Office of the Inspector-General of Intelligence and Security

Annual Report

For the year ended 30 June 2014

Cheryl Gwyn
Inspector-General of Intelligence and Security

17 February 2015

CONTENTS

INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY - FOREWORD 1

My appointment 1

My independence, legislative responsibility and statutory powers 1

Other oversight bodies 2

Ministerial responsibility 2

Political neutrality 3

FUNCTIONS OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY 4

THE INTELLIGENCE AND SECURITY AGENCIES 5

Government Communications and Security Bureau (GCSB or Bureau) 5

New Zealand Security Intelligence Service (NZSIS or Service) 5

THE YEAR IN REVIEW - HIGHLIGHTS 6

Expanded IGIS office 6

Legislative changes 6

Inspector-General of Intelligence and Security Amendment Act 2013 6

Intelligence and Security Committee Amendment Act 2013 7

Government Communications Security Bureau Amendment Act 2013 7

Telecommunications (Interception Capability and Security) Act 2013 8

THE YEAR AHEAD 9

Consolidation of the IGIS Office 9

Implementation of full programme of review and audit 9

2015 legislative review 9

INSPECTOR-GENERAL'S REVIEW 2013/14 10

Work programme 10

Measures of effectiveness 10

Agency engagement 10

Inquiries 10

Inquiries at the request of the Prime Minister or Minister 11

Own-motion inquiries 11

Inquiries into complaints 12

Security clearance complaints 13

Privacy Act complaints 13

Complaints about the actions of an intelligence and security agency 14

"Whistleblowing" 14

Telecommunications (Interception Capability and Security) Act 2013 14
General oversight and review and certification 14
Procedures in relation to warrants and authorisations 15
GCSB 15
Interception warrants and access authorisations 16
Warrantless interceptions 16
Review of GCSB's interception warrants and access authorisations 17
Compliance framework, policies and practices 17
Visits to satellite offices 19
NZSIS 19
Human intelligence collection 19
Covert surveillance 19
Intelligence warrants 20
Review of NZSIS intelligence warrants 20
Compliance policies and practice 21
Visits to satellite offices 22
IGIS OFFICE FINANCES AND ADMINISTRATIVE SUPPORT 23
Funding 23
2013/14 budget 23
Administrative support 23
Hon R A McGechan CNZM QC 23

OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

17 February 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 2013 - 30 June 2014.

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), together with a statement as to whether any matter has been excluded from that copy of the report.

Each of the agencies within my jurisdiction – the New Zealand Security Intelligence Service and the Government Communications Security Bureau – has confirmed that publication of those parts of the report which relate to the agency would not be prejudicial to the matters specified in s 27(4) of the Act. You may, of course, decide otherwise, but my expectations are that you will feel able to lay the entire report before Parliament.

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.

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

INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY - FOREWORD

My appointment

I was appointed by the Governor-General to the position of Inspector-General of Intelligence and Security, under s 5 of the Inspector-General of Intelligence and Security Act 1996 (IGIS Act), to take office from 5 May 2014, for a period of three years. I succeeded the Hon R A McGechan CNZM QC who had agreed to fill the position on an interim basis from 1 July 2013.

It has necessarily taken me some time to become familiar with the details of my jurisdiction and to get to grips with the legislative framework, operations and systems of the intelligence and security agencies which I oversee. That will be an ongoing process.

My independence, legislative responsibility and statutory powers

I am appointed to provide oversight of the activities of the New Zealand Security Intelligence Service (NZSIS) and the Government Communications Security Bureau (GCSB). The IGIS Act provides that any other agency may be declared by the Governor-General by Order in Council to be an intelligence and security agency for the purposes of oversight under the Act. I do not have power to scrutinise the activities of any government department or other agency that is not a designated "intelligence and security agency".

The role of the Inspector-General is set out in the IGIS Act and is, broadly, to assist each Minister who is responsible for an intelligence and security agency in the oversight and review of that agency and to assist the Minister to ensure that activities of that intelligence and security agency comply with the law and are proper. In that sense, my role is to strengthen the accountability of the intelligence and security agencies to the executive government.

However, as a statutory officeholder, I am not subject to general direction from the Prime Minister, the Minister for National Security and Intelligence, the Minister in charge of the NZSIS or the Minister responsible for the GCSB, or other Ministers, on how responsibilities under the IGIS Act should be carried out.

I am not part of the intelligence agencies and I carry out my role independently of them. I do not speak for the agencies and it is not my role to defend them.

It is important that the public have confidence in the oversight I provide and I believe that the public should be able to see, as far as is consistent with effective national security and law enforcement, how the intelligence and security agencies perform in terms of legislative compliance and public expectations. This report is intended to provide assurance that intelligence and security matters are open to scrutiny. The extent to which my office provides that scrutiny is developing, as set out in this report.

Gaining that assurance requires an understanding of what my oversight role entails. It is not easy to give a useful public account of what the intelligence and security agencies actually do because much of it is sensitive and classified and I am constrained by statutory provisions that prevent disclosure. Within those limits I have endeavoured to provide an informative description of my role and the activities of my office. In the coming year I will publish an unclassified version of my Office's programme for inspection and review of NZSIS and GCSB.

The intelligence and security agencies have wide-ranging powers to intrude upon the privacy of individuals. My role entails oversight of the exercise of those powers to ensure they are used lawfully and appropriately. My statutory powers allow me to access all of the documents and information held by the NZSIS and the GCSB, no matter how sensitive or highly classified these may be. The agencies routinely provide my staff with access to requested records for the purposes of inspection and review, or in response to complaints to me from members of the public.

