Office of the Inspector-General of Intelligence and Security

Annual Report

For the year ended 30 June 2016

Cheryl Gwyn
Inspector-General of Intelligence and Security
27 October 2016

Contents

OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

27 October 2016

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 2015 – 30 June 2016.

The Inspector-General of Intelligence and Security Act 1996 requires you, as soon as practicable, to present a copy of the report to the House of Representatives (s 27(3) of 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 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.

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

The Inspector-General's office marked its 20th anniversary this year. The position evolved from the Security Review Authority, which operated within the State Services Commission when the New Zealand Security Intelligence Service was first established by statute in 1969, and the later position of Commissioner of Security Appeals.

The Inspector-General of Intelligence and Security Act 1996 (IGIS Act) extended the jurisdiction to the Government Communications Security Bureau.

Parliament intended that the new role of Inspector-General would enhance the independent oversight of the intelligence and security agencies but the limited resources provided to the office made it difficult for my predecessors to give full effect to that intention: the Inspector-General was a retired High Court Judge who carried out the role on a part-time basis with little, if anything, in the way of permanent administrative, communications or legal support.

My predecessors were constrained by that lack of resources and, as remains the case for some of our current work, much of their work was not and is not public. In this anniversary year, I wish to acknowledge the important role that my predecessors carried out. I acknowledge in particular the recent loss of the Hon Paul Neazor QC and his career of great public service as Inspector-General from 2004-2013, as Solicitor-General and as a Judge of the High Court.

The challenges faced by my predecessors were recognised in the *Kitteridge Report.*[1] The report recommended that the New Zealand Inspector-General's office be bolstered to more closely resemble the office of the Inspector-General in Australia, which was described as "robust and assertive".[2] The recommendations included broadening the pool of candidates for Inspector-General, increasing the IGIS's resources and staff and making the IGIS work programme more explicit.

The consequent changes to the IGIS Act, introduced in late 2013, resulted in the mandate and resources of the IGIS office being better aligned to meet Parliament's and public expectations of rigorous, independent oversight.

The past 20 years have also seen a considerable change in the working environment of the two intelligence and security agencies. The legality and propriety of their actions are subject to increased scrutiny, through the Inspector-General's work but also through that of the other oversight mechanisms and through increased public awareness. Public awareness has been informed by both greater openness by the agencies and unauthorised disclosures. These changes have the potential to lead to greater clarity and more stringent safeguards for the agencies, for government and for the public. However, as I recognise in this report, meeting that potential is a challenge for agencies previously unaccustomed to it. I acknowledge the work of agency staff in effecting that change.

The first periodic review of the intelligence and security agencies, legislation governing them and their oversight legislation took place in this reporting year.[3] The review was carried out by

---

1 *Review of Compliance at the Government Communications Security Bureau*, Rebecca Kitteridge, March 2013 (*Kitteridge Report*), para 85.

2 *Kitteridge Report*, para 92.

3 As required by the Intelligence and Security Committee Act 1996 (ISC Act), s 21.

the Honourable Sir Michael Cullen, KNZM and Dame Patsy Reddy, DNZM (the Cullen/Reddy review).[4]

The New Zealand Intelligence and Security Bill (NZ I&S Bill), which is intended to implement the government response to the review, was introduced into the House after the end of this reporting year. The Bill, as introduced, will consolidate and clarify the jurisdiction and powers of the Inspector-General and I hope will continue to provide a robust framework for Inspector-General oversight of the agencies.

[4] Report of the First Independent Review of Intelligence and Security in New Zealand, *"Intelligence and Security in Free Society"*, which was released by the reviewers and tabled in Parliament on 9 March 2016.

ROLE OF THE INSPECTOR-GENERAL

The Inspector-General oversees the intelligence and security agencies, the New Zealand Security Intelligence Service (NZSIS or the Service) and the Government Communications Security Bureau (GCSB or the Bureau).

The Inspector-General's statutory role is to assist the Minister responsible for each of the agencies to ensure that their activities comply with the law.[5]

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.

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 a complaint by a member of the public, or an employee, or former employee, of an intelligence and security agency, if that 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.

In order to carry out these functions, I have a right of access to security records[6] held by the agencies and a right of access to the agencies' premises,[7] including the Bureau's two communications interception stations: the high-frequency radio interception and direction-finding station at Tangimoana and the satellite communications interception station at Waihopai.

My role is primarily after the fact — that is, after particular operations have concluded, or at least commenced — which is the most common 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, or to advise the agencies, there are situations where prior discussion with my office can help to ensure clarity about the legality and propriety of any planned activity, as well as making subsequent review more straightforward and effective.

I can only address the activities of 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.[8]

---

5 IGIS Act, s 4(a).

6 IGIS Act, ss 2 and 20.

7 IGIS Act, s 21.

8 This includes the National Assessments Bureau, the intelligence services of the New Zealand Defence Force, and the intelligence units of Immigration New Zealand, the New Zealand Customs Service and the New Zealand Police.

Key requirements for effective oversight

In my experience as Inspector-General, the key requirements to carry out the oversight role in an effective way are independence, access, adequate resources, investigative powers which can be employed on the Inspector-General's own initiative and the requirement for public reporting on the outcome of Inspector-General inquiries.

- *Independence* from the intelligence agencies themselves and from the executive is essential. The Inspector-General is an independent statutory office, organisationally separate from the NZSIS and GCSB and (unlike US intelligence Inspectors-General) there is no reporting line to the agencies. The office is at arm's-length from the executive. Although the current legislation provides that the role of the Inspector-General is to "assist" the Minister in charge of the agencies to ensure that their activities are lawful, that assistance takes the form of independent scrutiny: the IGIS is not subject to general direction from the responsible Minister, the Prime Minister or other Ministers on how responsibilities under the IGIS Act should be carried out.

