or its Director, but I did find that a number of errors of judgement were made which resulted in failures to take all reasonable steps to safeguard the political neutrality of the NZSIS as required by s 4AA(1) of the NZSIS Act. I had also found that the Director and senior staff of the NZSIS did not act with propriety in that they failed to recognise the gravity of the controversy arising from the release of the information and the potential for political exposure and failed to engage appropriately with the Leader of the Opposition and with the Prime Minister's Office.

The full findings of my inquiry and recommendations have been made public and are available at www.igis.govt.nz.

As part of our review work, I have monitored the responses by the Service to the recommendations in the inquiry report. I am satisfied with the implementation of the recommendations to date.

I am also pleased to report that the Service has taken several significant remedial steps with wider implications. For example, I had found that critical decisions within the scope of this inquiry were not, or not clearly, recorded and had likely suffered as a result and, in response, the Service has taken initiatives to improve recording of all significant decision-making.

Recommendation One

NZSIS should work with the Office of the Ombudsman to ensure that relevant NZSIS staff have a full understanding of, and training on, the substantive and procedural requirements of the Official Information Act 1982

NZSIS staff involved in Official Information Act (OIA) requests undertook training with the Office of the Ombudsman. The training covered the fundamental aspects of the OIA and the Privacy Act 1993.

A shorter OIA information session was also developed. This was presented to staff at an NZSIS all staff meeting in June, with a copy posted on the intranet for future reference. All new staff will receive an OIA information session as part of their induction programme.

Recommendation Two

NZSIS should review its structures and processes, in consultation with the Office of the Ombudsman and with an opportunity for comment to those individuals and news organisations who made Official Information Act requests here, to ensure that there is a consistent and workable approach to OIA requests and media inquiries

The NZSIS process for managing OIAs was reviewed and revised. The new management process, which includes a central register of all official information requests, has been operating since February 2015, with further enhancements (eg electronic workflow management) to be piloted from July 2015. An additional Official Information Advisor role has been created to assist with managing all information requests. An additional principal advisor position was also to be appointed after the reporting year.

NZSIS is reviewing its policy for requests made under the OIA and the Privacy Act and provided a draft for consultation to the Office of the Ombudsman and Office of the Privacy Commissioner in May 2015.

The New Zealand Intelligence Community communications staff, within the Department of the Prime Minister and Cabinet, has consulted affected media outlets (and current media contacts) on the new management process.

A combined NZSIS/GCSB official information report is also prepared on a weekly basis for the information of the Directors, DPMC and the Minister. NZSIS and GCSB also meet to coordinate official information issues, with assistance from NZIC communications staff.

Recommendation Three

NZSIS should work with GSCB, SSC, DPMC and others, to develop written guidance for ministerial office staff who deal with intelligence and security matters, on issues such as media comment, information security and political neutrality

NZSIS established the Protective Security Requirements (PSR) engagement team in late 2014 which is mandated by Cabinet to implement information security aspects of the PSR across the government sector.

Specific guidance for other parliamentary offices involved in the handling of NZIC information, classified or otherwise, was drafted during the reporting period but is now being further reviewed in conjunction with Department of Internal Affairs work on oversight of political advisors. This guidance will provide those working in Ministerial offices and the Leader of the Opposition's office, with clarity around the exceptional obligations of political neutrality that apply to the NZSIS and GCSB. The guidance also makes explicit the expectations on Ministerial staff in respect of those obligations.

Recommendation Four

NZSIS, together with the GCSB and DPMC, should consider locating a departmental adviser (representing the Intelligence Community) in the Prime Minister's office and/or in the Policy Advisory Group in DPMC, to be the principal point of liaison between the Intelligence Community and the Minister's office, and should work with SSC to develop best practice guidelines for those advisers

The position of NZIC Private Secretary has been established in the office of Hon Christopher Finlayson (as Minister in Charge of the NZSIS and Minister Responsible for the GCSB). The Private Secretary has been provided with State Services Commission's written guidance on political neutrality. In addition, the SSC has provided a mentor to the NZIC Private Secretary.