Other oversight bodies

The Inspector-General is part of a broader oversight and accountability framework. The Inspector-General focuses on the agencies' operational activities. This function is complemented by the Intelligence and Security Committee of Parliament (ISC). The Commissioner of Security Warrants also has a role, in authorising intelligence warrants for the NZSIS to carry out certain activities and warrants and authorisations for the GCSB to intercept communications or access information infrastructures.

I report to the Minister responsible for each agency and not to Parliament but I may, with the concurrence of the Prime Minister, report either generally or in respect of any particular matter to the ISC.

Contact with intelligence and security oversight bodies in other similar jurisdictions is important to keep abreast of issues and developments in the intelligence and oversight world and to avoid isolation. Shortly after our appointment, the Deputy Inspector-General and I met with my Australian counterpart Vivienne Thom, Inspector-General of Intelligence and Security. The Australian Inspector-General of Intelligence and Security Act 1986 is very similar to the New Zealand legislation and it will be useful to be able to draw on the Australian Inspector-General's practice and experience.

I was also able to participate in the biennial International Intelligence Review Agencies Conference (IIRAC) in London in May 2014. The 2014 conference was jointly hosted by the UK oversight bodies, the Intelligence and Security Committee of Parliament, the Intelligence Services Commissioner and the Interception of Communications Commissioner. Oversight bodies from fifteen countries were represented and the discussion included identifying what global trends could drive the investigative work of intelligence agencies between now and 2020; comparing models of accountability, and sharing experience and good practice; and considering how oversight bodies can become more visible and transparent.

Within New Zealand, each of the Inspector-General, Privacy Commissioner, Ombudsmen and Controller and Auditor-General has responsibility for oversight of some aspects of the activities of the NZSIS and the GCSB. We meet regularly to discuss areas of overlap in our responsibilities and any broader issues of common interest.

Ministerial responsibility

After this reporting period a new role of Minister for National Security and Intelligence was created and that portfolio assumed by the Prime Minister. The Minister for National Security and Intelligence has leadership of the national security system, is responsible for the overall policy

settings and legislative framework of the sector, chairs the National Security Committee of Cabinet and chairs the Intelligence and Security Committee (in his capacity as Prime Minister).

The Minister Responsible for the GCSB and Minister in Charge of the NZSIS exercises ministerial oversight of those two agencies and approves applications for warrants and authorisations under the GCSB and NZSIS Acts. He operates within the framework set by the Minister for National Security and Intelligence.

My reports are made to the Minister and I meet regularly with him. I will continue to meet from time to time with the Minister for National Security and Intelligence also.

Political neutrality

Both the NZSIS and the GCSB have statutory obligations to maintain political neutrality, including a requirement that their Directors consult regularly with the Leader of the Opposition.[1] Although there is no statutory obligation of consultation on the Inspector-General, I think it is important that the Leader of the Opposition is kept appraised of how the oversight function is being carried out. To that end, I have met with the Leader and Deputy Leader of the Opposition, to discuss the role and functions of the Inspector-General's Office and will do so again as necessary. I also offered to meet with the Leaders of all other parties represented in the Parliament and to date I have met with all but one of them.

[1] New Zealand Security Intelligence Service Act 1969 (NZSIS Act), s 4AA; Government Communications Security Bureau Act 2003 (GCSB Act), s 8D(3)(c) & (d).

FUNCTIONS OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

The Inspector-General's oversight and review function is achieved through the statutory authority of the Inspector-General to undertake an audit function, both routine and unscheduled, as well as to inquire into matters raised, whether as a result of the audit process, at the request of the Minister for further inquiry or by way of complaint.

The IGIS Act provides the legal basis for regular inspections of the intelligence and security agencies so as to assess the effectiveness and appropriateness of 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 (work programme) is submitted by the Inspector-General for the Minister's approval.

The inspection role of the Inspector-General is complemented by an inquiry function. The Inspector-General has strong investigative powers akin to those of a Royal Commission, including the power to compel persons to answer questions and produce documents, to take sworn evidence and to enter all the premises of the agencies.

The Inspector-General 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.

In order to carry out these functions, the Inspector-General has a right of access to security records[2] held by the agencies and a right of access to agencies' premises,[3] including to 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.

Under the Protected Disclosures Act 2000[4] NZSIS and GCSB employees may seek information and guidance from the Inspector-General on any matter concerning that Act and the Inspector-General is the only appropriate authority to whom they may disclose information in a "whistleblower" sense. The IGIS Act[5] provides protections for any employee making a protected disclosure against any penalty or discriminatory treatment by the employing agency for making that disclosure, unless the Inspector-General determines that the employee was not acting in good faith in making the disclosure. The employee also has the protections contained in the Protected Disclosures Act.

The Inspector-General also has a role under the Privacy Act 1993. The GCSB Amendment Act 2013 imported some of the principles of the Privacy Act into the GCSB Act and the Inspector-General has jurisdiction to investigate complaints into alleged breaches of those provisions.

The Inspector-General also potentially has a role in relation to the Telecommunications (Interception Capability and Security) Act 2013, where a New Zealand person is adversely affected by an intelligence and security agency exercising a function under that Act.

---

2 Inspector-General of Intelligence and Security Act (IGIS Act), ss 2 and 20.
3 IGIS Act, s 21.
4 Protected Disclosures Act 2000, s 12.
5 IGIS Act, s 18.