- *Access:* Total, unmediated access to security information held by the intelligence and security agencies is essential for effective oversight. Generally, accessing material involves a process of consultation and discussion with agency staff, but ultimately it must be for the Inspector-General, rather than the agency Director, to decide what information the Inspector-General should see. That right is protected by the IGIS Act[9] and carried over into the NZ I&S Bill. Giving full effect to that right requires the agencies to be adequately resourced and organised to respond to the oversight requirements in a timely way.

- *Resources:* Sufficient, appropriate resources are essential. Currently the office of the IGIS comprises the Inspector-General, the Deputy Inspector-General, four Investigating Officers, an Office Manager/Executive Assistant and an IT Manager/Security Advisor. The resources are modest but adequate to carry out the office's current review, inquiry and complaints work.

- *Own-motion jurisdiction and investigative powers:* The complaints and review work are the bread and butter of the Inspector-General's work, but the ability to initiate an inquiry into the legality or propriety of agency activities, where that is in the public interest, and without the need for government request or concurrence, is vital for the independence and perception of independence of the office.[10] That ability is enshrined in the current legislation and carried into the NZ I&S Bill as introduced. There are also specific areas of jurisdiction under other legislation, and more are currently proposed.

- *Mandatory public reporting* annually and of specific inquiries, is an important aspect of effective oversight and of public accountability of the overseer. Public reporting is required by the IGIS Act.[11]

---

9 IGIS Act, s 20.

10 See below at pp 10-12.

11 IGIS Act, ss 25A(1), 27(6A).

THE YEAR IN REVIEW

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

- continued work on current inquiries and reviews
- receipt and investigation of a range of complaints
- review of GCSB and NZSIS warrants and authorisations
- ongoing assessment of the soundness of compliance systems and practices in the two agencies.

Increased oversight means increased demand on the agencies

One effect of the expanded mandate and corresponding increase in resources for the Inspector-General, which is obvious in retrospect, is that an Inspector-General's office that has the capacity to investigate, review and audit more, to ask more questions, will inevitably place demands and some strain on the agencies which must respond. Some of the compliance issues my office has identified during my first two years in office are longstanding and systemic in nature and, because of the limited oversight in place until the 2013 legislative reforms, had been subject to limited or no scrutiny by the Inspector-General. It has, necessarily, taken the agencies some time to address those issues and to consolidate or develop adequate internal processes and resources to meet the requirements of Inspector-General oversight. The practical effect of that has, sometimes, been delays and complications in gaining access to necessary information.

Measures of effectiveness

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

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

I believe that the office is making good progress against these measures. The breadth and depth of inspection and review work is illustrated by the ongoing inquiries and reviews outlined in

this report.[12] To date, the agencies have acted on all of the Inspector-General's findings and recommendations.[13]

The relatively large number of inquiries and reviews instituted by the office in the preceding reporting period has meant some delay in concluding those investigations and finalising reports. I acknowledge that inquiries must be completed within a reasonable period. If the matter is in the public interest, the public needs to know the answer to the questions posed as soon as possible. Likewise, the agency under scrutiny is entitled to have any issues about its performance evaluated and reported on without undue delay. While it is not possible to have a hard and fast rule, my objective is to complete all inquiries and reviews within six to 12 months, depending on the nature and scope.

Statutory advisory panel

The IGIS advisory panel[14] comprises two external members (Christopher Hodson QC and Angela Foulkes, who were appointed in October 2014) and the Inspector-General. The panel has held 13 scheduled meetings (including by secure teleconference when members were away from Wellington) since the external members' appointment. One or both external panel members have also attended other meetings with the Inspector-General and/or staff, including to review draft reports, discuss proposed legislative amendments and assist in planning the office's work programme.

Panel members have also undertaken briefings with the intelligence agencies; a visit to the GCSB station at Waihopai; reviews of substantial written material; and *ad hoc* meetings and discussions with the Inspector-General.

The advisory panel provides valuable support to the Inspector-General, the members bringing a diversity of experience, intellectual rigour and judgement to the role. They have the highest-level security clearance and can provide an external, but informed, perspective on substantive matters relating to the Inspector-General's oversight of the agencies. That perspective is particularly important working in a closed, classified environment.

Intelligence and Security Committee

The Intelligence and Security Committee (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.[15] The Inspector-General may, with the concurrence of the Prime Minister, report either generally or in respect of any particular matter to the ISC.[16] At the ISC's invitation I attended before it at a private hearing on 10 November 2015 to discuss my 2014/15 annual report.

---

12 See pp 10-12 below.

13 See 2014/2015 annual report at pp 25-28 and below at p 15. During the reporting year, the NZSIS also acted on recommendations made in the course of warrant reviews; individual complaints over security clearance vetting and also general comments on NZSIS practice; and in the own-motion inquiry into a category of intelligence warrants.

14 IGIS Act, ss 15A-15F.

15 IGIS Act, s 27; ISC Act, s 61F.

16 IGIS Act, s 27(7).

Independent review of intelligence and security legislation

The Cullen/Reddy review[17] was timely: the NZSIS Act has been in effect for 47 years and the GCSB Act for 13 years. The Intelligence and Security Committee Act 1996 (ISC Act), like the IGIS Act, was enacted 20 years ago.

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

I welcomed the opportunity to meet on a number of occasions with the reviewers. The focus of my discussions was on the need for any new legislation to:

- set out clearly the powers of the agencies, purpose of those powers and controls on them
- include proper accountability and oversight mechanisms
- meet the requirements of legality and propriety and consistency with human rights.

17 See above, p 2.

THE YEAR AHEAD

Work programme

The IGIS Act requires me to prepare a programme of work for general oversight and review of the agencies I oversee, the NZSIS and the GCSB.[18] The bulk of the work programme is directed at the functions which are specified in the IGIS Act.[19]

I submit the work programme to the Minister responsible for each of the agencies[20] for approval.[21] 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 work programme in place during the reporting year was the first to be made public (www.igis.govt.nz/publications/igis-work-programme-july-2015/).