Recommendation Five

The Director should work with the Office of the Leader of the Opposition, in consultation with the responsible Minister, to set express expectations for consultation with the Leader of the Opposition. These expectations should include provision for the Leader of the Opposition to have secure access to classified material and for a member of the Leader of the Opposition's staff (with necessary security clearance) to attend consultation meetings

NZSIS has agreed a letter of engagement with the Leader of the Opposition that establishes, amongst other things, arrangements for a monthly meeting between the Leader of the Opposition and the Director, the continued attendance of others at that meeting, and provision for the handling and storage of classified information.

Recommendation Six

NZSIS should work with the GCSB, with such assistance as is appropriate from the SSC, the DPMC and others, to develop published guidelines on the political neutrality obligations in s 4AA of the NZSIS Act 1969 and s 8D of the GCSB Act 2003

Guidance on political neutrality has been developed for NZSIS staff, drawing on SSC advice, that will be published following consultation with the NZSIS Staff Association. GCSB provided advice to its staff shortly after the end of the reporting period.

Recommendation Seven

NZSIS, together with the broader Intelligence Community and SSC, should consider whether, as part of the Intelligence Community's leadership development, increased opportunities can be identified for secondments of Intelligence Community staff into the wider State Services and vice versa, to facilitate a broader understanding of the state services and of the political environment in which state servants carry out their role

Wider engagement by the NZIC is already a component of professional development and career development for staff. Some key activities underway include:

- SSC Career Development Boards are run as an initial step to identify talent within the wider government sector;
- tier 2 and 3 managers are considered through an internal career development board to identify high performers; and
- action learning groups at tier 2 promote learning and engagement within the broader NZIC.

NZSIS also seconds staff both into and out of the organisation. Agencies NZSIS commonly engages with in this way include DPMC, GCSB, NZ Customs Service, NZ Police, Immigration NZ, and the Aviation Security Service.

Recommendation Eight

NZSIS should provide an apology to the Hon Phil Goff for failing to adequately consult him in relation to Mr Cameron Slater's Official Information Act request; for releasing incomplete, inaccurate and misleading documents relating to the meeting between Mr Goff and the former Director on 14 March 2011 and for failing to recognise and seek to correct the harm that ensued from those errors

The Director of the NZSIS made a formal apology to the then Leader of the Opposition, Hon Phil Goff, and to current Leader of the Opposition, Andrew Little on 25 November 2014. The Director also apologised to the Prime Minister for NZSIS's shortcomings.

Warrants and authorisations

Regular review of warrants and access authorisations

An integral part of the IGIS office work programme[41] is the timely review of:

- all interception warrants, access authorisations and Director's authorisations issued under sections 15A and 16 of the GCSB Act; and
- all domestic and foreign intelligence warrants issued under s 4A, visual surveillance warrants under s 4IB and emergency authorisations made under s 4ID of the NZSIS Act.

These reviews provide both a general means of overseeing significant parts of the activities of both agencies and, more specifically, confirmation that the agencies have met their statutory requirements:

- the responsible agency has, in each case, established in seeking or making the warrant or authorisation that it is for the purpose of performing one of the agency's statutory functions and otherwise complies with the criteria under the relevant Act;
- where required, the warrant or authorisation has been issued by the responsible Minister, by the Commissioner of Security Warrants or the Director, on the basis of an application made in accordance with the relevant Act;
- where consultation with the Minister of Foreign Affairs is required, that has taken place;[42]
- the requirement that the GCSB does not target New Zealand citizens or permanent residents for intelligence-gathering purposes is complied with or, where an exception to that requirement applies, the exception is made out;
- in relation to NZSIS foreign intelligence warrants, the requirement that no New Zealand citizen or permanent resident is subject to the warrant is complied with;
- where applicable, how each agency ensures that the impact of the warrant or authorisation on third parties is minimised;
- where applicable, how the destruction of irrelevant records obtained by interception or tracking occurs as soon as practicable; and
- other applicable requirements of the relevant Act, such as avoiding interception of privileged information, are addressed.