THE INTELLIGENCE AND SECURITY AGENCIES

Government Communications and Security Bureau (GCSB or 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.

New Zealand Security Intelligence Service (NZSIS or 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.

During this reporting period, the Prime Minister was the Minister in charge of the NZSIS.

THE YEAR IN REVIEW - HIGHLIGHTS

Expanded IGIS office

At the beginning of the reporting period the Inspector-General's office comprised the Inspector-General and one part-time executive assistant. There were no investigating staff to assist the Inspector-General. The office was located in small premises, with inadequate communications systems and no website.

The Hon R A McGechan CNZM QC accepted appointment as Inspector-General from 1 July 2013, for an interim period. He assumed responsibility for relocating the IGIS office (to Freyberg House, where the office now occupies fully secure premises) and the appointment of two Investigating Officers, seconded from the New Zealand Defence Force and the Ministry of Foreign Affairs and Trade, and a part-time IT analyst. The Inspector-General's website (www.igis.govt.nz) was also established.

There were considerable delays in moving to the new office, achieving a fully compliant communications system and getting seconded staff in place. These delays appear to have stemmed from the security requirements in respect of staff, premises, equipment and systems. They necessarily had an impact on the ability of the Office to meet all of its statutory functions.

Notwithstanding the difficulties, the previous Inspector-General prepared comprehensive draft work programmes for the audit and review function, for each of the NZSIS and the GCSB, and commenced a systematic programme of inspection of warrants and authorisations.

Mr McGechan retired with effect from 4 May 2014 and was replaced by Cheryl Gwyn. A fulltime Deputy Inspector-General, Ben Keith, was appointed during the reporting period with the appointment taking effect from 2 July 2014.

Legislative changes

In the reporting period there were a number of legislative amendments impacting on the New Zealand Intelligence Community. The Government Communications Security Bureau Amendment Bill 2013 was an omnibus bill (later split into three separate amending bills) that amended the IGIS Act, the Intelligence and Security Committee Act 1996 and the GCSB Act. In addition, the Telecommunications (Interception Capability and Security) Act 2013 brought a new area of responsibility to the Bureau**.**

Inspector-General of Intelligence and Security Amendment Act 2013

The amendments to the IGIS Act:

- extended the Inspector-General's statutory work programme to require regular examination of system-wide issues that impact on operational activities;
- required the Inspector-General to certify in each year in his or her annual report whether the agencies' compliance systems are sound;

- provided for the Inspector-General to initiate inquiries into matters of propriety without requiring the concurrence of the responsible Minister;

- required the Inspector-General to make unclassified versions of inquiry reports, and the annual report, publicly available on the Inspector-General's website (www.igis.govt.nz);

- removed the legislative requirement that the Inspector-General be a retired High Court Judge, broadening the pool of potential candidates;

- provided for the appointment of a Deputy Inspector-General;

- established an Advisory Panel to provide advice to the Inspector-General.

Intelligence and Security Committee Amendment Act 2013

The principal changes were:

- the Prime Minister (who is the chairperson of the Committee) must relinquish the chair if the Committee, when discussing a financial review of an agency for which the Prime Minister is the responsible Minister, is discussing the performance of that agency;

- the Prime Minister is permitted to nominate either the Deputy Prime Minister or the Attorney-General to act as an alternate chair in some circumstances where that alternate is not already a member of the committee;

- subject to restrictions on the publication of sensitive information, the committee is required to table its reports in the House and make them publicly available on an internet site.

Government Communications Security Bureau Amendment Act 2013

The Amendment Act restated the three functions of GCSB (information assurance and cyber security; foreign intelligence; and cooperation with and assistance to other agencies) in separate provisions, with the intention of improving transparency and facilitating external oversight.

The Amendment Act restated the basic premise that the GCSB is not to conduct foreign intelligence activities against New Zealand citizens or permanent residents, except where the person comes within the definition of "foreign person" or "foreign organisation" in the GCSB Act. The provisions of the Act were reframed to clarify that this restriction on intercepting New Zealanders' communications applies only to the Bureau's foreign intelligence function. It does not apply to the information assurance/cyber security function or where the Bureau is providing assistance to other agencies under their legislative powers.

Any activity under the information assurance/cyber security function or the collection of foreign intelligence function that might involve intercepting the communications of New Zealanders requires an authorisation to be granted jointly by the responsible Minister and the Commissioner of Security Warrants.

The amendments also included new obligations on the GCSB. The first was a direction to keep a register of interception warrants and access authorisations, which must be made available to the Minister or the Inspector-General as and when requested.

The second relates to additional principles that must be applied by the GCSB to protect personal information (the principles relating to the purpose of collection, storage and security, accuracy, and not keeping information longer than is necessary). The responsibility to investigate complaints into these aspects of the GCSB Act rests with the Inspector-General. The Bureau began formulation of a policy on personal information during this reporting period, in consultation with the Inspector-General and the Privacy Commissioner.

Telecommunications (Interception Capability and Security) Act 2013

The Telecommunications (Interception Capability and Security) Act 2013 (TICSA) repealed the Telecommunications (Interceptions Capability) Act 2004. The TICSA updates network operator interception capability obligations and establishes a new legal framework for network security obligations.