The NZ I&S Bill will be passed in the 2016/17 reporting year and I anticipate it will generate a considerable amount of work, for both the agencies and my office, in implementing and overseeing revised procedures, particularly the proposed new authorisations regime.

As current reviews and inquiries are completed and reports issued, I will identify further areas of the agencies' operations for review and possible areas for thematic investigations.

Legislative review

The NZ I&S Bill was introduced into Parliament after this reporting period. The Bill implements the Cullen/Reddy review.

I anticipate making a submission to the Foreign Affairs, Defence and Trade Select Committee on some aspects of the Bill.

---

18 IGIS Act, s 11(1)(e).
19 IGIS Act, s 11(1)(a)-(da).
20 For the reporting period, the Hon Christopher Finlayson QC, who is both the Minister in charge of the NZSIS and the Minister responsible for the GCSB.
21 IGIS Act, s 11(1)(e).

I expect to engage with the agencies in preparation for the introduction of the new legislation, particularly the regime relating to authorisations for the agencies to carry out activities that would otherwise be unlawful[22] and the preparation and implementation of ministerial policy statements covering other covert activity.[23]

[22] NZ I&S Bill, Part 4, replacing the existing provisions in each of the NZSIS Act and GCSB Act, relating to interception and intelligence warrants and authorisations.

[23] NZ I&S Bill, Part 7.

INQUIRIES

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.

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 the two 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?

New own-motion inquiries

I did not initiate any new own-motion inquiries during the reporting period.

Reporting on own-motion inquiries carried over from previous reporting years

Complex and sensitive category of warrants

This inquiry was initiated by the previous Inspector-General in early 2014. The 2014/2015 annual report recorded that I had made provisional findings and recommendations in this inquiry and NZSIS had accepted those findings and agreed to implement the recommendations made in future warrant applications. I noted that I would comment on subsequent warrant applications of the same kind in my final inquiry report.

I completed a draft report at the end of the reporting year and consulted the NZSIS, to ensure the accuracy and fairness of its contents and to identify any matters that could not be made public. I concluded that it would be harmful to national security to disclose the operational

detail of individual warrants but that it was nonetheless possible to report in concrete terms about the inquiry, the issues and problems identified and the changes that I considered necessary. My public report will shortly be released on my office's website. In summary:

- the NZSIS has effectively implemented the recommendations made in my provisional findings in new warrant applications of the same kind;
- subsequent applications have met the requirements to disclose all relevant information and set out how the NZSIS believes the criteria for the issue of a warrant are met in the particular case; and
- while the additional information should not have been omitted and its inclusion substantially strengthened and clarified the new warrant applications, the omissions were not such as to materially misinform the responsible Minister and the Commissioner of Security Warrants. As flagged in the 2014/15 annual report, I reviewed the potential effect of the omission. Had I found a risk of material misinformation, I would have recommended that the Minister and Commissioner reconsider the relevant warrant decisions. The recommendations to strengthen warrant applications also apply to other NZSIS warrants.[24]

Inquiry into warnings given by NZSIS officers

I commenced this inquiry, about the giving of warnings by NZSIS officers to members of the public, in June 2014. As noted in the 2014/2015 annual report,[25] it proved very difficult to locate detailed information on which to proceed. For that reason and also to allow my office to progress other work, this inquiry remained outstanding at the end of this reporting year. As a result of internal policy and procedure reviews by the NZSIS, it has since been possible to finalise a draft report to provide to the NZSIS for discussion and I will finalise the inquiry as soon as possible after receiving NZSIS's response to the draft.

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

I commenced this inquiry in response to the issues that were raised in 2015 around a bid by the Hon Tim Groser MP, the then Minister of Trade, to become Director-General of the World Trade Organisation. Completion of the inquiry has been slower than anticipated because of volume of work and staff changes, but my draft report was provided to the GCSB and witnesses to the inquiry shortly after the end of the reporting year, for consultation as to factual accuracy and any adverse comment. I expect to complete a public report shortly.

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

In 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.

---

24 See pp 19-20 below.

25 Annual report 2014/15, pp 21-22.

My inquiry is into whether New Zealand's intelligence agencies knew or were otherwise connected with, or risked connection to, the activities discussed in the US Senate report.

Work on this inquiry is ongoing and I hope to be able to report publicly by late 2016/early 2017.

Inquiry into complaints regarding alleged GCSB surveillance in the South Pacific

This inquiry stemmed from a number of complaints that individuals may have been adversely affected by alleged GCSB surveillance in the South Pacific. I also examined the broader context of those complaints under my general review power. Most of the work on this inquiry has now been completed and I anticipate that, following consultation with affected parties, I will be able to release a public report in December 2016.

COMPLAINTS

Security vetting complaints

Three complaints were received by my office regarding security vetting requirements. I also received one further inquiry on this issue, which did not result in a formal complaint being accepted.

The first complaint concerned an application for a position within one of the intelligence agencies. The complainant was concerned that the intelligence agencies were not providing potential employees with enough initial information regarding the requirements they must meet in order to obtain a security clearance. The matter was satisfactorily resolved by discussion with both the Service and Bureau Directors regarding their job advertisements, which have since been amended to better inform potential applicants.

The second complainant had applied for and been offered employment with one of the intelligence agencies, conditional on obtaining a security clearance. The security vetting process was commenced but, after six months, it was realised that the candidate did not meet all of the threshold requirements to enter the clearance process. Although the employing agency was informed at that point, it took another six months for the complainant to be informed. I have completed my investigation into this complaint and have provided recommendations to both Directors, which they have accepted. These included that agency staff responsible for screening applicants be provided with clear and consistent guidelines regarding security vetting requirements and that should an offer of employment need to be withdrawn, this occurs expeditiously. I am assured that work is already under way to ensure better communication and facilitation between the agencies and candidates.