My office reviews these aspects of each warrant and authorisation, as well as any other concerns, as recorded in a standard template that we have developed. Where an issue or concern is identified in respect of a warrant or authorisation:

---

[41] IGIS Act, s 11(1)(d)(i): to review the effectiveness and appropriateness of the procedures adopted by each intelligence and security agency to ensure compliance with its governing legislation in relation to the issue and execution of warrants and authorisations.

[42] The Minister responsible for the GCSB must consult the Minister of Foreign Affairs before issuing an interception warrant or an access authorisation: GCSB Act, s 15A(3). The Minister in charge of the NZSIS must consult the Minister of Foreign Affairs about a foreign intelligence warrant where it is concerned with the identification of foreign capability, intentions, or activities within or relating to New Zealand that impact on New Zealand's international well-being or economic well-being.

- we undertake any further investigation that is necessary, for example reviewing any further relevant information held by or available to the agency;
- we raise the issue or concern with the responsible agency for its response; and
- I then consider the response and advise the agency and, where necessary, the responsible Minister, if in my view the warrant or authorisation should be rescinded, reviewed or subjected to conditions.

Both the GCSB and the NZSIS have procedures and practices that apply to the development of an application for a warrant or access authorisation. These procedures include checks of much the same matters as addressed in my office's template review.

However, there are inevitably questions that require closer analysis whether, for example, around new practices or issues – as noted below, we are undertaking a thorough review of the first exercise of the new visual surveillance warrant power – and around some systemic issues that deserve careful scrutiny.

Understanding and resolving the underlying issues is, necessarily, time-consuming. I am grateful to the Directors of both agencies and their staff for providing necessary assistance to my office to understand the technical issues related to our questions and their openness to discussing our substantive concerns. The Directors have also indicated their appreciation of the perspective and, where I have found change to be required, opportunity for reform afforded by such reviews. A specific instance of constructive engagement over one such difficult question is set out at page 21.

In addition, as at the end of this reporting period, my office is working through a range of questions over various warrant and access authorisations and it is instructive to set these out here. These questions do not indicate an adverse conclusion on my part. Once we have concluded the process of information-gathering and engagement with the responsible agency, I will report on the conclusions reached.

GCSB

During the reporting year my office reviewed 15 interception warrants in force in the reporting year; 26 access authorisations issued under s 15A of the GCSB Act during the year; and two Director's authorisations issued under s 16.

Interception warrants and access authorisations

The current areas of focus that have arisen from the review of warrants and access authorisations include the following:

- Whether there are appropriate safeguards to ensure that the actions carried out under an interception warrant or access authorisation do not go beyond what is necessary for the proper function of the GCSB.[43]
- Whether there are satisfactory arrangements in place to ensure that the nature and consequences of the work carried out are reasonable with regard to the purposes for which it is carried out.[44]

[43] GCSB Act, s 15A(2)(d).

[44] GCSB Act, s 15A(2)(e).

These questions relate to issues such as whether the scope of a warrant is proportionate and whether the arguments for targeting particular people or groups of people are sufficiently robust. They also require a balancing of the impact of the warrant or access authorisation on subjects with the purposes of a warrant.

- How personal data which is not the subject of a warrant or access authorisation is protected. This question can arise in relation to different aspects of the application, including circumstances where applications need to take particular care to identify clearly for the Minister and, where required, the Commissioner of Security Warrants, the risks of intercepting the communications of New Zealanders and the steps the Bureau intends to take to minimise those risks.
- Whether the Minister and, where required, the Commissioner, are adequately informed about the proposed mechanisms to minimise the impact of the warrant on third parties and the steps that will be taken to ensure that irrelevant records are destroyed, as required by the GCSB Act.

Director's authorisations

In addition to Ministerial interception warrants and access authorisations, the Director of the GCSB has 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.[45] That provision applies, 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.

Waihopai (a satellite communications interception station) and Tangimoana (a high frequency radio interception and direction-finding station) are covered by Director's authorisations.