If a New Zealand person[6] is adversely affected by an action of an intelligence and security agency exercising a function under the TICSA, the Inspector-General may inquire into the matter under the Inspector-General's complaints jurisdiction.[7]

If companies are adversely affected by the actions of the Bureau in respect of the application of this legislation, the Inspector-General has jurisdiction to receive complaints if the company falls within the definition of a New Zealand person.

6 IGIS Act, s 2.
7 IGIS Act, s 11(1)(b).

THE YEAR AHEAD

Consolidation of the IGIS Office

I expect that the set-up of office premises and secure communications systems and the recruitment of a full complement of staff (comprising four Investigating Officers, three of whom will be seconded from other government agencies, an IT Manager & Security Adviser and an Office Manager/Executive Assistant, in addition to the Inspector-General and Deputy Inspector-General) will be completed by February or March 2015. The increase in staff reflects the expanded responsibilities of the Inspector-General under the 2013 legislative amendments, particularly the new review, audit, inquiry and compliance certification functions and the need to meet those responsibilities in a robust and credible way. It also reflects the logistical requirements of carrying out fair, thorough and effective inquiries, such as the inquiry into the release of official information by the NZSIS,[8] and the demands posed by the greater visibility and contentiousness of the work of the NZSIS and the GCSB.

There will be some further, modest development of the IGIS Office website to make it more accessible and useful for members of the public, including facilitating the process for making a complaint to the Inspector-General.

The Advisory Panel members,[9] Christopher Hodson QC and Angela Foulkes, were appointed outside this reporting period and I anticipate the regular engagement of the Panel members with the Inspector-General's work in the year ahead.

Implementation of full programme of review and audit

As discussed later in this report, once it is fully staffed the Office will be able to better meet its statutory review and audit functions. Inquiries into complaints and other matters are important and may, over time, point to systemic issues, but it is the regular review and audit of the agencies that is critical to effective oversight. I and my staff are very focused on meeting this obligation and we are making progress. I will report on that in the next annual report.

2015 legislative review

A review of the intelligence and security agencies, the legislation governing them and their oversight legislation must be commenced before 30 June 2015.[10] The Attorney-General is to appoint the reviewers and specify the terms of reference for the review, after consulting the Intelligence and Security Committee. The reviewers may ask the Inspector-General to provide information for the conduct of the review and the Inspector-General may also provide information on the Inspector-General's own initiative.[11] I will seek an opportunity to make submissions on the review, primarily about the oversight legislation, but also in relation to the legislation governing the agencies, on the basis of my experience to date of monitoring compliance with that legislation.

---

[8] This inquiry was conducted outside the reporting period. The report of the inquiry is at www.igis/publications/investigation-reports.

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

[10] Intelligence and Security Committee Act 1996 (ISC Act), s 21.

[11] ISC Act, s 23.

INSPECTOR-GENERAL'S REVIEW 2013/14

Work programme

The IGIS Act requires that the Inspector-General prepare a programme of work covering general oversight and review and the particular functions set out in the IGIS Act, and submit it to the Minister for approval.

My predecessor developed comprehensive draft work programmes in respect of each agency, which I have adopted in large part and which will be submitted to the Minister for approval.

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
- 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 Inspector-General's office.

I will report on these measures in the next reporting period.

Agency engagement

I meet 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 also use these discussions to brief me on emerging risks 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.

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. 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.[12]

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 subject to any security concerns, the report must be made public on the IGIS website. The Inspector-General may determine the security classification of each report, after consulting the chief executive of the relevant agency.

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 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 Prime Minister or Minister

There were no requests from the Prime Minister (who was also the responsible Minister for both agencies) for the Inspector-General to inquire into any matter during this period.

Own-motion inquiries

Three inquiries of the Inspector-General's own motion were instigated during this reporting period. One was completed within the period and two were carried over into the next reporting period.

In February 2013 the Director of GCSB informed the previous Inspector-General that due to errors in the GCSB 2012/13 Annual-Report an erratum would need to be presented to the House of Representatives. The error related to the reported numbers of interception warrants and access authorisations in force and issued during the reporting period. The Inspector-General instigated an own-motion inquiry. The inquiry concluded that the error arose in part from a definitional misunderstanding and in large part from a legacy record problem. Both had been remedied and adequate safeguards had been or were being put in place to avoid recurrence. The former Inspector-General concluded that the risk of any recurrence was negligible and made no recommendations.

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

Two further own-motion inquiries which were commenced in the reporting period were not completed as at 30 June 2014 and have been carried over to the next reporting period. One of those inquiries, which relates to the NZSIS and which arose from the regular inspection of intelligence warrants, is the first Inspector-General inquiry into the "propriety" of particular activities of an intelligence and security agency.[13] The standard of propriety is not defined in the IGIS Act, but its value is that it can allow a broader inquiry that goes beyond questions of strict legality. So, for example, in the inquiry into the release of information by the NZSIS[14] it encompassed whether the agency acted in a way that a fully informed and objective observer would consider appropriate and justifiable in the circumstances.

I initiated a further inquiry as a result of the previous Inspector-General's report into a complaint about the Service (see p 14 below). The inquiry is into the legality and propriety of the NZSIS practice of issuing warnings.

Both of these inquiries involve consideration of classified operational activities and involve information which, if disclosed, would be likely to prejudice the continued discharge by the NZSIS of its functions. For that reason, I have not included details of the inquiries in this report. Once the inquiries are completed, I will make an unclassified summary of the reports into each inquiry publicly available, on the Inspector-General's website, in the normal course.