The third complainant had applied for and been offered employment with a New Zealand government agency, but the Director of Security recommended to his prospective employer that a security clearance not be granted because aspects of the candidate's behaviour gave rise to questions around his decision-making, honesty, and ability to abide by the laws of New Zealand. I found that the vetting process generally met standards of procedural fairness but there was an absence of clear guidance in some areas which had adversely affected this candidate. I recommended that particular conduct which might ultimately be of security concern must be described objectively and consistently, both across different candidates and within reporting on an individual candidate. I also recommended that NZSIS's vetting questionnaire be reworded so that vetting candidates understood the full scope of the questions they were answering and therefore the assessments and conclusions that vetting staff might draw from their answers. The Director has agreed to address these questions.

Citizenship application inquiry

I received an inquiry about an historical NZSIS recommendation to the Minister of Internal Affairs that a person not be granted New Zealand citizenship. 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 citizenship application that are relevant to security. While NZSIS may make recommendations, it is the Minister's decision to grant or deny citizenship. I am unable to release the detail of this inquiry, which contains sensitive information. However, the NZSIS has provided assurances that all citizenship assessments are conducted in good faith

and consider any current or recent information about the applicant relevant to the present day risk the applicant may pose to security. Where the NZSIS has previously issued an adverse recommendation in respect of a citizenship candidate this would not unduly influence any new assessment. Any historic information that is held by NZSIS would be considered having regard to the nature and the seriousness of the information, the passage of time, and any new material collected in the intervening period.

Privacy Act 1993 complaints

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

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.

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 agency 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.[26]

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 covers the mechanics of how protected disclosures are to be handled by IGIS staff.

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. In the meantime each agency has its own policy.

[26] IGIS Act, s 18.

GENERAL REVIEWS[27]

Review of NZSIS security vetting information practices

In January 2015 I commenced a review of the NZSIS'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 (vetting) and had anticipated concluding the review at the end of 2015. However, several unanticipated steps have taken further time:

- I decided, in late 2015, to report on this review in two stages, so as to allow the NZSIS to begin work promptly on a number of problems identified in the first stage. I completed that first stage in December 2015.
- The review has involved a great deal of information about NZSIS security measures and, as required under the Inspector-General of Intelligence and Security Act, it was necessary to consult with the NZSIS at length over what information could and could not be safely disclosed. That process took several months, culminating in the April 2016 public release of the first stage.[28]
- I completed provisional findings and recommendations in the second stage, concerning electronic records systems, at the end of this reporting year and expect to finalise those shortly.

Part one report

My *Public Report: Summary and Conclusions* was released in April 2016. I found that while NZSIS staff took their responsibilities seriously, aspects of the handling of this highly sensitive information did not comply either with general data protection principles, particularly in respect of intimate personal data collected, or with the New Zealand government *Protective Security Requirements*, which apply to government information that bears on national security. There were also inadequate safeguards around the use of this information and insufficient clarity for candidates for security clearances and for referees about the possible use of information provided.

In response, I made nine recommendations to bring NZSIS handling of all such information into compliance with these standards. The Director of the NZSIS accepted all of the recommendations. Of the nine recommendations, three have been partially implemented; three have not yet been implemented but material progress has been made towards implementation; two have not yet been implemented; and one does not currently require implementation because it relates to a procedure not currently used by the NZSIS.

I consider that while significant steps remain outstanding, the NZSIS has made meaningful progress. I am conscious that the security vetting aspect of the NZSIS's work is substantial: thousands of clearance assessments are made each year and the responsible staff comprise a significant proportion of total NZSIS personnel, such that changes in operating systems and

27 IGIS Act, s 11(1)(d)(ii).
28 www.igis.govt.nz/publications/investigation-reports/

procedures and staff training are substantial tasks. I will continue to closely monitor the NZSIS's implementation of these recommendations.

Summary of recommendations	**NZSIS implementation**	**Comment**
R1. Restrict access controls for vetting files so that relevant staff each have access only to those records that they need at the time. Consider exclusive use of electronic files to enable better access controls.	Some greater restriction on existing access controls; reminder to staff of access obligations; and new files exclusively electronic.	*Partially implemented*: Access controls do not yet meet "need to know" standard, as large groups of users retain access to most files. Reminder not a substitute for controls; use of electronic files a positive development.
R2. Greater restriction of biographical data accessible to other NZSIS staff.		*Not yet implemented.*
R3. Ensure recording and audit of access and reasons for access.	Activity on relevant electronic systems now comprehensively logged and audited by general security systems.	*Partially implemented*: Recording of reasons for access to records remains outstanding; audit measures to be addressed in part two report.
R4. Introduce clear standards and procedures to ensure any non-vetting use of information justified and subject to appropriate safeguards.	Any requests to use vetting information currently require managerial approval. Procedures under review.	*In progress.*
R5. Review existing arrangements for non-vetting use of information against new standards.	Awaiting completion of response to R4 steps.	*Not yet implemented.*
R6. Develop safeguards against unfair use of vetting information by employers.	Substantial review work under way both for the Service and for other employers.	*In progress.*
R7. Adopt express standards for any pre-emptive advice of security risks to ensure consistency, justification and appropriate safeguards.	Risk advisories currently in use; policy to be reviewed.	*Implementation not currently required.*
R8. Adopt consistent and unequivocal advice for candidates, referees and others about use of information.	Review and amendment of documents currently under way.	*In progress.*

R9. Address internal inconsistencies in vetting-related practices.	Some structural changes made and internal practices aligned. Further reforms under way through major Service reform project; policy review; and staff development.	*Partially implemented and other substantial work in progress.*

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

The 2014/2015 annual report noted that my office had been in discussion with the NZSIS over access to information collected under these Acts. The objective of those discussions was to ensure that there is a clear and properly regulated regime for any such access. I concluded a report which identified a number of issues requiring a response from NZSIS. I also recommended it seek legal advice. The NZSIS has not yet completed all steps necessary to respond to my report. Once it has done so, I will report publicly to the extent I can, having regard to legal privilege and/or national security objections.