The Director may 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 does not require that such authorisations be in writing, although the Bureau's practice is that they are written. Nor are s 16 authorisations subject to the additional, more substantive criteria that apply to interception warrants and access authorisations.[46]

The two s 16 authorisations that I reviewed during this reporting year were clear that they did not authorise s 15(1) activity and were for the purposes of furthering the Bureau's functions under ss 8A and 8B. The authorisations set out applicable controls to guard against the

[45] See sections 15(1) and 16(3) GCSB Act.

[46] 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.

interception being for the purpose of intercepting private communications of a New Zealander[47] and to minimise the impact of interception on third parties.[48]

The authorisations also detailed controls around submission and validation of collection requirements, including a requirement to enter auditable justifications for collection decisions, and other controls on access to the information collected. While there is a broader legislative policy question as to whether such interception activity ought to be subject to Ministerial oversight, I was satisfied that the current s 16 authorisations meet the requirements of the Act and include a range of material protections.

NZSIS

During the reporting year my office reviewed the 29 domestic intelligence warrants issued during the reporting period, as well as all of the foreign intelligence warrants, issued under s 4A of the NZSIS Act.[49] Two domestic visual surveillance warrants were issued during the reporting period and were also reviewed, as noted further below. No urgent or emergency authorisations for warrantless surveillance were issued by the Director within the reporting period.

As with the GCSB, we have raised a range of matters in the course of inspection of all warrants issued and from in depth, "end-to-end", reviews of a sample of warrants.

As a result of our review in the reporting year, we are pursuing a range of questions. As noted above, these questions do not indicate an adverse conclusion:

- How the NZSIS has demonstrated in its warrant applications and the process leading to those applications that there are reasonable grounds for believing that no New Zealand citizen or permanent resident will be identified as a person subject to a proposed warrant, such that the Minister can issue a foreign intelligence warrant,[50] without the need for parallel approval by the Commissioner of Security Warrants.

- How the NZSIS has proposed to minimise the impact of an intelligence warrant on a third party and how it has informed any assessment by the Minister and, where required, the Commissioner, as to whether to include conditions in a warrant to minimise that risk.[51]

- How the NZSIS establishes in its warrant application that the communication sought to be intercepted or seized under the proposed warrant is not privileged as defined by the NZSIS Act, including how any unforeseen interception or seizure of

---

47 GCSB Act, ss 14 & 16(1A)(b) & (3).

48 GCSB Act, s 24.

49 I intended to note in this report the number of foreign intelligence warrants issued. The Director requested that I not do so. Although the Director must include in every annual report the number of domestic intelligence warrants in force in the reporting year, there is no corresponding requirement in respect of foreign intelligence warrants. The Director's view is that to publicly disclose the number of foreign intelligence warrants in force raises issues both of legislative intent and of possible security or international relations risks that require further discussion and I have therefore agreed not to disclose that number for this reporting year, pending that discussion.

50 NZSIS Act, s 4A(2)(b).

51 NZSIS Act, s 4B(4).

privileged material is to be identified and resolved.[52] This includes circumstances relating to legal professional privilege and religious privilege.

- Where renewal of existing warrants is sought, how the information, if any, gathered under the previous warrant bears on the warrant application, including establishing the necessity for the proposed renewal and the time-frame sought.

First NZSIS visual surveillance warrants

Provision for visual surveillance warrants, including requirements for a copy of each warrant to be provided to this office as soon as practicable, was introduced in December 2014.

Two visual surveillance warrants were issued during the reporting period. NZSIS did not initially provide a copy of these warrants to my office.[53] Instead, the warrants and their supporting documentation were subsequently identified as part of my office's regular warrant review process. In response to that incident, NZSIS has now instituted appropriate arrangements to ensure that I am provided with a copy of any warrant issued on the day of issue or on the next working day, if it is impracticable to email on the day of issue. We also took that opportunity to ensure that appropriate arrangements were in place for immediate notification of any authorisation of emergency warrantless surveillance under s 4IE.