Inquiries into complaints

A New Zealand person or a person who is an employee, or former employee, of an intelligence and security agency, may complain to the Inspector-General that he or she has been or may have been adversely affected by any act, omission, practice, policy, or procedure of an intelligence and security agency (s 11(1)(b) IGIS Act).

Complaints must be in writing and addressed care of the Registrar or Deputy Registrar of the High Court at Wellington, who forwards them to the Inspector-General for determination. If complaints are received by the Inspector-General directly, the complainant is notified that they must first send their complaint to the Registrar before any action can be taken on it. The requirement to submit complaints via the High Court Registrar is anachronistic and I will seek a change to the relevant provision in the 2015 legislative review.

Where it may be more appropriate for the Inspector-General to determine a complaint, the Privacy Commissioner and the Ombudsman are able to transfer complaints received by them to the Inspector-General.

Each communication to my office is assessed to determine whether it falls within the functions of the office and the most appropriate way of dealing with it. In many cases, complaints and other communications can be resolved at an administrative level by my office talking with the relevant agency and looking at their files and discussing it with the complainant. This approach is useful in determining whether a particular question is within the Inspector-General's jurisdiction and whether it is appropriate to pursue a formal inquiry.

---

13 IGIS Act, s 11(1)(ca).

14 See above, n 8.

Ten complaints were received and completed during this reporting period and a further two complaints were carried over into the next reporting period. The complaints fall principally into three categories: the outcome of the security clearance vetting process undertaken by the Service, refusal of requests for information (Privacy Act) and actions of an intelligence and security agency.

Security clearance complaints

Government policy requires that all employees and contractors who have access to material having a national security classification must have a security clearance. The NZSIS is the organisation which undertakes a "vetting" process to determine a person's suitability for a security clearance. The higher the level of security clearance sought, the more detailed the vetting process. While the process is carried out with the individual's knowledge and consent it is, by its nature, personally intrusive and may have a significant impact on that person's employment status or prospects.

The Inspector-General does not review the substantive merits of any particular security vetting decision, but may examine the vetting process, determine whether an error may have occurred in the process and recommend that the Director reconsider the application in light of any identified error(s).

The office received four new complaints about the outcome of security vetting applications in this reporting period and two were carried over from the previous reporting year. Of the four new complaints, one was later withdrawn by the complainant; the second complaint was investigated but not upheld; in the third, further information was sought from the complainant on several occasions but not received and the file was closed; the fourth complaint remains open. In the two complaints carried over from the previous year, the Inspector-General recommended that the Service reconsider its findings and that occurred. A further two complaints were received directly by the Inspector-General and on requesting that the complaints be sent first to the Registrar of the High Court, as required by the IGIS Act, nothing further was heard from the complainant. No inquiry was started into these matters.

The details of these complaints (which include highly personal information) may not be included in a report that is to be made publicly available.[15]

Privacy Act complaints

The Inspector-General received two Privacy Act complaints during this period, both following a determination of the Privacy Commissioner that the agency (the Service in one case and the Bureau in the other) had a proper basis to withhold the information sought. In both cases the Inspector-General concluded that no further inquiry was necessary.

No complaints of this type were transferred from the Privacy Commissioner or Ombudsmen to the Inspector-General.

[15] IGIS Act, s 25A(2)(e).

Complaints about the actions of an intelligence and security agency

Two complaints were received and inquiries completed relating to allegations that actions of an intelligence and security agency had adversely affected a New Zealand person.

The first complaint related to the conduct of the Service during the overt execution of an intelligence warrant. The complaint was initially received by the Ombudsman and subsequently transferred to the Inspector-General. The Inspector-General's report included a recommendation that the Service suspend any practice of issuing planned warnings until it had received and considered legal advice from Crown Law. An unclassified version of the report is available on the IGIS website.[16]

Following from this complaint I commenced an own-motion inquiry into the legality and propriety of the Service practice of issuing warnings. I decided that such an inquiry is necessary because the activity in question is relevant beyond the particular complaint considered by my predecessor. That inquiry is ongoing.

The second complaint alleged actions had been taken by the Service against the complainant. The complaint also included a request for any information held by the Service about the complainant. The request for information was transferred to the Service as a Privacy Act request. As to the substance of the complaint, the Inspector-General determined that further inquiries were unnecessary[17] and, the inquiry into the matter was closed.

"Whistleblowing"

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

Telecommunications (Interception Capability and Security) Act 2013

No complaints in relation to the TICSA were received by the Inspector-General in the reporting year.

General oversight and review and certification

The Inspector-General must review at least 12 monthly the effectiveness and appropriateness of each agency's procedures to ensure compliance with its governing legislation relating to the issue and execution of warrants and authorisations and the effectiveness and appropriateness of each agency's compliance systems covering operational activity. There is a specific power to conduct unscheduled audits of those procedures and compliance systems.

The Inspector-General must also certify in the annual report the extent to which each agency's compliance systems are sound.

As at the end of this reporting period I had been Inspector-General for seven weeks. My predecessor was in the role for ten months, on an interim basis. During that period much of his time was necessarily spent in the time-consuming and protracted process of implementing the set-up of the expanded IGIS office, as discussed above, together with developing the draft work

[16] www.igis.govt.nz.
[17] IGIS Act, s 17(2).

programmes and undertaking a regular inspection of all warrants and authorisations issued by both the GCSB and the NZSIS.