Summary guide to procedural fairness in security clearance vetting

In the 2014/2015 year my office's inquiries into complaints about the NZSIS security clearance vetting process revealed that NZSIS practice and procedure did not adequately meet the legal requirement of procedural fairness.[29]

As noted below, the NZSIS has made substantial progress in line with the Director's commitment last year to address this issue.[30] Our work had identified a range of issues, from the fundamental obligation of disclosure of adverse material to a candidate to more specific questions such as engagement with clinical and other experts. In order to assist the NZSIS in revising its practice and procedures, we have compiled that work into a summary guide. It may also provide useful information for security clearance candidates. It is now available on my office's website.[31] We will update it as relevant law is clarified or amended.

29 Annual report 2014/15, pp 15-17.
30 See below at p 27 and annual report 2014/15, p 17.
31 See www.igis.govt.nz/publications.

WARRANTS AND AUTHORISATIONS

Government Communications Security Bureau

Register of warrants and authorisations

The Bureau is required to keep a register of all interception warrants and access authorisations.[32] The register must contain specified information which includes the purpose of the warrant/authorisation and its duration, whose communications may be intercepted and/or at what place, who is authorised to make the interception or obtain access; and whether any other person or body is requested by the Bureau to assist in giving effect to the warrant or authorisation.[33]

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

Review of warrants

During the reporting year my office reviewed 15 interception warrants and 30 access authorisations issued under s 15A of the GCSB Act during the year. My regular discussions with the Bureau's legal team about those warrants and authorisations canvassed a number of matters directed at ensuring that warrant authorisation applications contain all relevant information and meet the statutory requirements. By way of example, matters discussed included:

- whether potential target groups can be more tightly delineated;
- the nature of controls and checks imposed on partner agencies with whom the Bureau shares data collected under a warrant or authorisation.

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 action 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.[34] 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.

---

32 GCSB Act, s 19.
33 GCSB Act, s 15E.
34 GCSB Act, ss 15(1) and 16(3).

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 can be shown, by his or her actions, to fall 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 Director's authorisations subject to the additional, more substantive criteria that apply to interception warrants and access authorisations.[35]

The requirement to keep a register of warrants and authorisations does not extend to Director's authorisations and several Director's authorisations which were signed off by the Director during the reporting year did not come to my attention until after 30 June. I will report on my review of those authorisations in the next annual report. I have discussed with the Bureau the need for prompt notification to my office of any future Director's authorisations.[36]

New Zealand Security Intelligence Service

During the reporting year my office reviewed the 39 domestic intelligence and 18 foreign intelligence warrants issued during the reporting period under s 4A of the NZSIS Act.[37] Those statistics include one domestic visual surveillance warrant issued and reviewed during the reporting period and one urgent/emergency authorisation for domestic warrantless surveillance, also issued by the Director within the reporting period.

As with the GCSB, we have discussed with the NZSIS a range of matters raised in the course of inspection of all warrants issued and from two 'end to end' reviews, including:

- The level of detail required in NZSIS warrant applications as to the likelihood that the communications sought to be intercepted or seized under the proposed warrant are privileged, including how any unforeseen interception or seizure of privileged material is to be identified and resolved. This includes circumstances relating to legal professional privilege and religious privilege.

- What measures are required to minimise the risk of inadvertent interception of third party communications.

35 GCSB Act, see s 15A(2): 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.

36 The NZ I&S Bill, as introduced, does not include an equivalent to s 16 GCSB Act authorisations.

37 Further to my 2014/2015 annual report (p 32, n 49), I obtained agreement to report the latter number.

Visual surveillance warrants

One visual surveillance warrant was issued during the reporting period.[38] I was notified of the issue of this warrant on the same day it was signed by the Minister and Commissioner.

In the 2014/15 annual report, I committed to undertake an 'end to end' review of the first visual surveillance warrants sought and issued under the amended legislation, to assess both the basis on which the powers were sought and how they were exercised.

I concluded this review in December 2015 and made recommendations to the Director regarding the Service's warrant applications. These included recommendations about the specificity of the information sought to be obtained under warrant, the degree of detail to be provided to the Minister and/or the Commissioner of Security Warrants in the application for the warrant, the information regarding areas of uncertainty, the information relevant to impacts on third parties and the likelihood of intercepting privileged communications, and the need for on-going reviews of the necessity of warrants.

Later in the reporting year, the NZSIS notified me of another visual surveillance warrant.[39] We reviewed the warrant and warrant application and spoke to NZSIS personnel involved. The warrant application set out sufficient detail of the proposed surveillance and how that surveillance satisfied the requirements for issue, and the warranted powers sought were carefully framed. I considered that the application did not give rise to any concern and, in terms of NZSIS practice, was a positive step.

First authorisation for urgent surveillance without a warrant

During the reporting year, the Director notified me that she had issued an authorisation for urgent surveillance without a warrant under s 4ID(1) of the NZSIS Act. Notification was made immediately, as required by s 4IE(1)(b). The authorisation was the first since the late 2014 enactment of s 4ID, which permits surveillance without warrant for up to 24 hours in cases of urgency.