As these were the first visual surveillance warrants and because of the intrusive nature of the powers conferred by such warrants, we had committed to undertake an "end-to-end" review of the warrants. I expect to report on that review shortly and will address all of the requirements under the NZSIS Act for such warrants, including the extent to which those requirements – for example, meeting the standard of justification and minimising third party impact – are met in the inherently more intrusive and therefore more stringent context of visual surveillance.

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.[54]

As at 30 June 2014 I had been Inspector-General for seven weeks and was not able to certify that either the NZSIS or GCSB had overall systems which were sound, in whole or to any lesser extent. I noted in the 2013/14 annual report that should not be misconstrued as a statement that the respective systems were unsound.

As at 30 June 2015 I am in a position to make an assessment and certification as the IGIS Act requires.

---

[52] NZSIS Act, s 4A(3)(d).

[53] Section 4IB(9) of the NZSIS Act requires the NZSIS to provide a copy to the Inspector-General "as soon as practicable" after the warrant is issued.

[54] IGIS Act, s 27(2)(ba). See also IGIS Act, s 11(1)(d).

I have applied a "positive assurance" approach. That is, 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 actions. Because of the large volume of decisions and operations, I cannot scrutinise all actions – with the exception of warrants and authorisations – at all times and, in particular, must be selective about those actions 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.

In this work, as in our specific review and inquiry work, I have made full use of the powers of entry and of access to intelligence records, as well as interviewing or meeting with a significant number of agency personnel at all levels. In particular, I have a direct and independent right of access to the Service and the Bureau's ICT systems, documents and employees. This facilitates my inquiry, review and audit functions, and also builds direct relationships with operational staff.

Our objective in applying the certification requirement under the Act is that, if systems are sound, errors will be identified and, once identified, can be addressed both by the agencies themselves and, through reporting, by my office.

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.[55]

As such, 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 shortcomings, that may well indicate inadequacies in internal compliance mechanisms. Further, where compliance mechanisms are robust, that should not only lessen the likelihood of breach, but also support and assist the rigour and transparency of my office's review and inquiry work.

I have described the various compliance systems and steps 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.

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

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 the agencies' wider public, political and legal accountability.

Outline and assessment of GCSB compliance systems

Policy framework

GCSB has an overarching Compliance Policy and a Compliance Management Framework to give effect to that Policy. The Framework was developed as a direct result of the recommendations in the *Review of Compliance at the Government Communications Security Bureau*, March 2013 (the "*Kitteridge Report*"). The Framework is for the purpose of implementing the Bureau's range of corporate and operational policies, including the Legal and Compliance Policy. Operational policies are tiered:

- policy statements which cover the principles of operation are authorised by the Director;
- policy procedures instruct on how those principles will be undertaken and are signed by the relevant Deputy Director; and
- standard operating procedures, which are technical instructions, are approved by the relevant manager.

Compliance oversight structure

The GCSB has an independent Risk and Audit Committee, established by and reporting to the Director to give advice on the Bureau's risk management framework, Assurance System and Framework (including legal, policy and procedural compliance) and Audit system (internal and external). The Risk and Audit Committee currently consists of two former senior public servants and is scheduled to meet quarterly.

The Compliance and Policy Manager has overall responsibility for operational compliance. The Compliance and Policy Auditor, Compliance Advisor and Compliance and Policy Analyst report to the Manager. These roles are part of the Office of the Director. They have responsibility for compliance training, formal compliance reporting to the GCSB Board and the Inspector-General on a quarterly basis, regular compliance reviews, both scheduled (monthly, quarterly and annual) and as and when any compliance matter arises that is of potential concern requiring audit of compliance.

Compliance audit practices

The Bureau has a Compliance Audit Plan which focuses compliance audit activity on the highest risk activities. The Compliance and Policy Auditor implements the Audit Plan, undertaking planned and spot audits of areas of the Bureau's operations. Audits include, but are not limited to review of:

- operational activity to ensure that all activity is consistent with procedure, policy and legislation;
- appropriate access to and use of systems and tools;

- intelligence produced and the provision of such intelligence to customers;
- warrants and authorisations to ensure accuracy with legislative requirements; and
- accuracy of the register of warrants and authorisations.