No reviews of the compliance systems covering operational activity, or unscheduled audits, were carried out in the reporting period. For the reasons outlined above, it was not practicable to do so. It follows that I am not able, as at 30 June 2014, to certify that either NZSIS or GCSB has overall systems which are "sound" in whole or to any lesser extent. That statement should not be misconstrued as a statement the respective systems are unsound.

The GCSB has a compliance policy and framework and legal and compliance teams which have been significantly expanded since the Kitteridge report.[18] It has introduced processes for self-reporting of incidents and systematic audits/compliance checks. Where there is any material concern about compliance with legislation and/or internal policies and procedures, GCSB suspends the collection or other activity while that question is investigated and resolved.

The NZSIS's activities are regulated by a number of internal policies but, as at this reporting date, the Service did not have an overall compliance framework or dedicated compliance and audit staff. A Compliance Adviser has been appointed subsequently to review NZSIS's current compliance framework and to make recommendations to the Director of the NZSIS about any changes that may be necessary. The Director, who was appointed in May 2014, has indicated her intention to have a strong organisational focus on compliance matters.

I will report on relevant reviews, audits and certification in the next reporting period.

Procedures in relation to warrants and authorisations

In light of the set-up phase of the office and limited staff and resources available to the Inspector-General during the reporting period, attention was focused on inspection of warrant and access authorisation inspections. In this reporting period 34 NZSIS domestic warrant applications were reviewed, together with all foreign intelligence applications and other warrant-related documents (cancellations and amendments to warrants). Ten interception warrants and 48 access authorisations for the GCSB were reviewed. This represents 100% of the Service's applications and related documents and 93.5% of the total number of Bureau applications.

GCSB

The GCSB primarily relies on Signals intelligence (SIGINT), which refers to electronic transmissions that can be collected by ships, planes, ground sites or satellites. Communications intelligence or COMINT is a type of SIGINT and is intelligence gathered by the interception of communications between people. Electronic intelligence or ELINT is gathered from electronic signals not directly used in communication.

Interception of communications most often occurs in the digital sphere but also in relation to high frequency radio wave and satellite communications.

[18] Rebecca Kitteridge, *Review of Compliance at the Government Communications Security Bureau,* March 2013.

Interception warrants and access authorisations

The responsible Minister can authorise the GCSB to use an interception device to intercept communications or access specified information infrastructures,[19] where that would otherwise be unlawful.[20]

The interception warrant or access authorisation must be for the purpose of performing one or both of the Bureau's information assurance/cyber security or intelligence gathering functions.[21]

As already noted, the restriction on the Bureau doing anything for the purpose of intercepting the private communications of New Zealand citizens or permanent residents of New Zealand (unless and to the extent the individual comes within the definition of a foreign person or foreign organisation)[22] applies to its intelligence gathering function, but not to its information assurance/cyber security function.

Where authority is properly sought for the purpose of intercepting the private communications of New Zealand citizens, or permanent residents of New Zealand, then the application must be issued jointly by the Minister and Commissioner of Security Warrants.[23] This requirement applies to both the information assurance/cyber security function[24] and the intelligence-gathering function.[25]

Before issuing an interception warrant or access authorisation, the Minister must be satisfied[26] not only that it is for the purposes of either information assurance/cyber security or the collection of foreign intelligence (or both), but also that the outcome sought justifies the particular interception or access and is not likely to be achieved by any other means; there are satisfactory arrangements in place to ensure that nothing will be done in reliance on the warrant or authorisation beyond what is necessary for the proper performance of the Bureau's relevant function(s) and there are satisfactory arrangements in place to ensure that the nature and consequences of acts done in reliance on the warrant or authorisation will be reasonable, having regard to the purposes for which they are carried out.

The Minister must consult with the Minister of Foreign Affairs before issuing an interception warrant or access authorisation.

Warrantless interceptions[27]

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

19 "Information infrastructure" refers to the communications networks and associated software that support interaction among people and organisations, eg the Internet, telecommunications networks.
20 GCSB Act, s 15A.
21 GCSB Act, ss 8A and 8B.
22 GCSB Act, ss 4 and 14.
23 GCSB Act, s 15B.
24 GCSB Act, s 8A.
25 GCSB Act, s 8B.
26 GCSB Act, s 15A(2).
27 GCSB Act, s 16.

interception device to any part of an information infrastructure or installing an interception device in a place. An example of this would be the interception of high frequency signals of ships or other radio operators. 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 a permanent resident of New Zealand (unless and to the extent that person comes within the definition of a foreign person or foreign organisation).

Although the GCSB Act does not require it, the Director's authorisations are in writing.

Review of GCSB's interception warrants and access authorisations

The Inspector-General's review of warrants and authorisations involves my staff in reviewing both the application documents and the warrant or authorisation itself.

The application documents are scrutinised to ensure that the statutory requirements for and limitations on interceptions and access are recognised, whether an adequate basis is demonstrated for the application, and whether it was made to both the Minister and Commissioner of Warrants (where required).

The warrants and access authorisations are checked to ensure they have been signed by the appropriate person, specify all of the relevant information,[28] and are worded with sufficient clarity. Where issued urgently,[29] they are checked for sufficient information to satisfy the statutory requirements for urgency and that it is signed by the appropriate person.

During the reporting year my office reviewed applications for 10 interception warrants and 48 access authorisations. In the next reporting year there will, in addition, be a focus on reviewing Director's authorisations.

Compliance framework, policies and practices

The GCSB Security Audit Implementation Working Group was set up in this reporting period to assist the previous Inspector-General to work through a number of technical issues and processes which he had indicated were necessary to enhance compliance and enable more effective oversight and audit. The Working Group has continued to provide a useful forum for the Inspector-General for the discussion of emerging issues and risks and how the Bureau proposes to respond to them.