I am required to investigate such authorisations if the Minister or the Commissioner of Security Warrants directs the surveillance to stop; if the authorisation is not followed by an application for a surveillance warrant; or if an application is made but declined.[40] In this instance, the Minister and Commissioner did not direct surveillance to stop and, within the 24 hour period, received and granted an application for a surveillance warrant. For that reason, I was not required to carry out a specific investigation but my office did review the authorisation and supporting material as part of our regular review of warrants and authorisations. We provided some comment on how the authorisation could have been framed more clearly, but did not consider there to be any material concern.

---

38 NZSIS Act, ss 4IA-4IC.
39 NZSIS Act, s 4IB(9).
40 NZSIS Act, s 4IE.

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.[41]

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 activities. Because of the large volume of decisions and operations, I cannot scrutinise all activities – with the exception of warrants and authorisations – at all times and, in particular, must be selective about those activities to examine in depth; and
- 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.[42]

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

41 IGIS Act, s 27(2)(ba). See also IGIS Act, s 11(1)(d).

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

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 their work.

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

Compliance framework

GCSB has an overarching Legal and Compliance Policy which outlines GCSB's overall commitment to compliance. The Compliance Management Framework gives effect to the Legal and Compliance Policy and was developed as a direct result of the recommendations in the *Kitteridge Report*.

The Compliance Management Framework establishes a strategic framework that defines the responsibilities of GCSB management and employees, and facilitates the implementation of robust practices for the effective management of compliance obligations.

Joint policy framework for GCSB and NZSIS

GCSB and NZSIS have a Joint Policy Framework which establishes requirements for the development, approval, implementation and review of GCSB and NZSIS policy instruments. Its purposes are to:

- support consistent and high-quality policy development, implementation and review within GCSB and NZSIS;
- provide clarity about the application of policy instruments; and
- enhance compliance and accountability across both agencies.

The Framework has been in force since 10 June 2016 and was a collaborative effort between both GCSB and NZSIS Compliance and Policy teams.

Compliance oversight structure

During the review period there were some changes to the GCSB's Compliance and Policy structure. The separate Compliance Auditor and Compliance Adviser roles were disestablished and replaced with two Compliance Adviser roles, responsible for advice, audits and investigations. Alongside these positions are two Policy Analyst roles. Expert audit advice and oversight is provided by the NZSIS Compliance Manager. The Compliance Trainer sits within the Learning and Development Team but the great majority of her time is dedicated to developing, providing and overseeing compliance training.

Compliance audit practices

The Bureau has a Compliance Audit Plan focused on the highest risk activities. The Compliance Team 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.

It will be important for the Bureau to maintain its previous rigorous audit practice under the new compliance structure. I will monitor this during the next 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 possible breach of a procedure, policy, warrant or authorisation, or 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 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.

The Bureau advised my office of the results of four completed investigations of possible incidents during the reporting year. The Bureau also notified seven other possible incidents during the reporting year which compliance staff are currently investigating, together with two commenced in 2014-2015.

Each of the completed investigations relates to particular cybersecurity or intelligence-gathering activities and, to avoid prejudice to the national security objectives of those activities, it is necessary to withhold the detail of that activity. However, it is possible to provide the following information:

- One investigation related to a potential error in reporting of historical unlawful intelligence-gathering, along the lines already identified in the *Kitteridge Report*. The compliance investigation determined that any further inquiry would be frustrated by poor past documentation and incomplete historical records. In any event, the Director concluded, there was no credible reason to suspect that there was unlawful intelligence-gathering further to that already identified. On that basis there was no further audit or investigation. The recommendations of the investigation

included a review of internal policies to ensure retention of records is consistent with the Public Records Act and other relevant legislation.

- Two investigations related to cybersecurity activities and each involved collection of data beyond the scope of the intended activity and corresponding authorisation. The collection of excess data was unintentional and arose from technical attributes of the collection process: the excess data was isolated and deleted and steps taken to prevent recurrence. Similarly, a third investigation relating to an information assurance activity found unintended data collection that was an inevitable, but unanticipated, effect of the intended activity – that is, the activity could not be carried out without collecting that data. In that instance, no data was retained and changes were made for future such activities.

I am currently considering whether it is possible and, if so, necessary to inquire any further into the historical issue.

I am satisfied that the cybersecurity and information assurance matters involved inadvertent error, rather than systemic deficiency, and that there was no material adverse consequence.

I expect to receive, assess and report on the current investigations in the course of the 2016/17 reporting year. I emphasise that, at this stage, these are only potential incidents and do not indicate actual non-compliance: in any case, in my view, they indicate a healthy internal reporting and review process. However, I will take all necessary steps if either the Bureau's own investigation or my office's review into these matters reveal pressing concerns. In particular, I will consider in each such instance above whether it indicates any systemic shortcomings or simple error and will ensure that deletion of data and any other necessary remedial steps have been taken.

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, discussion of proposed investigative and/or remedial steps with the Compliance and Policy Manager and sometimes the Chief Legal Adviser;

- consultation with my office on novel or likely contentious actions or issues. While it would be inconsistent with my review and oversight role to provide prior authorisation for particular actions, such consultation does provide 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 his senior staff, including in regular joint meetings with the Director and senior staff of the NZSIS;
- monthly meetings with the Chief Legal Adviser to discuss any questions or issues identified in our regular review of warrants and authorisations; and
- consultation on draft policies and procedures.

My compliance 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, I assess that Bureau staff are well-directed and 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. One case reflected historical deficiencies in record-keeping which, I am satisfied, have now been addressed.

I have flagged two areas for specific monitoring:

- the ability to maintain a rigorous audit practice, as noted above; and
- as at the end of the reporting year, there was no finalised Data Retention Policy in place. This is critical, particularly for a signals intelligence agency because of the large volumes of data collected. A draft policy has been the subject of extended discussion between the GCSB and my office. It is important that a final and rigorous policy is implemented as soon as possible.