My office was briefed on the 2014-2015 Audit Plan and on the results of specific audits undertaken during the course of this reporting year.

Self-reporting of incidents

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 a possible breach of a procedure, 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 units 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.

Five incidents were reported to me by the Bureau's Compliance Manager during the reporting year.

- A compliance investigation was carried out by the Bureau into whether the Register of Interception Warrants and Access Authorisations met the statutory criteria.[56] The investigation concluded that not all of the information required had been captured and the register was not set up as a standalone document or a standalone electronic repository (although relevant information could be assembled by running appropriate searches on the document management system). After discussion with my office the necessary changes were made by the Bureau to ensure that all necessary information is captured in the register itself.[57]
- An inadvertent query of New Zealand metadata by a partner agency occurred as the result of a typing error by the responsible partner agency analyst. The results were immediately cleared and no further analysis or reporting on the New Zealand metadata occurred. The analyst self-reported the incident to that person's compliance team and it was then notified to the GCSB by the director of compliance of the partner agency. In view of the swift notification and implementation of remedial steps the GCSB determined that no further action was required. I reached the view that there was no breach by the GCSB of its legislation and policy and that, given the steps taken, no further action was required.
- The third incident involved inadvertent interception by the GCSB of New Zealanders' communications during the course of a regular query. The GCSB analyst identified two communications which were from New Zealanders. The analyst immediately stopped viewing the returns and advised management. All

[56] GCSB Act, s 19(2).

[57] See IGIS Annual Report 2013/14, p 18.

potentially relevant selectors were detasked; no further analysis of the material collected was conducted. The material was retained in the event that I wished to analyse it; when I advised that I did not, it was destroyed. While I am not able to provide further detail of this incident without revealing details of specific operational matters, I was satisfied that the interception was inadvertent, could not have been foreseen and that all appropriate steps were taken by way of cessation of the interception and destruction of the data without further analysis.

- The fourth incident involved inadvertent targeting of the communications of a New Zealand permanent resident by a partner agency. The targeting was not conducted by, or undertaken with the knowledge of the GCSB. GCSB became aware of it when the partner's compliance team reported it to the Bureau. The partner agency advised that appropriate mitigation steps had been taken – the agency's holdings were updated to reflect the individual's New Zealand nationality; reporting arising from the period when that person was targeted was cancelled and relevant SIGINT[58] data from the agency's holdings was deleted. The Bureau Compliance Team determined that there was no breach by the Bureau of its governing legislation or policy as the targeting had been undertaken by the partner agency without its knowledge. I am satisfied that the early detection and self-reporting by the partner agency demonstrated appropriate and robust reciprocal arrangements to detect and rectify such inadvertent breaches. I concluded that no further action was required by the Bureau or by my office.

- The final incident notified to me was a failure by the Bureau to respond to an Official Information Act (OIA) request within 20 working days, in breach of s 15A of the OIA and a divergence from internal draft policy procedure. The Bureau advised me that the cause of the delay was a combination of staff absences and the manual internal process for tracking and responding to OIAs, which resulted in paperwork being mislaid and not followed up in a timely manner. The GCSB is now considering a workflow tool to help mitigate this risk. In light of the fact this was an isolated incident and steps being taken to avoid a recurrence, I determined that no action was required by my office.

Register of warrants and authorisations

The Bureau is required to keep a register of all interception warrants and access authorisations.[59] 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 give assistance in giving effect to the warrant or authorisation.[60]

The Director must make the register available to the Minister or the Inspector-General as when requested and if a warrant relates to the interception of communications of a New Zealand

[58] SIGINT (Signals Intelligence) is intelligence derived from electronic signals and systems.

[59] GCSB Act, s 19.