The Bureau provides the Inspector-General with a quarterly compliance and policy report which has covered the following areas:

- progress on implementing the recommendations of the Kitteridge report,

[28] GCSB Act, s 15D: date of issue; person(s) authorised to make the interception/obtain the access; period for which it is issued (maximum of 12 months); function(s) of the Bureau to which it relates; purpose; any conditions under which interception may be made or access obtained.

[29] GCSB Act, s 19A.

- development of policies and compliance as a result of amendments to the GCSB legislation,
- methods of self-auditing compliance against the policies being established,
- training developments,
- numbers of Official Information Act 1982 and Privacy Act requests, and
- self-reported incidents.

The GCSB uses a Compliance Incident Register to track and manage incidents discovered or reported during the course of the Bureau's business activities where an incident involves a possible breach of a warrant or authorisation or of the governing legislation. The Bureau's compliance and policy team investigate the incident, determine whether it was a breach, determine the remedial action where required and notify the Inspector-General of the outcome of the investigation. The technical and complex nature of the Bureau's work make this self-reporting function particularly important.

Five incidents were notified to my office during this reporting period. Two revealed no breach of a warrant or authorisation or of the governing legislation, but did result in GCSB establishing clearer internal processes. The other three cases were inadvertent breaches. In each of those cases any data collected was destroyed, appropriate systems changes were made and/or educative steps were taken, to prevent recurrence. In each of the three the Inspector-General, after reviewing the files, determined that the nature of the incidents and the remedial steps taken by GCSB meant that no further inquiry or action by the Inspector-General's office was necessary.

The Bureau is required[30] to keep a register of interception warrants and access authorisations issued under Part 3 of the GCSB Act. The register must contain specified information which includes the purpose of the warrant and its duration, whose communications may be intercepted and/or at what place, who is authorised to make the interception or obtain access; whether any other person or body is requested by the Bureau to give assistance in giving effect to the warrant or authorisation.[31] The Director must make the register available to the Minister or Inspector-General as and when requested and if a warrant relates to the interception of communications of a New Zealand citizen or permanent resident, the Director must notify the Inspector-General as soon as possible after the information is entered in the register. As at the end of this reporting period, all of the requisite information was being held in Bureau documentation, and was able to be produced for inspection by the Inspector-General if required. Outside of the 2013/14 reporting year, the Bureau determined that it was necessary to keep all relevant information in the register, not only in subsidiary documentation. Changes have now been made to ensure that all relevant information is captured in the register itself.

30 GCSB Act, s 19.
31 GCSB Act, s 15E.

Visits to satellite offices

During the reporting period there were a number of site visits to the Bureau's Waihopai and Tangimoana stations.

The first visit to Waihopai took place in October 2013 and the previous Inspector-General received an introductory presentation on the operational activities carried out from Waihopai and a tour of the facilities. The second visit took place in March 2014, when the two seconded Investigating Officers were also given an introduction to the facilities and the operations carried out there.

The previous Inspector-General visited Tangimoana in October 2013. The purpose of this first visit was to receive an overview and tour of the facility and its functions. A second visit, including the two Investigating Officers, took place in February 2014.

I have visited Waihopai and Tangimoana since I became Inspector-General and will regularly visit both facilities as part of my regular scrutiny of the activities of the Bureau.

NZSIS

NZSIS's collection of foreign intelligence relies on a variety of intelligence methods, including the use of human sources, special powers authorised by warrant and published sources. The warranted powers include the ability to intercept or seize communications, documents or things, or to undertake electronic tracking. The target of an intelligence warrant can be either a New Zealand or foreign person and different issuing requirements exist for each.

Human intelligence collection

Human intelligence (HUMINT) is intelligence gathered from human sources, rather than through technical intelligence gathering means such as SIGINT. Some HUMINT collection involves clandestine or covert activities, but much of it is done openly, such as interviewing potential sources of intelligence or gathering published material. The Service does not require legislative authority to conduct human intelligence collection but its internal policy recognises the potential impact of direct contact with members of the public. The policy requires approvals prior to an interaction, including the limited circumstances when those approvals can be sought retrospectively, and reporting after an interaction.

Covert surveillance

Surveillance without a warrant, conducted by the Service, is restricted to visual surveillance where the participants in the activity being observed or recorded would not expect that activity to be private. Where there is no expectation of privacy there is no requirement for a warrant under section 4A of the NZSIS Act. The Service has identified the requirement to have a more comprehensive policy which codifies the processes in place covering planning, risk analysis and approval of surveillance activities. I will review this policy in the next reporting period.

Intelligence warrants

Where the Service is conducting surveillance either by interception of communications or by electronic tracking an intelligence warrant under s 4A of the NZSIS Act is required.[32] The Service may seek either a domestic intelligence warrant[33] or a foreign intelligence warrant.[34]

A domestic intelligence warrant is issued jointly by the Minister and the Commissioner of Security Warrants against a named person, entity or place.

A foreign intelligence warrant is issued by the Minister alone, who must be satisfied that there are reasonable grounds for believing that the subject of the intelligence warrant is not a New Zealand citizen or permanent resident and that any places specified are occupied by a foreign organisation or a foreign person.

The Minister must consult the Minister of Foreign Affairs about the 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.