Overall, 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

In my 2014/2015 annual report, I noted the importance of the agencies having clear, workable and auditable internal compliance systems. I recorded that, at that point, I was not able to conclude that the NZSIS had sound compliance procedures and systems in place. As I also recorded, however, the NZSIS had conducted an internal compliance review, which was concluded in June 2015, and had committed to implement the findings of that review over two to three years. I also recognised that there were some existing areas of strong practice.

Substantial structural and policy reforms

The NZSIS has made significant progress in building a compliance framework and implementing compliance practices in its operations:

- It has a Joint Policy Framework with the GCSB, as noted above.
- It has a Compliance Framework for operational activity in place since 10 June 2016 which commits NZSIS staff to:
  - identifying compliance obligations
  - tracking the number and severity of compliance incidents and reporting these to management
  - developing the annual compliance audit plan on a risk-based approach
  - undertaking compliance audits
  - monitoring the process of implementing audit recommendations
  - reporting and investigating suspected or actual non-compliance.
- It has a fulltime Compliance Manager and an Advisor for operational policy.
- It has done a stocktake of existing policies and standard operating procedures (SOPs) and instituted a plan to develop guidance to fill any gaps. Of eight discrete policy areas identified by NZSIS, it has completed review and development work in three; it has draft materials under way in two more and expects to complete the remaining three by the end of this reporting year. The review and drafting of SOPs is being done, in the main, by operational staff, which means the SOPs are practical, useful and "owned" by those staff, but with oversight and support from compliance staff.
- Access to policy and procedure documents has dramatically improved: in contrast to the position in June 2015, when it was difficult to locate many such documents and to determine whether they were current or outdated, draft, or otherwise incomplete, the NZSIS intranet now provides

straightforward access to policy and procedure. It also provides a mechanism for staff to query or seek amendment to procedures.

- NZSIS has installed and commenced use of specialised compliance-reporting software.

Examples of compliance strength

In addition to these structural changes, my office's wider work with the NZSIS provides specific indications of how compliance works in practice. The NZSIS has made significant reforms to its working practices in two substantial areas, in part in response to issues identified in my office's inquiry and review work:

- The first area, which I mentioned in my 2014/2015 annual report, related to the application of procedural fairness in security clearance vetting. NZSIS has implemented significant improvements in its practices and is continuing to refine them. It intends to also reform its guiding policy documents, including in light of the summary guide that my office compiled.

- The second concerns the extent to which applications for intelligence warrants provide the responsible Minister and the Commissioner of Security Warrants with adequate information and assessment to allow those decision-makers to make an informed decision and, if necessary, to impose conditions on a warrant. My office has undertaken substantial work with the NZSIS, both in respect of the complex warrants inquiry mentioned and in our ongoing review work.[43] The NZSIS has adopted the changes I have recommended and my staff have regular discussions with the NZSIS legal team as new issues and questions arise.[44]

A compliance omission

One matter causes me significant concern. In early 2015 I raised a serious issue about whether certain NZSIS activity was lawful and, if not, how that was to be remedied. I raised the issue with the Director in June 2015 and provided the Director with detailed provisional findings on my view of the legality of the activity in August 2015. The NZSIS provided its first substantive response to the questions raised in March-April 2016.

I appreciate that the underlying issue is complex and substantial work is still under way on the outstanding aspects of the questions I raised. However, and regardless of the ultimate conclusions on the lawfulness of the activity in question, the time taken to engage with and resolve this significant issue is in itself a matter of concern. To ensure it operates lawfully, the NZSIS must be able to deal with such issues in a more timely way. I will report fully on this issue as soon as possible.[45]

---

43 See above at p 10.

44 We also meet regularly with senior staff responsible for compliance.

45 After consultation with the NZSIS, I have concluded that it is not currently possible to disclose the nature of the particular activity, as to do so would pose a risk to national security and public safety. It is also appropriate to wait on further information that the NZSIS is to provide.

Self-reporting of incidents

I noted in last year's annual report the NZSIS had set up a register for self-reported incidents of inadvertent interception. As I have observed previously, a robust self-reporting process is a necessary feature of a strong compliance culture and I welcomed this step.

Within this reporting year my office has reviewed the 12 incidents from 2014/15 (advised retrospectively when the register was set up) and the five incidents reported to us during the 2015/16 year.

In our examination of the 2014/15 and 2015/16 reports I noted that there appeared to be three main categories of inadvertent intercepts. These were:

- interception of incorrect telephone numbers;
- telephone numbers being intercepted correctly but subsequently being abandoned by the target and/or adopted by a non-target; and
- organisations assisting the Service with interception not being given the correct or most up to date documentation, eg assistance forms. This meant that those assisting had not signed the assistance forms relating to the most recent iteration of a warrant.

As to the first category, a SOP has since been developed to assist in reducing the number of the incidents. The SOP gives clear guidance to NZSIS officers and sets out a clear process. As to the second, all connected telephone lines are reviewed as frequently as possible, generally weekly. While this will not always prevent issues arising, it should ensure that the risk of error is reduced and any issues are picked up as soon as possible. As to the third category, the Service's internal documentation regarding warrants has been amended so that there is now a primary document for Service staff to refer to when checking whether an organisation providing assistance has signed the assistance forms.

I was also notified of an incident outside the above categories, relating to failure to follow instructions during an operation. The compliance report into this incident set out steps taken in response, including measures to reduce the likelihood of this occurring in future operations and speaking to staff. This incident appears discrete and I think the measures taken by NZSIS to reduce the risk of similar incidents occurring are sufficient.

Two other incidents came to my attention while carrying out warrant inspections. They were not 'inadvertent intercepts' so were not reported to my office through inclusion in the NZSIS register, but they were compliance incidents in a broader sense. I am continuing to discuss these incidents in the context of my office's regular review of warrants. I therefore recommended to the Director that it would be useful in the future to include all compliance incidents and investigations in a regular report to my office.