[60] GCSB Act, s 15E.

citizen or permanent resident, the Director 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.[61]

Interaction with IGIS office

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 and, where necessary, discussing proposed investigative and/or remedial steps with the Compliance and Policy Manager and sometimes the Chief Legal Advisor;
- consultation with my office on novel or likely contentious actions or issues. While, as above, it would be inconsistent with my review and oversight role to provide prior authorisation for particular actions, such consultation does afford an opportunity to avert obvious errors;
- monthly GCSB Security Audit Implementation 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; and
- quarterly 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 of the GCSB and her senior staff, including in regular joint meetings with the Director and senior staff of the NZSIS; and
- consultation on draft policies and procedures.

My assessment

The Bureau's adoption of robust compliance measures means, in my assessment, that errors are promptly identified and that appropriate remedies are put in place. Most policies and procedures are comprehensive and up-to-date and those that are not are under review. There are a range of safeguard mechanisms in place, including training/certification requirements, logging of significant actions and audit of those logs.

Further, from engagement both with managerial and compliance staff and with individual operational staff in the context of reviews and inquiries, Bureau staff are well-directed and

[61] See above, p 29.

supported in meeting their obligations. Legal and compliance advice informs operational activities and there is a strong culture of commitment to compliance and reporting of errors.

Formal institutional measures, staff perceptions and organisational culture must, of course, be verified by end results. To that end, I have reviewed the nature of the incidents and errors that I have identified, both from my office's own reviews and inquiries and from Bureau self-reporting. I consider that the errors that have been identified in the reporting period have reflected inadvertence, unforeseen circumstances and/or simple factual or other mistakes.

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

Outline and assessment of NZSIS compliance systems

General status of compliance measures

In my previous annual report, I reported that the Service did not have an overall compliance framework or dedicated compliance and audit staff. That remained the case through this reporting year.

However, as I also noted, the Service had appointed a Compliance Adviser to conduct an internal review of compliance. The compliance review was comprehensive and rigorous. It was completed in June 2015.

The final review report contains a large number of recommendations for compliance improvement and implementation and, as at the date of this report, steps are in train to appoint a full-time Compliance Manager. A full-time Training Manager has now been appointed.

I also acknowledge that, notwithstanding the lack of a compliance framework, staff strive to act in a lawful and proper manner and there are some important areas of the organisation where approval regimes, which are strictly adhered to, have been developed to govern operational activities. One such example is the process for approval of intelligence warrants, which must be checked at three levels – intelligence directorate management, the Service's legal team – both a legal advisor and the Chief Legal Advisor - and the Director of Security, before it is submitted to the Minister and either the Commissioner of Security Warrants or Minister of Foreign Affairs.

The measures already taken and the further steps underway (as noted above) mark important progress. As at the end of the reporting period, however, the Service still lacked an overall compliance framework or dedicated compliance staffing. More specifically, my office's review and inquiry work indicated that:

- policy guidance and standard operating procedures were in place in some areas, but more often were of uncertain status (not clearly draft or final), not readily accessible or non-existent;
- internal reporting and review, for example seeking management approval or legal advice, occurred on an *ad hoc* basis;
- some monitoring of compliance occurs, but is under-developed or ineffective; and

- while there is some staff training concerning overall legal and policy requirements, particularly for new staff, role-specific and refresher training has been inadequate.

These conclusions are broadly consistent with those reached in the internal compliance review.

Spreadsheet of surveillance warrants

Although there is no provision in the NZSIS Act comparable to s 19 of the GCSB Act, requiring the Service to keep a register of all surveillance warrants, during this reporting year the NZSIS instituted a system whereby it maintains a standing spreadsheet of surveillance warrants issued during the current reporting year, to which my staff and I have access. The spreadsheet contains warrant name, type (domestic or foreign), date of issue, term, target and a summary of the application for warrant. My office is notified when a new warrant is signed.

Self-reporting of incidents

I noted in last year's annual report that the NZSIS did not at that time have any formal mechanism for recording self-reported incidents, nor a formal policy of notifying the Inspector-General when these occur, although in practice some such incidents were reported to me. I observed that both a formal register and policy and a process for reporting to the Inspector-General were desirable.