An intelligence warrant provides an authorisation for the Service to intercept or seize any communication, document, or thing not otherwise lawfully obtainable or to undertake electronic tracking of identified persons.

Before the Minister and the Commissioner (if required) issue an intelligence warrant they must be satisfied on the basis of the evidence provided on oath by the Director of the Service that:

- the warrant is necessary for the detection of activities prejudicial to security or that it is necessary for the purpose of gathering foreign intelligence information that is essential to security;[35]
- the value of the information sought to be obtained under the proposed warrant justifies the particular interception or seizure or electronic tracking;
- the information is not likely to be obtained by any other means; and
- any communication sought to be intercepted or seized under the proposed intelligence warrant is not privileged.[36]

Review of NZSIS intelligence warrants

The Inspector-General's review of intelligence warrants involves my staff in reviewing both the application documents and the warrant itself.

---

32 After this reporting period the New Zealand Security Intelligence Service Act 1969 (NZSIS Act) was amended to allow the Director of the NZSIS to authorise interception or seizure, electronic tracking, or visual surveillance, without a warrant in some situations of emergency or urgency: NZSIS Act, ss 4ID-4IF.

33 NZSIS Act, s 4A(1).

34 NZSIS Act, s 4A(2).

35 NZSIS Act, s 2.

36 In proceedings in a court of law under section 58 or 59 of the Evidence Act 2006; or any rule of law that confers privilege on communication of a professional nature between a lawyer and his or her client.

The application documents are scrutinised to ensure the Director made written application, it was supported by evidence on oath and refers to all relevant statutory requirements.[37] Each warrant is checked to ensure that it states whether it is a domestic or foreign intelligence warrant; if the former, that it is issued jointly by the Minister and the Commissioner of Security Warrants, if the latter is issued by the Minister; authorises only those activities provided for in the legislation; states details as to type, identity, location and description as required by the statute; follows consultation with the Minister of Foreign Affairs where that is required; states that the conditions on which the Minister (and the Commissioner of Security Warrants where relevant) must be satisfied, are satisfied. I do not form a view on whether the Minister and Commissioner were right or wrong, but rather whether there is information on which, on balance, the view they reached was open to them.

During the reporting period my Office reviewed all applications for domestic and foreign warrants issued under section 4A(1) and (2) of the NZSIS Act, both new warrants and renewal of existing warrants. The intelligence warrants approved the use of all powers or some combination of the ability to intercept, seize and electronically track.

Two operations of short duration were selected for a more thorough review, which involved checking the supporting intelligence referred to in the application and the intelligence collected in reliance on the warrant. The review of the intelligence collected focussed on whether it was lawfully collected within the scope of the warrant as well as whether it was proper for it to be collected. In each case the intelligence warrant application met the statutory standard[38] and was open to the Minister on the basis of the supporting documents. The information collected in reliance on the warrant was, in each case, within the scope of the warrant and no action was taken outside the terms of the warrant.

In the next reporting period my staff will give more detailed scrutiny to a selection of domestic intelligence warrants, chosen at random. In respect of both foreign and domestic intelligence warrants, we will conduct unscheduled, random audits of the process and path by which warrant applications were formulated, from the commencement document to the signed application. As noted above, the review of warrants in this reporting period led to the initiation of an own-motion inquiry.

Compliance policies and practice

The NZSIS does not 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 are reported to the Inspector-General. Both a formal register and policy and a process for reporting to the Inspector-General are desirable. There was one self-reported incident notified to the Inspector-General during this reporting period which involved the inadvertent interception of third party communications. The information collected was deleted without being listened to and the identity of those recorded was not collected. The Inspector-General determined that the non-warranted interception was unavoidable in the circumstances and the remedial action taken on discovery was sufficient. No further action was necessary.

---

37 NZSIS Act, s 4A.

38 NZSIS Act, s 4A(3).

Visits to satellite offices

In February 2014 the previous Inspector-General visited the NZSIS Auckland Region Office, to familiarise himself with the facility, speak to staff stationed there about their work, and to begin to determine how the operational functions undertaken that are particular to that office could be reviewed and audited by the IGIS office.

Since my appointment I have visited the Auckland Region Office once and will do so regularly in the future.

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 and the Deputy Inspector-General.[39] The second is the operating costs of the office which are funded from Vote: Justice (Equity Promotion and Protection Services), 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.

2013/14 budget

	Actual	Budget
	$000's	$000's
Staff and travel	157	190
Property and rental	156	159
Other	50	45
Total	363	394

Surplus to be carried forward $31,000.

	Actual	Budget
	$000's	$000's
Non-Departmental Output Expenses (PLA)	320	371

It is noted that this reporting year is not a typical year because the expanded office provided for in the 2013 legislative amendments was still in the process of being set up and the office was not fully staffed.

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 Department of the Prime Minister and Cabinet has provided assistance during the set-up of the expanded office. The New Zealand Defence Force has provided secure offices for the IGIS office within Freyberg House and also provides IT support, on a cost recovery basis. I am grateful for the assistance of all three agencies.

Hon R A McGechan CNZM QC

Finally, I wish to acknowledge my predecessor the Hon R A McGechan CNZM QC who accepted appointment as Inspector-General on an interim basis in July 2013. In the ten months in which he held office, he made substantial progress, in an inherently difficult environment, in setting up an expanded Inspector-General's office and developing a comprehensive draft work programme for the office in respect of each agency. His work provides a strong platform for the continued oversight work of the office.

[39] IGIS Act, s 8.

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