The Compliance Framework, in accordance with my recommendation, requires staff to report suspected or identified breaches of a compliance obligation (not just those relating to inadvertent intercepts) through their manager, to the Compliance Manager.[46] As a result all compliance incidents are now reported to my office. Within the next reporting year the

[46] See above at p 26.

Compliance Manager will also institute a quarterly compliance report, to provide my office and NZSIS senior leadership team with updates on implementation of the compliance programme and compliance incidents. The adoption of these measures means that errors are more likely to be promptly identified and appropriate remedies put in place. The ongoing work to update and develop policies and procedures will strengthen the proposed measures.

Interaction with IGIS Office

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

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

My compliance assessment

The systemic changes commenced by the NZSIS during the reporting year are welcome and will ultimately provide both day-to-day support for NZSIS operational activities and a means by which those activities can be more consistently and reliably planned, implemented, recorded and reviewed.

The expanded compliance structure and dedicated compliance staff will encourage NZSIS staff to see compliance with legislation and policy as an inherent part of their work and a safeguard for the organisation. It also enables the NZSIS to more readily engage with my office's review work in a constructive and effective way.

I have also noted substantive improvements in specific activities and operations, such as those given above.

I expect in the next reporting year the NZSIS will continue to operationalise its compliance policy and framework. As the Service recognises, compliance measures are not an optional extra or just about having the right documents in place. Those measures are intrinsic to the NZSIS's ability to operate lawfully and effectively. Adoption of robust compliance measures means:

- errors are promptly identified and appropriate remedial steps put in place, minimising legal and reputational exposure;
- NZSIS operational personnel will have appropriate safeguards in place, which are necessary to carry out work that is sometimes difficult or complex, and in some instances personally dangerous;

- IGIS review and oversight is easier and more comprehensive; and
- the Director, the Minister in charge of the NZSIS and the public will have greater confidence that the NZSIS acts lawfully and with propriety.

As well as consolidation of the positive steps taken to date, in the next reporting year I expect to see, for example, regular tracking and analysis of any trends arising from the self-reported incidents; full and timely records of operational activity and decision-making, and development and implementation of an audit plan.

I hope too that the increased funding available to the agencies in the next reporting year will enable the NZSIS to better manage the demands inevitably placed on the organisation by systematic Inspector-General oversight and review, and to do so in a timely and efficient way, while dealing with the pressures of operational activity.

Overall, I conclude that some further work is required before I can assess NZSIS's compliance procedures and systems as sound, but on the basis of the considerable progress made in this reporting year and the clear commitment of the organisation to maintain that momentum, I hope to be able to do so in my next annual report.

OTHER ACTIVITIES

The Privacy Commissioner, Chief Ombudsman, Auditor-General and I meet regularly as the Intelligence and Security Oversight Coordination Group. Each of us has a role in oversight of the intelligence and security agencies and it has proved useful to discuss areas of overlap in our responsibilities and broader issues of common interest.

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 Dame Silvia Cartwright Lecture (Auckland Women Lawyers' Association) and to WIIS (Women in International Security). I participated in the New Zealand Centre for Public Law Public Office-Holders Series and was a panel member on the Surveillance and Privacy Panel at the Wellington Privacy Forum. I was also invited to give a presentation on the role of intelligence and security oversight in building confidence about privacy and data protection, at the 37th International Conference of Data Protection and Privacy Commissioners, in Amsterdam, in October 2015.

I contributed to Rod Vaughan's *Listener* article "Secrets and Spies" and to Anthony Hubbard's "National Portrait" in the *Dominion Post* and gave interviews to journalists Andrea Vance (TVNZ) and Jane Patterson (RNZ).

The Deputy Inspector-General presented in March 2016 at a conference organised by the International Association of Constitutional Law and Kings College London on *Accountability for Transnational Counter-terrorism Operations*.

Two of my staff and I met with the Australian Inspector-General in April 2016 to discuss common issues and best oversight practice.

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.[47] 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.

2015/16 budget and actual expenditure

Total expenditure for the 2015/2016 year was $1.267 million, as follows:

	Actual ($000s)	*Budget*
Staff salaries/advisory panel fees; travel	586	*690*
Premises rental and associated services	99	*97*
Other expenses	-3	*121*
Non-Departmental Output Expenses (PLA)	585	*590*
Total	1,267	*1,498*

Total budgeted expenditure remained at approximately one percent of the 2015/2016 budgeted estimates for the two intelligence agencies, which were $140.279 million before supplementary appropriations.

The variance (-15.5%) between actual and budgeted expenditure is largely due to two matters:

- The personnel variance is largely a result of the early departure of one seconded staff member as a result of her appointment as a coroner and necessary delays between staff departures and replacement appointments to allow for security clearance procedures. Advisory panel expenditure was also slightly lower than forecast. Staff expenditure is likely to increase slightly as staff departures/arrivals become more settled and because of the greater seniority of some replacement staff.
- The variance in "other expenses" largely relates to amounts accrued from the 2014/2015 year to cover potential costs remaining from the 2013/2014 establishment of the current office space in Freyberg House. Some anticipated costs of the Freyberg House establishment did not arise. I was also grateful that the Ministry of Justice was able to secure a sublease of the office space previously used much earlier than anticipated, again lessening overall cost.

Budgeted expenditure for the 2016/2017 year is not yet fixed, largely because that will depend on when replacement staff members are able to start. However, subject to any increase in

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

workload or other demands for statutory or operational reasons, expenditure should remain at about the same level as for this reporting year.

Administrative support

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

Office of the Inspector-General of Intelligence and Security
P O Box 5609
Wellington 6145
64 4 439 6721
enquiries@igis.govt.nz
www.igis.govt.nz

Follow us on Twitter @igis.nz