The Director advised me in early June 2015 that an internal NZSIS register had been created for the purpose of recording all incidents of inadvertent interception and for identifying any systemic issues that need to be addressed. As at that date, all incidents that the Service had identified in this reporting year (ie since 1 July 2014) were recorded on the register. My office has access to the register and is to be notified when an incident is identified and recorded on the register.

The setting up of the register is a positive step. While the register for the reporting period was provided only retrospectively, so it was not possible to undertake a review of the notified incidents either in real time or within the present reporting period, I have incorporated the register into my office's ongoing review work for this reporting year and will report on it in the 2015-2016 annual report.

Interaction with IGIS office

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

- regular meetings with the IGIS/NZSIS Liaison Group, discussed below; and
- 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, including in joint meetings with the Directors of both agencies and their senior staff.

I initiated an NZSIS/IGIS Liaison Group in early 2015. This has provided 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.

My assessment

As noted above, the Service lacked a compliance framework and policy, audit framework and dedicated staffing throughout this reporting period. While I acknowledge that there are specific strengths in the Service's warrant procedures and in the management of operational risks, the absence of such compliance systems mean that there was no general, objective safeguard against breaches of legislation or policy and no general assurance that breaches would be identified and addressed.

The absence of structures and policies meant that NZSIS staff, despite their best intentions, were not sufficiently supported to ensure compliance with NZSIS legal and policy obligations.

For those reasons, I cannot conclude that NZSIS had sound compliance procedures and systems in place. In expressing that conclusion, I want to emphasise the efforts made by NZSIS to institute changes and the potential of those efforts:

- Undertaking the compliance review was a necessary and important first step. The compliance review was undertaken over a period of six months and covered all operational areas. Throughout this period, NZSIS constructively engaged with my office regarding the preliminary findings and conclusions of the compliance review, the reviewer's draft report and the Director's final report.

- The review reached similar conclusions to those that I have set out here and, while outside the current reporting period, I acknowledge the decisions by NZSIS to act on that review. The Director has advised me that implementation will take two to three years but she is hopeful that changes made in 2015-2016 will provide a stronger basis to assess the adequacy of compliance measures and that is my expectation also.

- NZSIS has also engaged constructively with my office's reviews and inquiries on several fronts and that engagement has contributed to stronger practices in those particular areas.

Other activities

I meet regularly with the Privacy Commissioner, Chief Ombudsman and Auditor-General, each of whom has a role in oversight of the intelligence and security agencies, to discuss areas of overlap in our responsibilities and broader issues of common interest.

Visits to regional facilities

My staff and I regularly 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, with a view to shedding more light on what the intelligence and security agencies do and how I oversee and review those activities. In the course of this reporting year I spoke at the Ombudsmen's Conference, Judges' Clerks' Conference and Massey University Contact Course and also provided an interview to Law News.

IGIS 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, the Deputy Inspector-General and the advisory panel.[62] 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.

Pursuant to Cabinet direction (DES Min (13)13/1) the capital costs of establishing the expanded IGIS office and its operational costs were funded from reprioritising existing New Zealand Intelligence Community baselines.

2014/15 budget and actual expenditure

Appropriation	Actual ($000s)	*Budget*
Staff salaries; travel	375	*420*
Premises rental and associated services	136[63]	*128*
Other operating expenses	148	*285*
Non-Departmental Output Expenses (PLA)	542	*573*
Total	**1,187**	***1,362***

The 12% underspend for the 2014-2015 reporting year in part reflects planned set-up costs that were either not incurred at all or not incurred in this reporting period. Further, as the office was not fully staffed for part of the reporting year, salary and some related costs will be higher in the coming year. At the time of reporting, we are working to set the budget, including the set-up expenses to be carried over, for the 2015-2016 year.

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 secure offices within Freyberg House and also provides IT support, both on a cost recovery basis.

[62] IGIS Act, ss 8 and 15D.

[63] Excess over budgeted figure reflects costs of surrender of previous premises lease.

Office of the Inspector-General of Intelligence and Security
P O Box 5609
Wellington 6145
04 439 6721
enquiries@igis.govt.nz
www.igis.govt.nz

Follow us on Twitter @igisnz